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

Albert D. Lumingkewas<sup>(1)</sup>, Arie S.M. Lumenta, ST., MT<sup>(2)</sup>, Xaverius B.N. Najoan, ST., MT<sup>(3)</sup> (1)Mahasiswa, (2)Pembimbing 1, (3)Pembimbing 2 E-Mail : danielkleak@yahoo.co.id<sup>(1)</sup>,al@unsrat.ac.id<sup>(2)</sup>,xnajoan@unsrat.ac.id<sup>(3)</sup>

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 failover 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

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*.

# PC Gate why Master PC Gate why Master FC Gate why Master

#### **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 ISP1. Saat ISP1 down, maka koneksi akan dipindahkan ke ISP1. Saat ISP1 down, maka koneksi akan dipindahkan ke ISP2. Saat ISP1 kembali normal, maka koneksi akan dipindahkan ke ISP2.

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 1. Perancangan jaringan

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*.



#### 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

πιαπιαί Π	. 192.100.30.1
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
	Eth0	192.168.50.60	192.168.1.1	192.168.50.3
Client			192.168.100.1	
	Eth1	192.168.50.1		
	Eth2	192.168.100.8	192.168.1.1	192.168.1.1
Gateway Master	Eth3	192.168.1.102	192.168.100.1	192.168.100.1
	Carp1	192.168.50.3		
	Eth0	192.168.100.7		
Gateway	Eth1	192.168.50.2	192.168.1.1	192.168.1.1
Backup	Eth3	192.168.1.103	192.168.100.1	192.168.100.1
	Carp1	192.168.50.3		



Gambar 5. Flowchart Program Absensi RFID

Dikonfigurasi sebagai berikut:

U	0
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

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 l > /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 MASOUERADE

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.

😳 Zenmap		- • •
Scan Tools Profile He	p	
Target: 192.168.50.0/24	▼ Profile:	▼ Scan Cancel
Command: nmap -sn 192	168.50.0/24	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS ◀ Host 🔹	nmap -sn 192.168.50.0/24	💌 📱 Details
<ul> <li>192.168.100.8</li> <li>192.168.100.7</li> <li>192.168.100.1</li> <li>192.168.50.60</li> <li>192.168.50.3</li> <li>192.168.50.2</li> <li>192.168.50.1</li> <li>192.168.50.1</li> <li>192.168.1003</li> <li>192.168.1002</li> </ul>	Starting Nmap 6.498ETA2 ( http://nmap.org ) at 2015-06-21 20:16           Nmap scan report for 192.168.50.1           Host is up (0.00s latency).           MAC Address: 44:87:FC:91:99:4F (Elitegroup Computer System CO.)           Nmap scan report for 192.168.50.2           Host is up (0.00s latency).           MAC Address: C4:6E:1F:05:DC:4D (Tp-1ink Technologies Co.)           Nmap scan report for 192.168.50.3           Host is up (0.00s latency).           MAC Address: C4:6E:1F:09:199:4F (Elitegroup Computer System CO.)           Nmap scan report for 192.168.50.3           Host is up (0.00s latency).           MAC Address: 44:87:FC:91:99:4F (Elitegroup Computer System CO.)           Nmap scan report for 192.168.50.60           Host is up.           Naps zen report for 192.168.50.40           Naps zen report for 192.168.50.60           Nost is up.           Naps zen report for 192.168.50.60           Nost is up.           Naps zen report for 192.168.50.60           Nost is up.	China Standard Time

#### 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 featurefeature scanning lainnya. Menjalankan perintah nmap pada komputer client untuk memeriksa alamat IP komputerkomputer 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

🐑 Zenmap	
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> e	łp
Target: 192.168.1.1/24	▼ Profile: Scan Cancel
Command: nmap -sn 192	16811/24
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans
OS 4 Host	nmap - sn 192.168.1.1/24 🔹 🗐 Details
<ul> <li>192.168.1.1</li> <li>192.168.1.102</li> <li>192.168.1.103</li> </ul>	Starting Nmap 6.498ETA2 ( http://nmap.org ) at 2015-06-21 17:54 China Standard Time Nmap scan report for 192.168.1.1 Host is up (0.005 latency). Nmap scan report for 192.168.1.102 Host is up (0.00050s latency). Nmap scan report for 192.168.1.103 Host is up. <u>Nmap done:</u> 256 IP addresses (3 hosts up) scanned in 127.67 seconds

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

Files A Littlentra Setting	Online
🖌 Lathanhar Samay	
Carlos - Los Ana Constantes	Website     Montain and a substitute     Montain and a substitute of the substite of the substitute of the substitute of the substitu
	Initial Designation     Initial State     Initial State     Initial State     Initial State     Initial State     Initial      Initia      Initial      Initia      Initial      Initial      Initial

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 <u>www.google.com</u> 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 <u>www.youtube.com</u> 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 <u>www.google.com</u>) *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

着 dier gw 16 den BC okprapeg (Mirestwik 1.12)	i (d.1264) geblice inv	n mate-112(	o ê 🖸
fie fat yen ho hatae gradue gado	ics Telephony Icols	Internalt. Help	
CONTRACTOR OF	*****		QQE #255 2
Rtei		bpesion.	las lage las
Ne. Time Scarce	Detiration	Potacel 1	angh Ho
14.000000192.168.50.60	74.125.130.105	1049	74 Ecto (ping) request, id=haMd, seq=45/22785, tt]=64 (no response found))
2 0.0006200192.168.50.60	74.125.130.106	1049	74 Echo (ping) request ind=bn000, seq=345/22785, ttl=63 (no response found!)
3 0.00009300192.008.30.00	74.125.130.100	1089	(4 ECD (pTmg) replest 10=000001, SEE=345/22/05, TTI=02 (ND RESPONDE TOURD!) 74 Tele (sign) convert id:0=00001 cons.316/32705 ttl_01 (see)) is 51
5 8 87541606 74 135 136 106	147 168 50 60	1/10	74 Echo (ping) respect (sensitive, second 25/7785 tt)-44 (respect in 4)
6 0. 52957400 192, 168, 50, 1	224.0.0.18	V000	7) Annuncement, (v2)
7 0.99836700192.168.50.60	74.125.130.105	ICM9	74 Echo (ping) request id=0x0001, sep=346/23041, ttl=64 (no response found!)
8 0. 99642800 192, 168, 50, 60	74.125.130.105	1049	74 Echo (ping) request id=UnUNE, sep=346/23041, ttl=63 (no response found!)
9.0.99846500192.168.50.60	74.125.130.106	106	74 Echo (ping) request id=0x0001, seq=146/23041, ttl=62 (no response found!)
10 -0. 99849500 192. 168. 50. 60	74.125.130.106	10%	74 Echo (ping) request id=0x0001, seq=346/23041, ttl=81 (reply in 11)
11 1.0/238400 /4.125.150.106	192.168.50.80	106	/4 Ecro (pring) reply 14=0x000, sep=346/23041, ttl=44 (replest in 10)
12 1. 32940100 192.108.30.1	224,0.0.18	7002	10 ATTORNEEDER. (VZ) 26 Teles (ning) consect iskulaMM1 con 3/7/32307 ttl.48 (on recence frankl)
14 1. 44676300147 168.50 60	74.125.130.106	100	74 Echo (ping) respect industrial, ang-967/22257, icinite (no respect round)
15 1, 99681400 192, 168, 50, 60	74.125.130.105	ICAS	74 Echo (ping) request id=0n000, seq=347/23397, ttl=62 (no response found!)
16 1, 99684300 192, 168, 50, 60	74.125.130.105	1049	74 Echo (ping) request id=1wWML, seq=347/132397, ttl=61 (reply in 17)
17 2.07233900 74.125.130.106	192.168.50.60	10%	74 Echo (ping) reply id=200001, seq=347/23397, ttl=44 (request in 16)
18 2.52948000 192.168.50.1	224.0.0.18	1880	70 Announcement (v2)
19 2, 99514600 192, 168, 50, 60	74.125.130.105	ION	74 Echo (ping) request id=2xXXX, seq=348/23553, tt1=64 (no response found!)
AU 2.99520/00192.168.50.60	/4.123.130.106	106	/4 ECTO (ping) request 14-Invite, seq=348(2353), tti=63 (no response found!)
21 2, 99324200 192, 106, 30, 50	74.123.130.100	109	14 ECRO (pTrog) request in-initial, sep-s46/2000; TCT=T2 (no response round))
22 2. 99927200 192. 200. 30. 00	102 168 50 60	1099	<pre>/# ELD (ping) respect N=NNNN, SEP=940(2000, L1=EL (respect in 20) 20 Erbs (nins) canly id=0.0000 can-308/73553 trl=0 (respect in 20)</pre>
24 3, 52950000 192, 168, 50, 1	224.0.0.18	1000	10 insurcement (v2)
25 3, 99346800 192, 168, 50, 60	74.125.130.106	1019	74 Echo (ping) request id=bNM01, seq=349/23009, ttl=64 (no response found!)
26 3. 99352600 192. 168. 50. 60	74.125.130.106	1092	74 Echo (ping) request id=2x0001, seg=349/23809, tt1=63 (no response found!)
27 1.99355800 192.168.50.60	74.125.130.105	IO6	74 Echo (ping) request id=0x0001, seq=349/23809, ttl=62 (no response found!)
28 3. 99956700 192. 168. 50. 60	74.125.130.106	ICAb	74 Echo (ping) request id=Nu001, seq=349/23809, ttl=EL (reply in 29)
29 4.07116600 74.125.130.106	192.168.50.60	IONo	74 Echo (ping) reply id=0x0001, sep=349/23009, tt1=44 (request in 28)
914.3/900/00192.108.30.1 21.5 AATAGOO 483 156 50 50	124.0.0.18 TA 105 100 106	1000	A ATTACKERET (V2) 14 Teles (sign) consert id. AnNAN you. 200/2005 stl.46 (an excessor frond))
22 5, 00753000 142 168 50 60	74.123.130.100	1040	24 trib (ping) repeat service, separation (in repeate control) 24 trib (nim) repeate (id-10001 con-350/2005, trl-6) (or records front)
23 5 00756500 102 168 50 60	74 125 130 106	TCVD	74 Echo (ninn) request id=0v0001 sen=250/24065 ttl=62 (no resnonse found1)
34 5,00759600 192,168,50,60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, sep=350/24065, tt]=61 (reply in 35)
35 5.08223200 74.125.130.106	192,168,50,60	ICMP	74 Echo (ping) reply id=0x0001, sep=350/24065, tt]=44 (repuest in 34)
36 6.00595700 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=351/24321, ttl=64 (no response found!)
37 6.00604100 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=351/24321, ttl=63 (no response found!)
38 6.00608400 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=351/24321, ttl=62 (no response found!)
39 6.00612100 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=351/24321, ttl=61 (no response found!)
40 8.60602800 192.168.50.2	224.0.0.18	VRRP	70 Announcement (v2)
41 8.83213800 192.168.50.2	224.0.0.251	MONS	140 Standard query 0x0000 ANY 3.50.168.192.in-addr.arpa, "QM" question ANY gu-desktop-19.local, "QM" c
42 8.83299200 192.168.50.2	224.0.0.251	MONS	140 standard query response 0x0000 AAAA, cache flush fe80::c66e:1fff:fe05:dc4d HINFO, cache flush 1686
43 9.082/9100192.168.50.2	224.0.0.251	MONS	140 Standard query UXUUUU ANY 3.50.108.192.10-a007.arpa, QM question ANY gi-oesktop-19.10cal, QM q 140 Standard query 0-0000 ANY 3.50.168.192.in-addr app. "Ou" question ANY gi-oesktop-19.10cal, QM q
44 9,00000000000000000000000000000000000	224.0.0.201	NUNC	ing standard niery records (NADON) AND 5.30.100.132. Intraux. atpa, UM QUESTION ANT Girtlesktup-19.10Cal, UM C 140 Standard niery records (NADON) Adda, carbe flick fe00::r666:1fff:fe0S:deld utuen, carbo flick fe00:
4.5 9.53440700192.100.30.2	224.0.0.231	NUNS	ано эсолиого цисту незроляе околого жини, сасле низл неоо.сове:Int.neo.cote плино, cache fluch 100 1000 128 Standard nuerv resonnse OxONON PTR rache flush nu-deskton-10 loral д rache flush 100 168 50 2
47 9, 92538900 192, 168, 50, 2	224.0.0.18	Vppp	70 Announcement (v)
48 10.7688010 192.168.50.2	224.0.0.251	MONS	144 Standard ouery response 0x0000 PTR, cache flush ow-desktop-19, local A, cache flush 192.168.50.3 A.
49 11.0134350 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=352/24577, ttl=64 (no response found!)
50 11.0135200 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=352/24577, ttl=63 (no response found!)
51 11.0135640 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=352/24577, ttl=62 (no response found!)
52 11.0136030 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seq=352/24577, ttl=61 (no response found!)
53 11, 3167950 192, 168, 50, 2	224.0.0.18	VRRP	70 Announcement (v2)
54 12.7083300 192.168.50.2	224.0.0.18	VRRP	70 Announcement (v2)
55 13.0053120 192.168.50.2	224.0.0.251	MONS	144 stanoaro query response 0x0000 PTR, cache flush gw-desktop-19.local A, cache flush 192.168.50.3 A,
50 14.099/430 192.168.50.2	224.0.0.18	VRRP	/V ANNOUNCEMENT (VZ)
5/ 15.49102/0192.108.50.2 58 16 0052450 102 168 50 50	74 105 100 106	TCHD	/U ANNUUNCHENI (VZ) 71 Echo (ning) request id_00001 con_252/0022 ++1_61 (no normanico foundi)
50 10.0032430 192.100.30.00	74.123.130.100	TCND	re cum (μπημ) request τα=υλουσμ, seq=33/24000, tll=04 (ND Responde found)) 74 Crbn (ninn) request id=0x0001 seq=353/24832 ttl=62 (no reconorse found))
60 16, 0053720 192 168 50 F0	74, 125, 130, 100	TCAN	74 Echo (ping) request id=0x0001, sep=353/24033, tcl=05 (no response round)
61 16.0054110 192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seg=353/24833, ttl=61 (no resoonse found!)
62 16. 8824150 192. 168. 50. 2	224.0.0.18	VRRP	70 Announcement (v2)
63 18.2739740 192.168.50.2	224.0.0.18	VRRP	70 Announcement (v2)
64 19.6653880 192.168.50.2	224.0.0.18	VRRP	70 Announcement (y2)

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 <u>www.google.com</u> 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.

 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 <u>www.google.com</u> pada terminal komputer client.
- Mematikan jalur ISP 1
- Mengaktifkan kembali jalur ISP 1

Elle Edit View Go Lapture Analyze Statis	tocs Telephony <u>T</u> ools , 🗢 🔿 🌍 🖥 🛓	Internals Help	Q. Q. 🗇   📓 🗟 🥵 %   📓
Filter		· Expression .	Clear Apply Save
No. Time Source	Destination	Protocol L	ength Info
1 0.00000000 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=208/53248, ttl=64 (reply in 2)
3 1 00003600 102 168 1 102	173 104 117 116	TCNP	100 Echn (ninn) request id=0x12ca, seq=200/S3240, tt1=64 (request in 1)
4 1,00959900 192,168,100,8	224.0.0.251	IGNPV2	48 Membership Report group 224, 0.0, 251
5 1.07494600 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=209/53504, ttl=54 (request in 3)
6 2.00200300 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=210/53760, ttl=64 (reply in 7)
7 2.07695000 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=210/53760, ttl=54 (request in 6)
8 3.00302000 192.168.1.102	1/3.194.11/.116	ICMP	100 Echo (ping) request id=0x12ca, seq=211/54016, ttl=64 (reply in 9)
10.4.00402700.192.168.1.102	173 194 117 116	TCNP	100 Echo (ning) reply tomotized, sequezzi 34010, clm34 (request in 8)
11 4.07794700 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=212/54272, ttl=54 (request in 10)
12 5.00500400 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=213/54528, ttl=64 (reply in 13)
13 5.07994700 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=213/54528, ttl=54 (request in 12)
14 6.00599900 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=214/54784, ttl=64 (reply in 15)
15 6.08394400 1/3.194.11/.116	192.168.1.102	ICMP	100 Echo (ping) reply 10=0x12ca, seq=214/54/84, ttl=54 (request in 14)
17 7 07006500 192.108.1.102	102 168 1 102	TCMP	100 Echo (ping) request id=0x122ca, Seq=213/33040, t1=04 (reply in 17) 100 Echo (ping) reply id=0x12ca, seq=215/55040, t1=54 (request in 16)
18 8,00804200 192, 168, 1, 102	173.194.117.116	TCNP	100 Echo (ping) repuy id=0x12ca, seq=216/55296, ttl=64 (reply in 19)
19 8.08194500 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=216/55296, ttl=54 (request in 18)
20 9.00901300 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=217/55552, ttl=64 (reply in 21)
21 9.08295400 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=217/55552, ttl=54 (request in 20)
22 10.0106330 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=218/55808, ttl=64 (reply in 23)
23 10.0839390 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=218/55808, ttl=54 (request in 22)
24 11,0110110 192,108,1,102 25 11 0840550 173 104 117 116	102 168 1 102	TCNP	100 Echo (ping) request 10+0X12cd, SEQ=219/30004, tt=04 (repiy in 23) 100 Echo (ninn) reniv id=0x12ca sen=210/56064 tt=1=54 (request in 24)
26 12,0129910 192,168,1,102	173, 194, 117, 116	TCNP	100 Echo (ping) reply id=0x12ca, seq=220/56320, tt]=64 (reply in 27)
27 12.0919370 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seg=220/56320, ttl=54 (request in 26)
28 13.0139940 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=221/56576, ttl=64 (reply in 29)
29 13.0899480 173.194.117.116	192.168.1.102	ICMP	100 Echo (ping) reply id=0x12ca, seq=221/56576, ttl=54 (request in 28)
30 14.0150130 192.168.1.102	173.194.117.116	ICMP	100 Echo (ping) request id=0x12ca, seq=222/56832, ttl=64 (reply in 31)
31 14.08994/01/3.194.11/.116	192.168.1.102	ICMP	100 ECH0 (ping) reply 10=0x12c2, seq=222/50832, ttl=54 (replyin 20)
52 13.0100030 132.108.1.102	1/3.154.11/.110	IOAP	Too Echo (phig) Tequest To=0x12ca, Seq=223/3/000, tc1=04 (Feb/y III 53)
33 15,0949490173.194,117,116	192.166.1.102	TONE	100 Ecbo (ptng) reply (d-0d2ca, sep-223/57088, tt1+54 (repest in 32)
54 15.9282660 127.0.0.1	12/.0.1.1	BN5	/s Standard query OctT4F A Gaisy abunta, con
35 15.9281830 127.0.0.1	127.0.1.1	015	78 Scandard query Oxofol AAAA daisy, ubuntu.com
96 15 9282410 192 168 100. #	192.166.1.1	045	ra standard query outdur a deisy.uturtu.com
1/ 15.9/82500 192.168.100.8	192.168.1.1	96	75 Standard query 0x00/7 A daisy.sbunto.com
16 15.9282890 192.108.100.8	192.188.1.1	UND I	A SEARCHIE GROUP ANAL BEISY, CONTUNCT, CONT SE Manhaethie States (Lange States 734 & 5.75)
39 13, 955644 192, 108, 50, 2 40 15 0465365 103 168 3 2	102 168 105 8	TURINS	The Avenue ratio and a service and the service of t
40 11 9401100 141 100-111	191-190-100-5	040	LEP SAME TO A TRANSPORT A LEASE AND A LEASE ALL
42.15.0504876102.168.1.1	192 165 100 8	DVS	113 Standard wany removes (nb/77 + 8 194 4) 57 ± 01 195 80 55
421400000000000000000000000000000000000	102100-100-1	1045	AND ADDRESS OF A TRADE OF A TRADE AND A TRADE AND A
44 16 0003170 197 168 1.1	197 168 100 8	240	155 transmi overv recome Intifit
45 16.0007730 127.0.1.1	127.0.0.1	DNS	150 Standard gamy retorne Dub/b4
40-10-7074960-192-178-100-1	COLUMN THE OWNER	105	THE PHER (WITH PARAMEL INDERING AND ADDRESS OF THE
47 16 0901119177.194 117.118	192.168.100.8	IOP	100 Echo (ging) reply 10-0x22x, sep-234/57344, tt1-54 (repart (n.45)
48 16.2376360 192.168.50.1	224.0.0.22	100Pv3	56 Rendership Report / Lesve proop 224.0.0.251
49 17.0176320 192.168.100.8	173.194.117.116	IOP	100 Echo (ping) request 1d=0012ca, sep=225/57600, ttl=64 (reply in 50).
50 17.0693580 173.194.117.116	192.168.100.F	IOW	100 Echo (ping) reply id-0x12ta, sep-225/57600, tt1-54 (ressent in 49)
51 18.0194680 192.168.100.8	173.194.117.116	IOP	100 Echo (ping) request id=0x02ca, sep=228/37830, ttl=64 (reply in 32)
52 18.0915720173.194.117.11F	192.168.100.8	10MP	100 Ecto (ping) reply id=0x12cz, sep=126/57850, ttl=54 (request in 51)
53 19.0006290 192.168.100.E	173.194.117.118	100	100 Eche (ping) request id-0x37ca, seq-227/58112, tt1-64 (reply in 54)
54 19.0920770173.194.117.11F	192.168.100.8	ICMP	100 Echn (ping) reply id=002zz, sep=227/58112, ttl=54 (request in 53)
55 20.0221370-192.168.100.B	173.194.117.116	IOF	100 Echo (ging) request (d=0xd2ca, 1eq=228/38368, ttl=64 (reply in 56)
56 20.0943478173.194.117.118	192.168.100.8	ICMP	100 Echo (ping) reply 16-0012ca, sep-228/38368, tt1-64 (request in 55)
57 20.9296530 127.0.0.1	177.0.1.1	9N5	78 Standard query Oxff4f A daisy, aburtu.com
58 20.9297740 192,168,100.8	192.168.1.1	06	78 standard query Qelido A daisy.sbuttu.com
59 20, 9488580 192, 168, 1, 1	192.168.100.8	015	110 Standard query response Extlick & 41,189,92,57 & 91,189,92,53
60 20.9489430127.0.1.1	127.0.0.1	DNS	110 Standard query response Doff4F & 41,169,92.57 & 91,189,92.55
61 30.9490100 127.0.0.1	127.0.1.1	DN5	78 standard query Oxbfb4 AAAA daisy: oburtu.com
62 20.9490740 192.168.100.8	192.168.1.1	015	78 Standard query Ox8299 AAAA daisy, vburtu.com
63 20.9677680 192.168.1.1	192.158.100.8	DNS	139 Standard query response 0x8219
64 20.9677730127.0.1.1	127.0.0.1	DNS	139 Standard overy response (obf)4

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 <u>www.youtube.com</u> 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 <u>www.google.com</u>) 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 <u>www.google.com</u> 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	
0.0000000		
1.00093600	1.00093600	
1.00093600		
2.00200300	1.00106700	
2.00200300		
3.00302000	1.00101700	
3.00302000		
4.00402700	1.00100700	
Rata-rata	<b>1.00100675</b> (detik)	

#### TABEL V. WAKTU PERALIHAN ISP 1-ISP 2

Waktu advertisement ISP 1	15.0949490
Waktu advertisement ISP 2	16.2376160
Waktu peralihan	<b>1,1426670</b> ( <i>detik</i> )

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 <u>www.google.com</u> 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 <u>www.youtube.com</u> dan <u>www.yahoo.com</u>.

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

File Edit View Go	Capture Analyze Statistic	s Telephony Iools (inter	nals <u>H</u> elp	
00111		🗧 🛊 🏟 🐺 🛓 📃	I Q	ର୍ ଦ୍ 🔟 📓 🕅 🦉 % 🔛
Filter:		*	Expression	Clear Apply Save
No. Time	Source	Destination	Protocol Le	ngh Info
1 0.000000	192.168.50.1	224.0.0.18	VRRP	72 Announcement (v2)
2 0.45/446	192.165.1.103	74.125.200.105	TONP	100 Echo (ping) request 10=0x1fid, seq=249/63/44, ttl=64 (reply in 3) 100 Echo (ning) request id=0x1fid, seq=240/63744, ttl=45 (request in 2)
4 0.998801	192.168.50.1	224.0.0.18	VRRP	72 Announcement (v2)
5 1.438876	192.168.1.103	74.125.200.103	ICMP	100 Echo (ping) request id=0x1f1d, seq=250/64000, ttl=64 (reply in 6)
6 1.512300	74.125.200.103	192.168.1.103	ICMP	100 Echo (ping) reply id=0x1f1d, seq=250/64000, ttl=45 (request in 5)
7 1.998308	192.168.50.1	224.0.0.18	VRRP	72 Announcement (V2)
9 2. 514798	74, 125, 200, 103	197.168.1.103	TCNP	100 Echo (ping) request io=0x110, seq=31/04230, tt1=04 (repry in 9)
10 2.997814	192.168.50.1	224.0.0.18	VRRP	72 Announcement (v2)
11 3.442595	192.168.1.103	74.125.200.103	ICNP	100 Echo (ping) request id=0x1f1d, seq=252/64512, ttl=64 (reply in 15)
12 3.504559	192.168.1.103	224.0.0.251	MDNS	189 Standard query response 0x0000 PTR, cache flush gw-desktop-19. local AAAA, cache flush fe80::2e0:4c <sup></sup>
14 3.510036	192.168.100.7	224.0.0.22	IGNPV3	56 Membership Report / Leave group 224.0.0.251
15 3.515318	74.125.200.103	192.168.1.103	ICMP	100 Echo (ping) reply id=0x1f1d, seq=252/64512, ttl=45 (request in 11)
16 3.521339	127.0.0.1	127.0.0.1	DNS	78 Standard guery 0x8971 A daisy.ubuntu.com
1/ 3.521409	Intercor_/0:/0:20 D_LinkTo 81:59:44		ARP	44 WHO NAS 192.168.100.17 TETT 192.168.100.7 62 192 168 100 1 is at c0:a0:bb:81:f0:44
19 3.521979	192.168.100.7	192.168.1.1	DNS	78 Standard guery 0x6064 A daisy.ubuntu.com
20 3.545415	192.168.1.1	192.168.100.7	DNS	110 Standard query response 0x6064 A 91.189.92.55 A 91.189.92.57
21 3.545653	127.0.0.1	127.0.0.1	DNS	110 Standard query response 0x8971 A 91.189.92.55 A 91.189.92.57
22 3.99/324	192.168.50.1	224.0.0.18 ff021.ff52.4459	VRRP	/2 Announcement (V2) 80 waiabbar salisitation for fa90+2x0+4xFF+fa52+4458
24 4.085983		ff02::16	ICNPV6	112 Multicast Listener Report Message V2
25 4.225998	192.168.100.7	224.0.0.22	IGNPV3	56 Membership Report / Leave group 224.0.0.251
26 4.442045	192.168.100.7	74.125.200.103	ICMP	100 Echo (ping) request id=0x1f1d, seq=253/64768, ttl=64 (reply in 27)
2/ 4.519836	/4.125.200.103	192.168.100.7	ICMP	100 Echo (ping) reply id=0x1r1d, seq=253/64/68, tt I=45 (request in 26)
29 4. 523957	192.168.100.7	192.168.1.1	DNS	78 Standard guery 0xb631 A daisy ubuntu.com
30 4.542483	192.168.1.1	192.168.100.7	DNS	110 Standard query response 0xb631 A 91.189.92.55 A 91.189.92.57
31 4.542612	127.0.0.1	127.0.0.1	DNS	110 Standard query response 0xc6e7 A 91.189.92.55 A 91.189.92.57
33 5:00756500	192:188:30:60	74.125.130.106	¥8NÞ	/2 announcement (V2) /4 Echo (ping) request id=0x0001, seq=350/24065, tti=62 (no response found!)
34 5.00759600	192.168.50.60	74.125.130.106	ICNP	74 Echo (ping) request id=0x0001, seq=350/24065, ttl=61 (reply in 35)
35 5.08223200	74.125.130.106	192.168.50.60	ICMP	74 Echo (ping) reply id=0x0001, seg=350/24065, ttl=44 (request in 34)
36 6.00595700	192.168.50.60	74.125.130.106	ICNP	74 Echo (ping) request id=0x0001, seq=351/24321, ttl=64 (no response found!)
37 6.00604100	192.168.50.60	74.125.130.106	ICNP	74 Echo (ping) request id=0x0001, seg=351/24321, ttl=63 (no response found!)
38 6.00608400	192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seg=351/24321, ttl=62 (no response found!)
39 6.00612100	192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seg=351/24321, ttl=61 (no response found!)
40 8.60602800	192.168.50.2	224.0.0.18	VRRP	70 Announcement (v2)
41 8.83213800	192.168.50.2	224.0.0.251	MDNS	140 Standard query 0x0000 ANY 3.50.168.192.in-addr.arpa, "ON" question ANY ow-desktop-19.local, "ON" on
42 8.83299200	192.168.50.2	224.0.0.251	MDNS	140 Standard query response 0x0000 AAAA, cache flush fe80::c66e:1fff:fe05:dc4d HINFO, cache flush I68E
43 9.08279100	192.168.50.2	224.0.0.251	MDNS	140 Standard query 0x0000 ANY 3.50.168.192, in-addr.arpa, "ON" question ANY ow-desktop-19. local, "ON" c
44 9, 33355200	192.168.50.2	224.0.0.251	MDNS	140 Standard query 0x0000 ANY 3.50.168.192.in-addr.arpa. "ON" question ANY qw-desktop-19.local, "ON" c
45 9, 33440700	192.168.50.2	224.0.0.251	MDNS	140 Standard query response 0x0000 AAAA, cache flush fe80::c66e:1fff:fe05:dc4d HINFO, cache flush I68E
46 9, 53407600	192.168.50.2	224.0.0.251	MDNS	128 Standard overv response 0x0000 PTR, cache flush ow-desktop-19. local A, cache flush 192.168.50.3
47 9,92538900	192.168.50.2	224.0.0.18	VRRP	70 Announcement (v2)
48 10, 7688010	192.168.50.2	224.0.0.251	MDNS	144 Standard overv response 0x0000 PTR, cache flush ow-desktop-19, local A, cache flush 192,168,50.3 A,
49 11.0134350	192.168.50.60	74.125.130.106	ICMP	74 Echo (ping) request id=0x0001, seg=352/24577, ttl=64 (no response found!)
50 11, 01 35200	192,168,50,60	74, 125, 130, 106	TCNP	74 Echo (ning) request id=0x0001, seg=352/24577, ttl=63 (no response found)
51 11 0135640	192, 168, 50, 60	74, 125, 130, 106	TCNP	74 Erbo (nino) request id=0x0001, seq=352/24577, ttl=62 (no response found!)
52 11 0136030	192 168 50 60	74 125 130 106	TCNP	74 Echo (ninn) request id=0v0001_seq=352/24577_tt]=61 (no response found1)
53 11 3167950	192 168 50 2	224 0 0 18	VDDD	70 Announcement (v2)
54 12, 7083300	192,168,50,2	224.0.0.18	VRRP	70 Announcement (v2)
55 13 0053120	102 168 50 2	224 0 0 251	NDNS	144 Standard nuery records 0y0000 PTP, cache fluch nu-desition-10 local & cache fluch 102 168 50 3 &
56 14. 0997430	192.168.50.2	224.0.0.18	VRRP	70 announcement (v2)
57 15 4010270	192 168 50 2	224 0 0 18	VDDD	70 Announcement (v2)
58 16 0052450	192 168 50 60	74 125 130 106	TCNP	74 Echo (minn) request id=0x0001 seq=353/24833 tt]=64 (no response found!)
50 16 0052200	102 168 50 60	74 125 130 106	TCNP	74 Echo (nino) request id-0x0001 seq-353/24033, ttl=63 (no response found)
60 16 0052700	192 168 50 60	74 125 130 106	TCNP	74 Echo (nino) request id=0x0001 seq=353/24033 tt]=62 (no response found))
61 16 005/11/	192 168 50 60	74 125 130 106	TCNP	74 Echo (nino) request id=0x0001 seq=353/24033 tt]=61 (no response found))
62 16 8824150	102 168 50 2	224 0 0 18	VDDD	70 Announcement (v2)
62 18 2720740	102 168 50 2	224.0.0.18	VDDD	70 Announcement (V2)
03 10.2/39/40	102.100.30.2	224.0.0.10	VARP	70 Kindunceren (V2)

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 <u>www.google.com</u>) 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 <u>www.google.com</u> 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	<b>1.001716</b> (detik)

#### TABEL VII. WAKTU PERALIHAN ISP 1-ISP 2

Waktu advertisement ISP 1	3.515318
Waktu advertisement ISP 2	4.442045
Waktu peralihan	<b>0.926727</b> (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 <u>www.youtube.com</u> 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.

- 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 didownload 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

- B. Raharjo : "Keamanan Sistem Informasi Berbasis Internet". PT Insan Infonesia, Jakarta, 2005
- [2] OpenBSD, Pf: firewall redundancy with carp and pfsync, [Online], Tersedia di : <u>http://openbsd.org/faq/pf/carp.html</u>,
- [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.