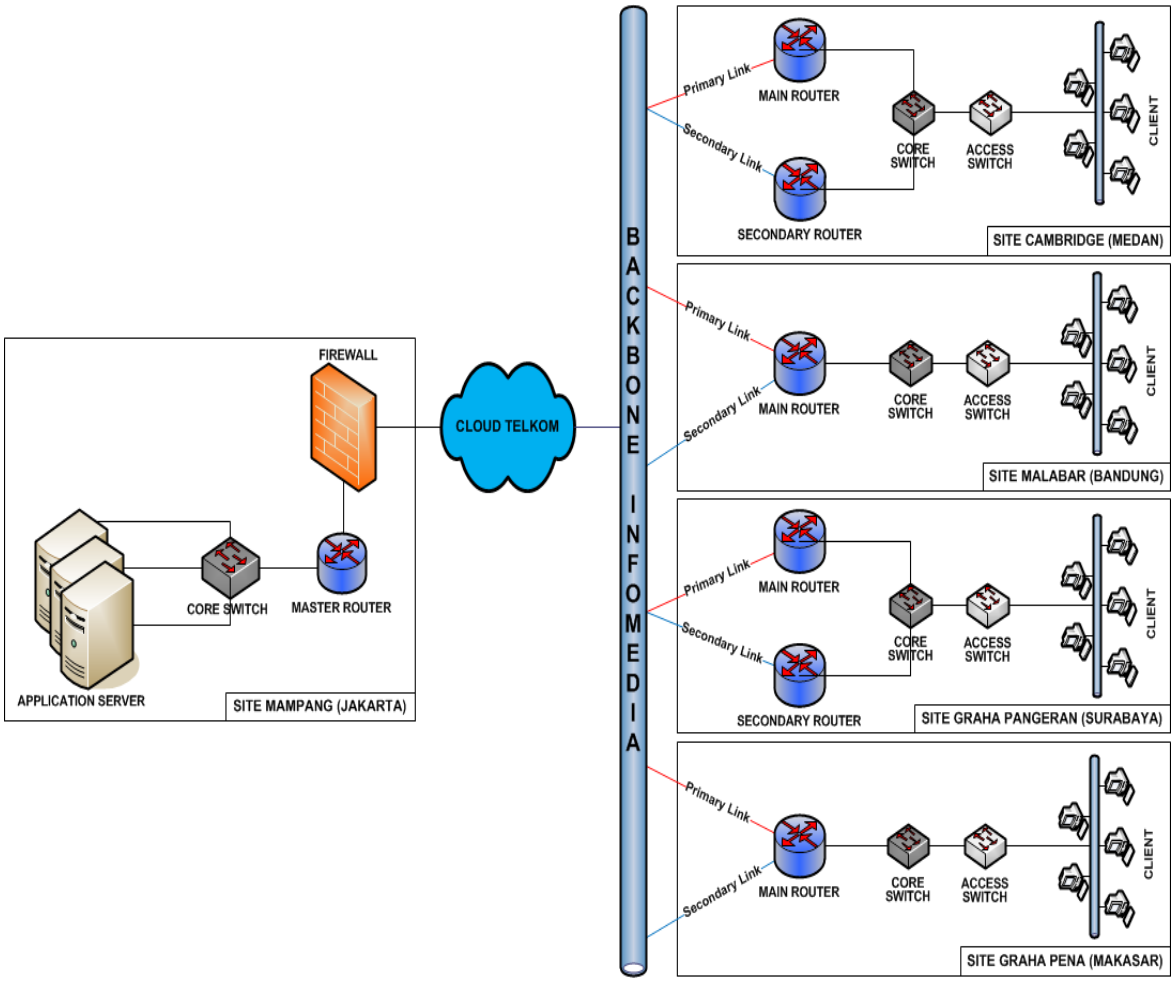
BAB 3
ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Sistem

Analisa merupakan suatu tindakan untuk mengetahui lebih jauh tentang semua objek yang akan diteliti. Pada bab ini menjelaskan tentang topologi jaringan yang telah berjalan, melakukan proses pengujian terhadap jaringan *cilent-server* di PT. Infomedia Nusantara dan melakukan perancangan berserta implementasi metode *Virtual Router Redudancy Protocol* (VRRP) yang digunakan dalam meningkatkan reliabilitas jaringan *client-server*. Sebelum dilakukan pengembangan dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan-kebutuhan pokok dalam membangun jaringan *client-server* menggunakan metode VRPP.

3.1.1 Analisis Jaringan Metro-E

Jaringan *Metro Ethernet* (Metro-E) yang diimplementasikan oleh PT. Infomedia Nusantara merupakan layanan akses *internet* dan komunikasi data dengan cakupan Metropolitan dengan kecepatan tinggi (*high speed*). Jaringan Metro-E memberikan kemudahan dalam layanan karena menggunakan *ethernet* sebagai *interface* yang sudah sangat dikenal oleh para pengguna piranti IT ataupun jaringan LAN dan telah memiliki sistem standar *interoperability* yang sudah baku (IEEE 802.3x), sehingga hampir disetiap perangkat yang dapat terhubung dalam konektivitas jaringan memiliki *interface* ini serta menggunakan sistem *Peer to Peer* (P2P), yang artinya pada jaringan *client-server* dikedua sisinya dapat saling bertukar *resource* tanpa memandang mana peran *client* maupun peran *server*. Pada jaringan Metro-E merupakan berbasis topologi jaringan *Wide Area Network* (WAN) dimana umumnya menggunakan kabel serat optik sebagai penghantarnya.



Gambar 3.1 Topologi Metro-E PT. Infomedia Nusantara

Tabel 3.1 Distribusi IP Address PT. Infomedia Nusantara

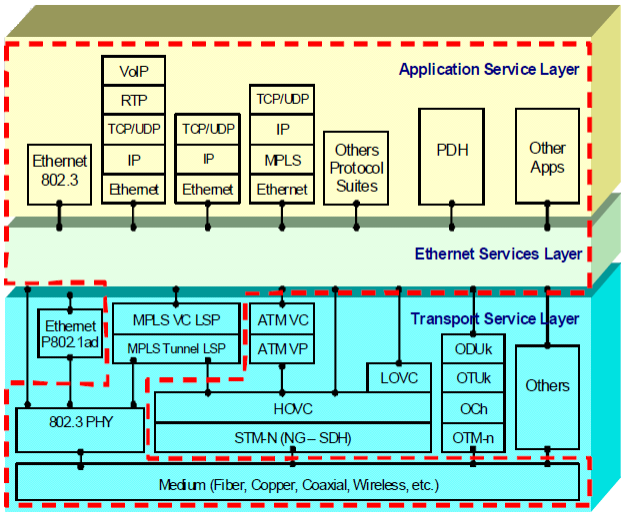
SITE	IP ROUTER			LINK BANDWIDTH			CLIENT
	Master	Main	Secondary	Master	Main	Secondary	
Jakarta	172.16.1.0/24	-	-	100 Mbps	-	-	-
Medan	-	192.168.11.0/24	192.168.12.0/24	-	10 Mbps	5 Mbps	172.181.65.0/24
Bandung	-	192.168.7.0/24	-	-	20 Mbps	10 Mbps	192.168.7.0/24
Surabaya	-	192.168.22.0/24	192.168.23.0/24	-	20 Mbps	10 Mbps	172.181.22.0/24
Makasar	-	192.168.89.0/24	-	-	10 Mbps	5 Mbps	192.168.89.0/24

Pada Gambar 3.1 merupakan jaringan Metro-E yang telah digunakan pada jaringan *client-server* PT. Infomedia Nusantara. Setiap *router* dimasing-masing *site* dihubungkan oleh Metro-E yang mempunyai *bandwidth* 20 Mbps untuk *link* utama

dan 10 Mbps untuk *link backup*. Jaringan Metro-E pada PT. Infomedia Nusantara digunakan untuk keperluan yang meliputi:

1. *Resource sharing*, seperti *sharing file* dan *sharing device*.
2. *Webserver*, seperti aplikasi-aplikasi web internal perusahaan.
3. *Webmail*, seperti aplikasi *email coorporate* perusahaan.
4. *Remote Management*, melalui port SSH dan *Virtual Network Computing* (VNC).

Arsitektur *Metro Ethernet Network* (MEN) yang digunakan oleh PT. Infomedia Nusantara telah distandarisasi oleh Telkom RDC mengadopsi model generik dan komposisi lapisan protokol infrastruktur MEN yang telah didefinisikan oleh *Metro Ethernet Forum* (MEF). Infrastruktur tersebut terbagi atas 3 bagian (*network layer*) yaitu: *application services layer*, *ethernet services layer* dan *transport service layer*.



Gambar 3.2 Lapisan Protokol Infrastruktur MEN

Setiap lapisan penyusun arsitektur memiliki protokol-protokol terkait Pada Gambar 3.4, yaitu:

1. *Ethernet Services Layer* (ETH layer), berfungsi untuk mengatur disekitar lingkungan dan bermacam-macam hal yang berurusan dengan *frame ethernet.*
2. *Transport Services Layer* (TRAN layer), berfungsi untuk mengatur konektivitas antar layer ETH dan layer ini bertugas untuk mengatur

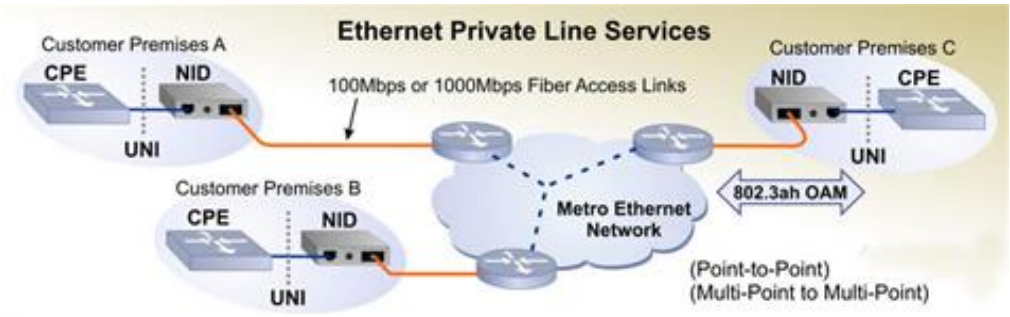
transmisi *frame ethernet* dari layer atasnya. Teknologi yang bisa digunakan untuk TRAN, yaitu: IEEE 802.3 PHY, IEEE 802.1 *bridged networks*, dan lain-lain.

3. *Application Services Layer* (APP layer), berfungsi untuk mendukung layanan aplikasi yang akan dibawa oleh frame ethernet dari MEN. Aplikasi disini bukanlah layer aplikasi OSI atau macam-macam protokol HTTP, melainkan layanan aplikasi yang dibawa oleh MEN yaitu: IP, E1, MPLS.

3.1.1.1 Ethernet Point-to-Point

Pada konsep jaringan *Ethernet Point-to-Point client-server* PT. Infomedia Nusantara menggunakan *Ethernet Private Line* (EPL) yang berbasis *port ethernet* pada layer 2. Lalu lintas data langsung diarahkan kepada *Time Division Multiplexing* (TDM). Keuntungan menggunakan EPL adalah:

1. Cakupan geografis yang luas.
2. Akses multiservice.
3. VLAN tagging yang memungkinkan menghubungkan beberapa sirkuit EPL.
4. Menjaga kualitas pelayanan jaringan yang lebih tinggi dengan biaya pemeliharaan yang rendah.
5. Menjaga nilai SLA dan MTTR.

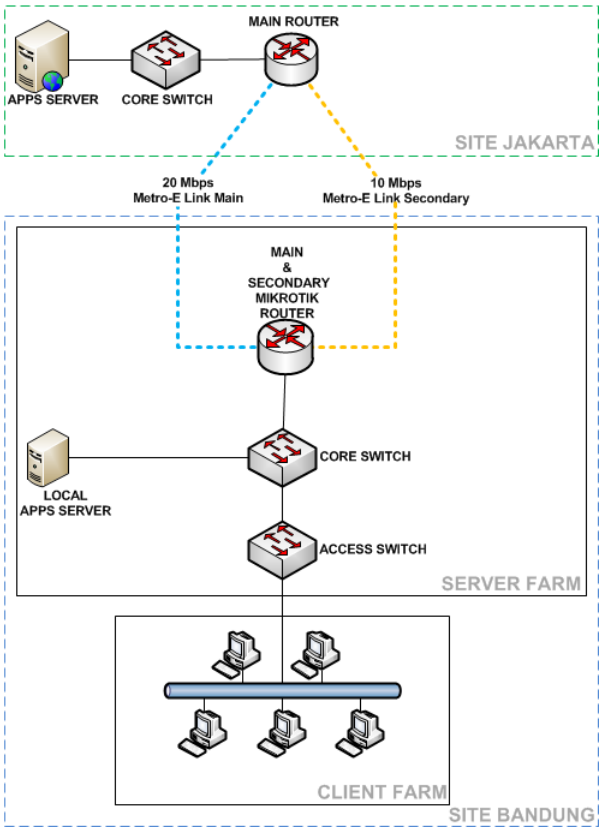


Gambar 3.3 Ethernet Private Line

3.2 Analisis Sistem Yang Telah Berjalan

PT. Infomedia Nusantara menerapkan jaringan utama *Peer to Peer* (P2P) Metro-E 20 Mbps dan jaringan *backup Peer to Peer* (P2P) Metro-E 10 Mbps yang menghubungkan antar *site*, dengan kondisi *web server* yang berada di kota Jakarta

dan *client* sebagai pengguna aplikasi yang berada di kota Bandung. Masalah terjadi ketika seringnya *link* utama mengalami kegagalan yang diharuskan melakukan perpindahan ke *link backup*. Saat ini kedua link tersebut melewati satu *router* yang sama, lalu pada saat terjadi kegagalan *link* dilakukan perpindahan dari *link* utama ke *link backup* secara *manual* yang memakan waktu *downtime* yang lama. Oleh karena itu, dibutuhkan suatu protokol redudansi yang dapat menjaga kondisi *link* selalu tersedia (reliabel) dan memperkecil waktu downtime ketika terjadi kegagalan link.



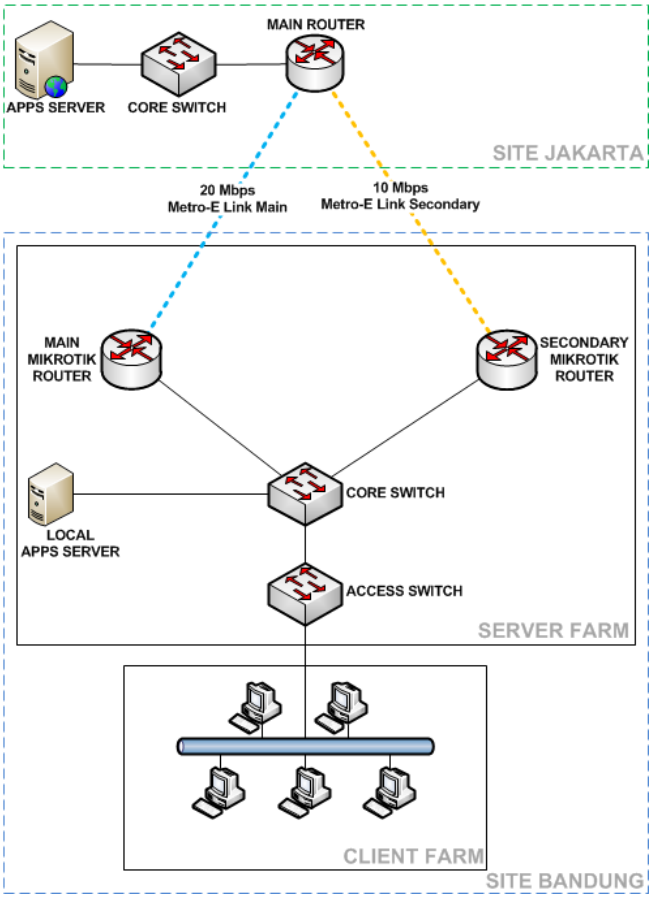
Gambar 3.4 Topologi Client-Server PT. Infomedia Nusantara

Pada Gambar 3.4 menunjukan kondisi awal dari topologi jaringan *client-server* PT. Infomedia Nusantara dimana terdapat dua *site* atau tempat yang berbeda dihubungkan oleh kedua jaringan Metro-E sebagai jalur utama dan jaringan *backup*. Ketika jalur utama mengalami kegagalan maka jalur cadangan yang akan mengambil alih serta kedua jalur tersebut melewati router yang sama.

3.2.1 Analisis Jaringan Redundansi

Ketersediaan jaringan komputer sangat penting untuk mencapai suatu tujuan tertentu. Oleh karena itu layanan jaringan harus tersedia 24 jam sehari untuk melayani mereka yang membutuhkan jaringan demi kepentingan bisnis. Kegagalan *link* masih menjadi salah satu kendala utama dalam mempertahankan ketersediaan jaringan komputer, hal tersebut dapat diatasi dengan menyediakan jaringan redundansi yang bertujuan untuk meningkatkan kualitas pelayanan jaringan. Konsep dasar dari jaringan redudansi adalah dengan menyediakan perangkat dan *link backup*. Ketika perangkat dan *link* utama mengalami kegagalan, perangkat dan *link backup* akan mengambil alih perannya.

PT. Infomedia Nusantara menggunakan 2 jalur link yang menghubungkan antar *site*, yaitu jaringan Metro-E 20 Mbps sebagai *link* utama dan jaringan Metro-E 10 Mbps sebagai *link backup*. Pada gambar 3.1 merupakan topologi jaringan *client-server* yang sedang berjalan di PT. Infomedia Nusantara dimana 2 jalur link yang menghubungkan antar *site* melewati *router* yang sama. Pada kondisi saat ini jika terjadi kegagalan pada *link* utama yang dikarenakan *force majeure* ataupun sedang terjadi *maintenance*, diharuskan untuk mengganti ke *link backup* secara *manual* agar dapat kembali normal.



Gambar 3.5 Topologi Client-Server PT. Infomedia Nusantara Menggunakan Protokol Redudansi VRRP

Pada Gambar 3.5 menunjukan kondisi pengembangan dari topologi jaringan *client-server* PT. Infomedia Nusantara dimana terdapat dua *site* atau tempat yang berbeda dihubungkan oleh jaringan Metro-E 20 Mbps sebagai jalur utama dan jaringan Metro-E 10 Mbps sebagai jalur cadangan. Dengan menambahkan satu router, maka protokol redudansi VRRP dapat berjalan dengan baik.

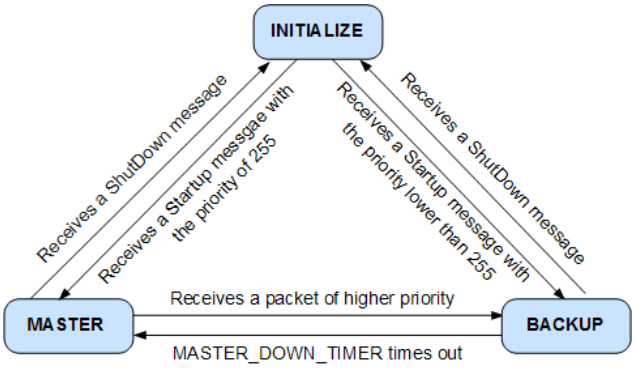
3.2.2 Analisis Protokol Redudansi VRRP

VRRP (Virtual Router Redundancy Protocol) adalah protokol redundansi *open source* yang artinya dapat digunakan diberbagai merk perangkat dan dirancang untuk meningkatkan ketersediaan pelayanan *default host gateway* pada *subnet* yang sama. *Virtual Router Redundancy Protocol* adalah solusi alternatif jaringan redudansi selain *Hot Standby Router Protocol* (HSRP) yang diakui oleh Cisco dan didefinisikan dalam standar IETF RFC 3768. Kedua teknologi serupa

dalam konsep, tapi tidak saling kompatibel. Keuntungan menggunakan VRRP adalah mendapatkan ketersediaan tinggi untuk *default path* tanpa memerlukan konfigurasi routing atau penemuan router protokol dinamis pada setiap *host*.

VRRP *router*, dikenal sebagai "kelompok redundansi", berbagi tanggung jawabnya untuk meneruskan paket seolah-olah mereka memiliki alamat IP yang sesuai dengan *default gateway* yang dikonfigurasi pada *host*. Pada setiap saat, salah satu *router* VRRP bertindak sebagai *master* dan *router* lainnya VRRP bertindak sebagai *backup*. Jika *router* utama gagal, *router* cadangan menjadi master. Dengan cara ini, redundansi *router* selalu tersedia, sehingga lalu lintas di jaringan akan dialihkan tanpa bergantung pada satu *router*.

Router fisik yang saat *forwarding* data diberi *virtual router* yang disebut *router* utama. Jika jaringan utama *down*, *router* VRRP yang tersisa akan menjadi *router* utama. *Router* utama akan meneruskan paket atas nama pemilik dengan mengambil alih alamat MAC *virtual* yang digunakan oleh pemilik. *Router* utama memiliki prioritas 255 dan router cadangan dapat memiliki prioritas antara 1-254. Sebuah *virtual router* harus menggunakan *MAC Address* 00-00-5E-00-01-XX. Byte terakhir dari alamat (XX) adalah *Virtual Router Identifier* (VRID), yang berbeda untuk setiap *virtual router* dalam jaringan. Alamat ini digunakan hanya oleh satu *router* fisik pada satu waktu dan satu-satunya cara *router* fisik lainnya mengenali router utama adalah dengan *virtual router*.



Gambar 3.6 VRRP State

Pada Gambar 3.6 merupakan diagram cara kerja dari VRRP yang terdiri dari 3 *state*, yaitu *Initialize State*, *Backup State*, dan *Master State*. Berikut penjelasannya:

Tabel 3.2 Deskripsi VRRP State

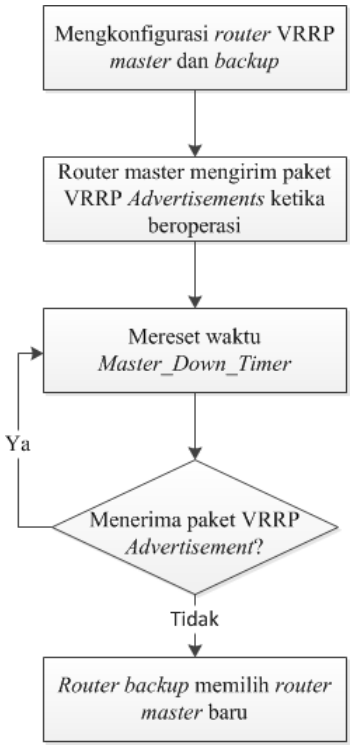
State	Deskripsi
Initialize	Jika VRRP tidak tersedia, perangkat *router* di *Initialize State* tidak bisa meneruskan proses paket VRRP. Ketika perangkat *router* berfungsi atau mendeteksi kesalahan, masuk pada fase *Initialize State.*
Master	Pada perangkat *router* yang menggunakan VRRP ketika memasuki *Master State,* akan melakukan operasi berikut: 1. Mengirim paket VRRP Advertisement disetiap interval waktu. 2. Menggunakan *virtual MAC address* untuk merespon paket ARP yang ditujukan kepada *virtual IP Address.* 3. Meneruskan paket IP yang ditujukan ke *virtual MAC Address.* 4. Memproses paket IP yang ditujukan untuk *virtual IP Address.*
Backup	Pada perangkat router yang menggunakan VRRP ketika memasuki *Backup State*, akan melakukan operasi berikut: 1. Menerima paket VRRP *Advertisement* dari *Router Master* dan menentukan apakah *Router Master* bekerja dengan baik. 2. Tidak akan merespon permintaan paket ARP yang ditujukan untuk alamat IP *virtual.* 3. Menyingkirkan paket IP yang ditujukan ke *virtual MAC address* dan *virtual* IP *address* 4. Menyingkirkan paket yang membawa prioritas yang lebih rendah dari perangkat dan tidak akan mereset waktu Master_Down_Timer. Jika kondisi Master_Down_ Timer direset akan membandingkan alamat IP yang diterima dengan membawa prioritas yang sama dengan perangkat

3.2.2.1 Mekanisme VRRP

Pada protokol redudansi VRRP memungkinkan dua atau lebih *router* dapat secara automatis memilih satu *router* untuk bertindak sebagai *master* dan satu atau lebih *router* lain bertindak sebagai *router backup* untuk melayani *router master*. Pada implementasinya protokol redudansi VRRP tidak dapat menentukan sendiri *router master* dan *router backup*, oleh karena itu pada Gambar 3.7 dijelaskan bahwa hal pertama yang dilakukan adalah dengan mengkonfigurasi dan menentukan secara manual *router* mana yang akan bertindak sebagai *master* dan *backup*. Setelah melakukan konfigurasi lalu yang dilakukan oleh *router master* adalah mengirimkan

paket *Advertisements* kepada *router* lain selama *router* lain berfungsi normal. Pada dasarnya *router master* akan menyebarkan alamat IPnya sendiri bahwa alamat IP tersebut adalah miliknya. Hal tersebut bertujuan untuk menginformasikan kepada *router* yang lain bahwa *router master* masih normal dan belum mengalami kegagalan.

Ketika *router backup* menerima paket *Advertisement* dari *router master*, maka waktu dari *master_down_timer* akan reset dan menunggu paket *Advertisement* selanjutnya. Jika paket *Advertisement* tidak diterima oleh *router backup* sebelum waktu *master_down_timer* berakhir, maka *router backup* akan memilih *router master* baru yang kemudian akan bertanggung jawab untuk merespon ARP *requests, fowarding packet*, dan lain lain yang berhubungan dengan satu atau lebih alamat *virtual* IP yang terkait dengan *router master* sebelumnya.



Gambar 3.7 VRRP Flowchart

3.3 Analisis Masalah

Setelah melakukan analisa terlebih dahulu terhadap jaringan redudansi yang berjalan di PT. Infomedia Nusantara ditemui kendala. Waktu *downtime* yang sangat lama menjadi kendala utama dan menyebabkan *availability* pelayanan jaringan menjadi berkurang. Faktor yang menyebabkan hal kendala tersebut dikarenakan

belum adanya otomatisasi fungsi dari jaringan redudansi ketika jaringan utama mengalami kegagalan.

Analisa dilakukan dengan menghitung nilai *downtime* dengan parameter perhitungan waktu *downtime*, yaitu *Time Finish* (Waktu Selesai Gangguan) - *Time Start* (Waktu Mulai gangguan). Lalu menghitung nilai *Mean Time Between Failures* (MTBF):

$$MTBF = \frac{\Sigma(Operation\ Availability - Downtime)}{Number\ of\ Repairs}$$

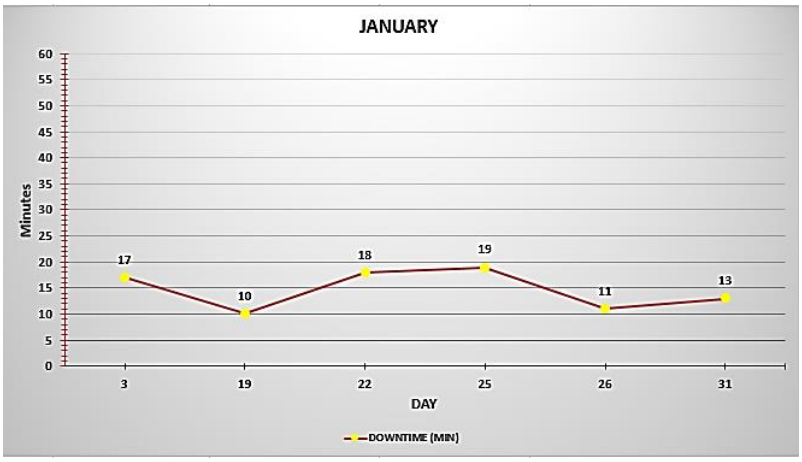
Setelah nilai MTBF didapat, maka yang selanjutnya dilakukan adalah menghitung nilai *Mean Time To Repair* (MTTR):

$$MTTR = \frac{Total\ Maintenance\ Time}{Number\ of\ Repairs}$$

Dengan hasil dari perhitungan MTBF dan MTTR, maka perhitungan nilai *availability* sistem dapat dilakukan dengan menggunakan penjumlahan sebagai berikut:

$$Availability = \frac{MTBF}{MTBF + MTTR} * 100$$

Berikut ini adalah rekap data *downtime* link network yang terjadi selama periode tahun 2015 di PT. Infomedia Nusantara yang bersumber dari *logbook*. Data disajikan dengan bentuk *chart* perbulan dengan parameter analisa MTBF, MTTR dan *availability*:

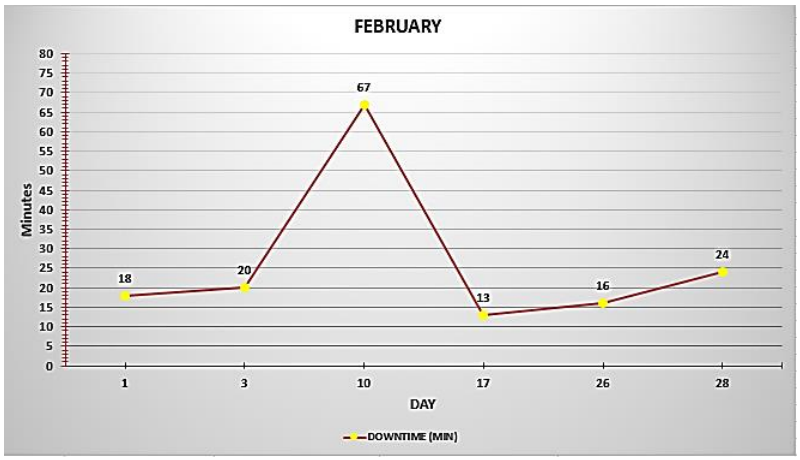


Gambar 3.8 Grafik Downtime Bulan Januari

Tabel 3.3 Analisa Availability Bulan Januari

Date	Time Start	Time Finish	Downtime (min)
3-Jan	10:18 AM	10:35 AM	17
10-Jan	1:21 PM	1:40 PM	19
19-Jan	9:14 AM	9:24 AM	10
22-Jan	3:56 PM	4:14 PM	18
25-Jan	7:55 AM	8:14 AM	19
26-Jan	4:17 PM	4:28 PM	11
31-Jan	8:19 AM	8:32 AM	13
Total Downtime (min)			**107**

Operation Availability (min/month)	**43.829**
Frequence	**7**
MTBF (min)	**6246**
MTTR (min)	**15**
AVAILABILITY	**99.76%**



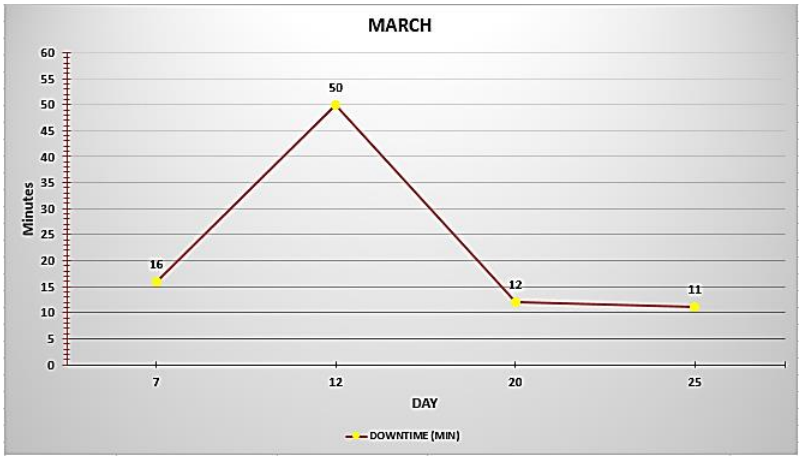
Gambar 3.9 Grafik Downtime Bulan Februari

Tabel 3.4 Analisa Availability Bulan Februari

Date	Time Start	Time Finish	Downtime (min)
1-Feb	8:09 AM	8:27 AM	18
3-Feb	3:10 PM	3:30 PM	20
10-Feb	9:10 AM	10:17 AM	67
17-Feb	4:18 PM	4:31 PM	13
26-Feb	11:47 AM	12:03 PM	16
28-Feb	2:15 PM	2:39 PM	24

Total Downtime (min)	**158**

Operation Availability (min/month)	**43.829**
Frequence	**6**
MTBF (min)	**7279**
MTTR (min)	**26**
AVAILABILITY	**99.64%**

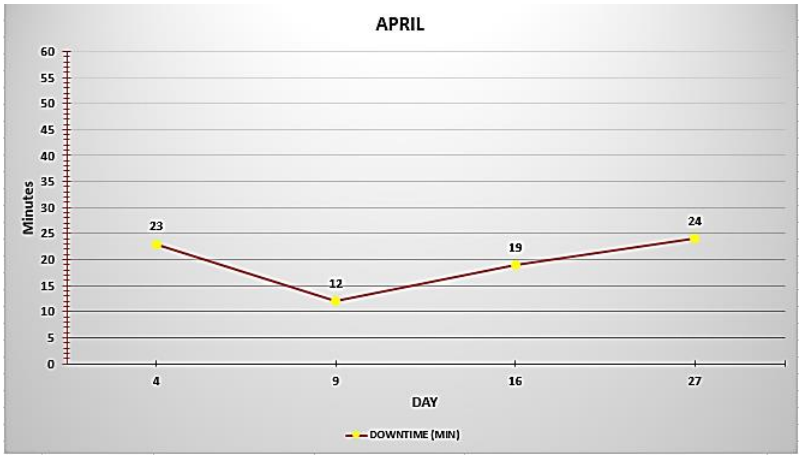


Gambar 3.10 Grafik Downtime Bulan Maret

Tabel 3.5 Analisa Availability Bulan Maret

Date	Time Start	Time Finish	Downtime (min)
7-Mar	9:56 AM	10:12 AM	16
12-Mar	11:17 AM	12:07 PM	50
20-Mar	2:47 PM	2:59 PM	12
25-Mar	12:25 PM	12:36 PM	11
Total Downtime (min)			**89**

Operation Availability (min/month)	**43.829**
Frequence	**4**
MTBF (min)	**10935**
MTTR (min)	**22**
AVAILABILITY	**99.80%**

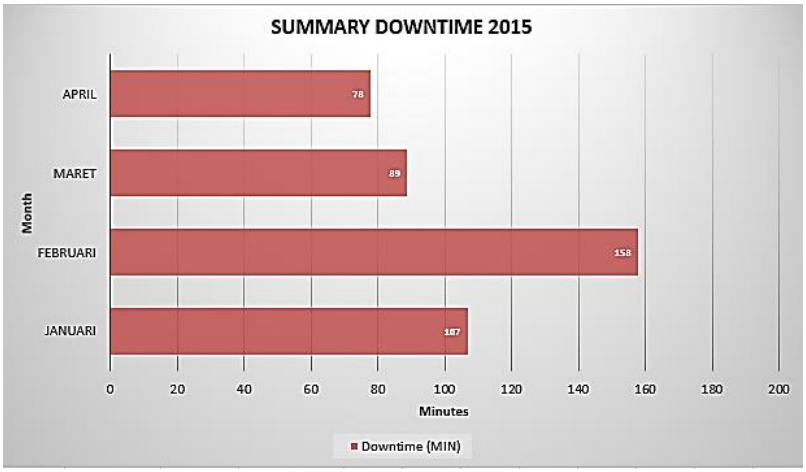


Gambar 3.11 Grafik Downtime Bulan April

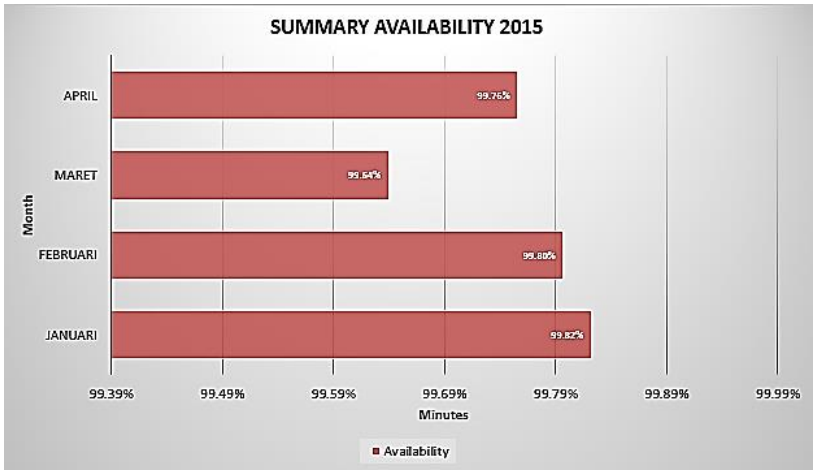
Tabel 3.6 Analisa Availability Bulan April

Date	Time Start	Time Finish	Downtime (min)
4-Apr	10:12 AM	10:35 AM	23
9-Apr	2:33 PM	2:45 PM	12
16-Apr	9:56 AM	10:15 AM	19
27-Apr	4:47 PM	5:11 PM	24
Total Downtime (min)			**78**

Operation Availability (min/month)	**43.829**
Frequence	**4**
MTBF (min)	**10938**
MTTR (min)	**20**
AVAILABILITY	**99.82%**



Gambar 3.12 Grafik Total Downtime Tahun 2015



Gambar 3.13 Grafik Summary Availability Tahun 2015

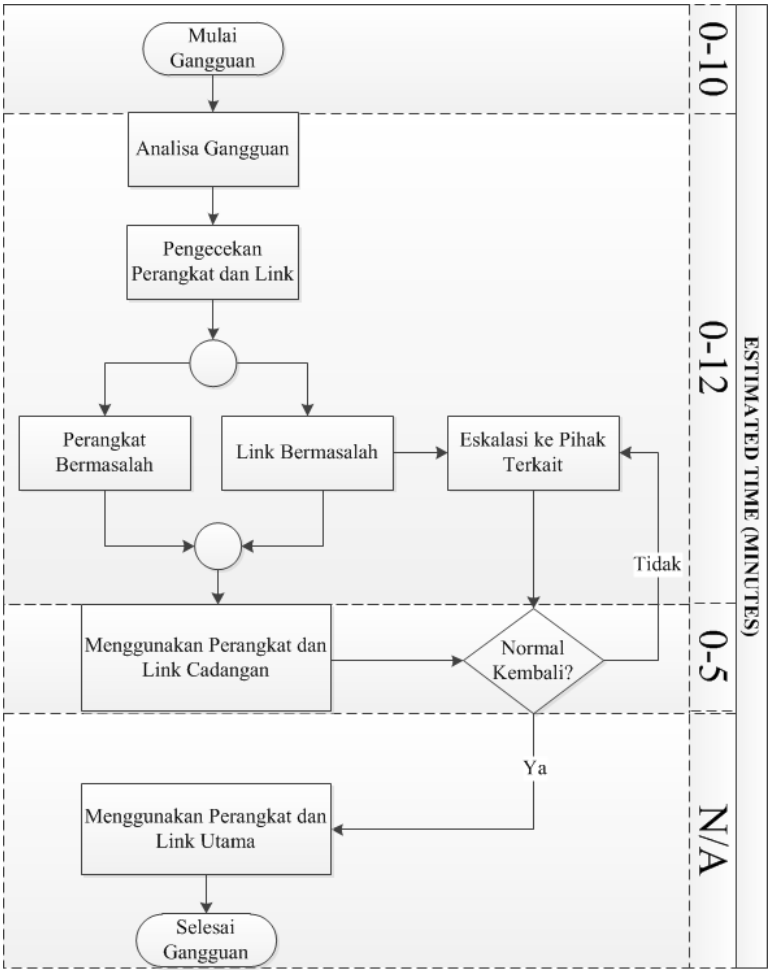
Pada gambar diatas dijelaskan grafik jumlah waktu *downtime* yang meliputi jaringan Metro-E mengalami *flicker link* (terputusnya *link* secara tiba-tiba) maupun adanya proses *maintenance* oleh provider yang digunakan.

3.4 Analisis Downtime

Pada analisis downtime akan dijelaskan setiap elemen pokok dari permasalahan serta bagaimana suatu gangguan dapat menghabiskan waktu dari mulai gangguan sampai dengan berakhirnya suatu gangguan dapat diatasi.

Tabel 3.7 Contoh Rekap Data Logbook Downtime

DAY	START TIME	RESOLVED TIME	DOWNTIME (MIN)	PROBLEM	IDENTIFICATION	ANALYSIS & SOLVE
1						
2						
3	10:18 AM	10:35 AM	17	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
4						
5						
6						
7						
8						
9						
10	01:21 PM	01:40 PM	19	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
11						
12						
13						
14						
15						
16						
17						
18						
19	09:14 AM	09:24 AM	10	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
20						
21						
22	03:56 PM	04:14 PM	18	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
23						
24						
25	07:55 AM	08:14 AM	19	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
26	04:17 PM	04:28 PM	11	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
27						
28						
29						
30						
31	08:19 AM	08:32 AM	13	Aplikasi tidak dapat diakses	Flicker link main Metro-E	Koordinasi dengan C4 Telkom dan switch link backup
TOTAL DOWNTIME			107			



Gambar 3.14 Penanganan Gangguan Eksisting

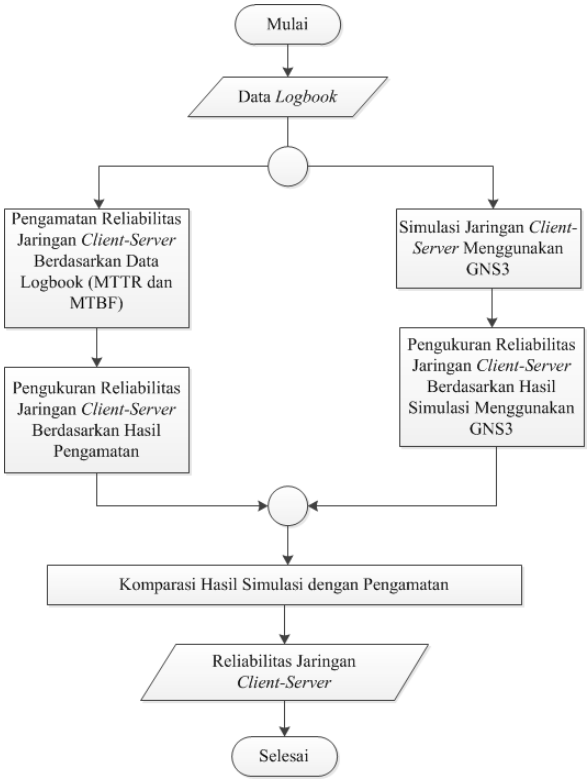
Pada Gambar 3.14 menunjukan bagaimana dari setiap proses yang dilakukan ketika terjadi gangguan pada *link* maupun perangkat diukur berdasarkan waktu (menit) yang mengakibatkan terganggunya kegiatan operasional PT. Infomedia Nusantara. Berikut penjelasan dari Gambar 3.14:

1. Mulai gangguan: Pada bagian ini merupakan awal dari kegagalan fungsi dari perangkat ataupun *link*.
2. Analisa Gangguan: Pada bagian ini dilakukan proses identifikasi bagaimana suatu kegagalan dapat terjadi.
3. Pengecekan perangkat dan *link*: Pada bagian ini dilakukan pengecekan dari sisi perangkat jaringan maupun *link* yang bermasalah.

4. Perangkat bermasalah: Pada bagian ini suatu perangkat jaringan mengalami kegagalan sehingga tidak berfungsi ataupun tidak stabil.
5. *Link* bermasalah: Pada bagian ini *link* mengalami kendala, baik mengalami *flicker link* maupun ada *maintenance* dari vendor.
6. Eskalasi ke pihak terkait: Pada bagian ini merupakan menginformasikan kepada pihak vendor yang bertanggung jawab terhadap jaringan maupun perangkat.
7. Menggunakan perangkat dan *link* cadangan: Pada bagian ini dilakukan penggantian perangkat ataupun *link* yang berkendala ke cadangan agar dapat berfungsi secara normal.
8. Menggunakan perangkat dan *link* utama: Pada bagian ini dilakukan penggantian perangkat dan *link* jika kondisi keduanya sudah berjalan normal.
9. Selesai Gangguan: Pada bagian ini merupakan akhir dari kegagalan fungsi dari perangkat ataupun *link*.

3.5 Analisis Pengukuran Reliabilitas

Pada analisis pengukuran reliabilitas jaringan *client-server* meliputi komponen pengambilan data *logbook* yang berisi data tentang bagaimana dan kapan suatu kejadian terputusnya *link.* Pengamatan diperlukan untuk mengetahui sejauh mana *availability* jaringan *client-server* dapat diukur melalui perhitungan *Mean Time To Repair* (MTTR) dan *Mean Time Between Failure* (MTBF), karena untuk dapat mengukur nilai *reliability* suatu jaringan diperlukan proses perhitungan *availability* dan *downtime*. Selanjutnya pengembangan sistem akan dilakukan dengan bantuan simulator GNS3 dan akan didapatkan hasil yang akan dibandingkan dengan sistem yang sudah berjalan.



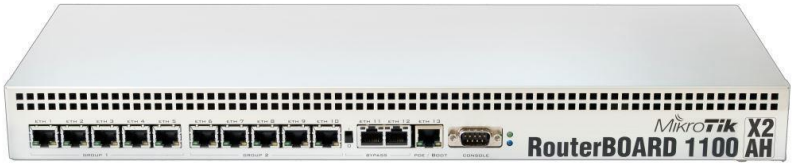
Gambar 3.15 Diagram Alir Pengukuran Reliabilitas

3.6 Analisis Kebutuhan Infrastruktur

Pada tahap ini dilakukan persiapan perangkat apa saja yang dibutuhkan ketika akan mengembangkan suatu sistem, agar dalam proses uji coba dan simulasi berjalan sesuai keinginan.

Tabel 3.8 Spesifikasi Perangkat Keras PC

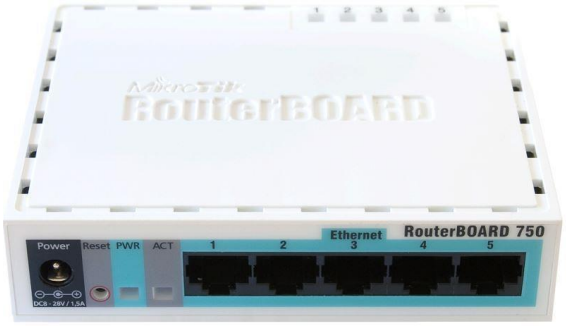
Hardware	Server	Client
Processor	Intel® Xeon® E5-2609 v2 2.5GHz	Core i3 2348M 2.3Ghz
Memory	16 Gb	2 Gb
Harddisk	3 Tb	500 Gb
Sistem Operasi	Windows Server 2008	Windows XP SP3



Gambar 3.16 Mikrotik RB 1100AHX2

Tabel 3.9 Spesifikasi Mikrotik RB 1100AHX2

CPU	PowerPC P2020 dual core 1066MHz network CPU with IPsec accelerator
Memory	SODIMM DDR Slot, 2GB installed (RouterOS will use only up to 1.5GB)
Boot loader	RouterBOOT, 1Mbit Flash chip
Data storage	Onboard NAND memory chip, one microSD card slot
Ethernet	Thirteen 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
Ethernet	Includes switch to enable Ethernet bypass mode in two ports
miniPCI	None
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch, beeper, voltage and temperature sensors
Power options	Built-in power supply (IEC C14 standard connector 110/220V), PoE (12-24V on port 13)
Fan	Built in fans, and Fan headers
Dimensions	1U case: 44 x 176 x 442 mm, 1275g. Board only: 365g
Operating System	MikroTik RouterOS, Level 6 license



Gambar 3.17 Mikrotik RB 750

Tabel 3.10 Spesifikasi Mikrotik RB 750

CPU nominal frequency	400 MHz
CPU core count	1
Size of RAM	32 MB
Architecture	MIPS-BE
10/100 Ethernet ports	5
Power Jack	1
Supported input voltage	10 V - 28 V
PoE in	Yes

Dimensions	113x89x28mm. Weight without packaging and cables: 129g
Operating System	RouterOS
Operating temperature range	-40℃ to +55℃
License level	4
CPU	AR7241-AH1A
Max Power consumption	2.5W
Serial port	None

3.6.1 Analisis Kebutuhan Perangkat Lunak

Berikut ini adalah kebutuhan perangkat lunak yang digunakan dalam pengambangan sistem.

Tabel 3.11 Spesifikasi Perangkat lunak

Nama Perangkat	Perangkat Lunak	Keterangan
Router OS	v5.4	Router OS versi 5.4
	v6.10	Router OS versi 6.10
Server	AppServ	Digunakan untuk akses aplikasi
Client	Wireshark	Digunakan sebagai capture packet data

3.6.2 Analisis Kebutuhan Simulasi

Pada proses pengembangan sistem segala komponen harus disiapkan termasuk suatu simulasi untuk menunjukan konsep dasar sistem yang akan dibangun. Berikut ini analisis kebutuhan untuk simulasi:

Tabel 3.12 Spesifikasi Kebutuhan Simulasi

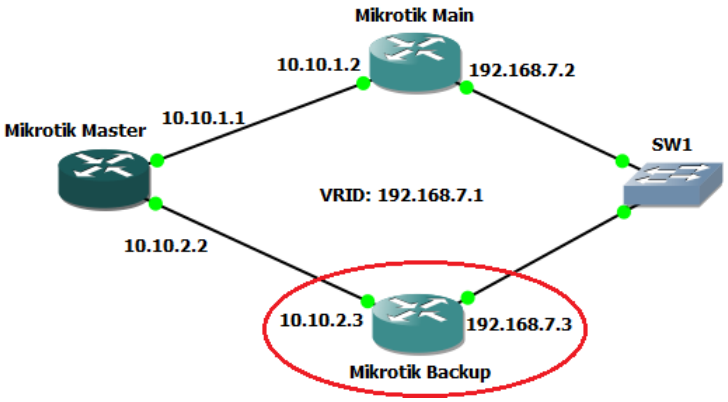
Hardware	Laptop	Virtual Sever	Virtual Client 1	Virtual Client 2	Virtual Client 3
Processor	AMD A8-4500 2,8 GHz				
Memory	4 Gb	1 Gb	192 Mb		
Hardisk	750 Gb	30 Gb	2 Gb		
Sistem Operasi	Windows 7 Ultimate	Windows Server 2008	Windows XP SP 3		

Tabel 3.13 Spesifikasi Kebutuhan Simulasi 2

Hardware	Router Master	Router Main	Router Secondary	Switch 1	Switch 2
Memory	128 Mb			-	-
Hardisk	2 Gb			-	-
Interface	3	2		3	2
Sistem Operasi	Mikrotik OS			-	-

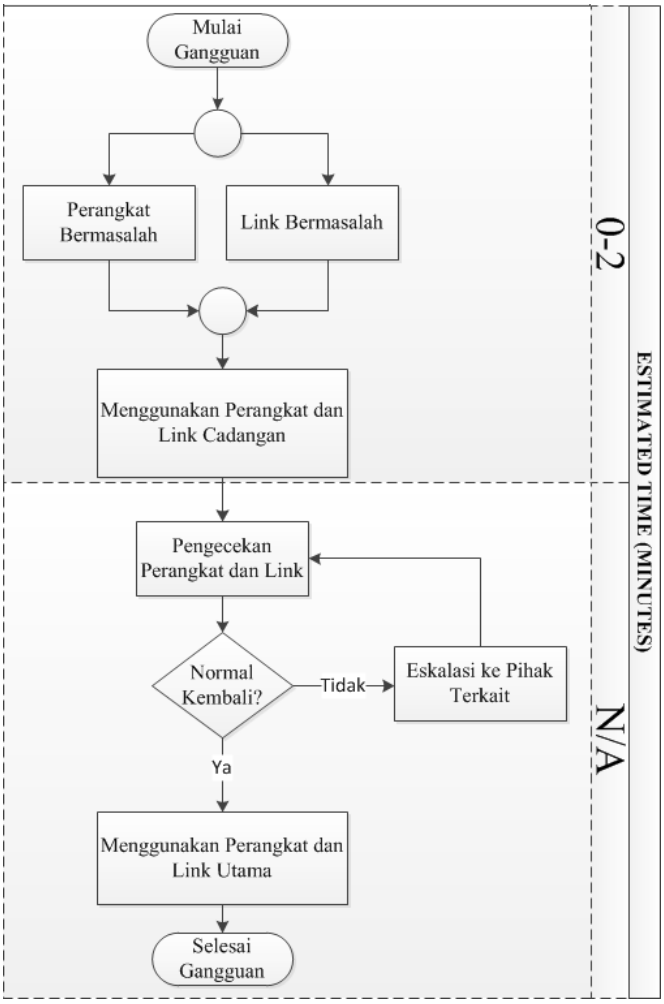
3.7 Perancangan Sistem

Pada perancangan sistem akan dijelaskan mengenai perancangan simulasi, perancangan arsitektur pengujian dan beberapa perancangan lainnya yang berhubungan dengan pengembangan sistem.



Gambar 3.18 Infrastruktur Jaringan *Client-Server* dengan Protokol Redudansi VRRP

Perancangan pengembangan sistem dan simulasi dilakukan dengan menambahkan satu perangkat router cadangan ketika *client* akan mengakses ke *server* dengan implementasi protokol redudansi yaitu *Virtual Router Redudancy Protocol* (VRRP).



Gambar 3.19 Penanganan Gangguan dengan Protokol Redudansi VRRP

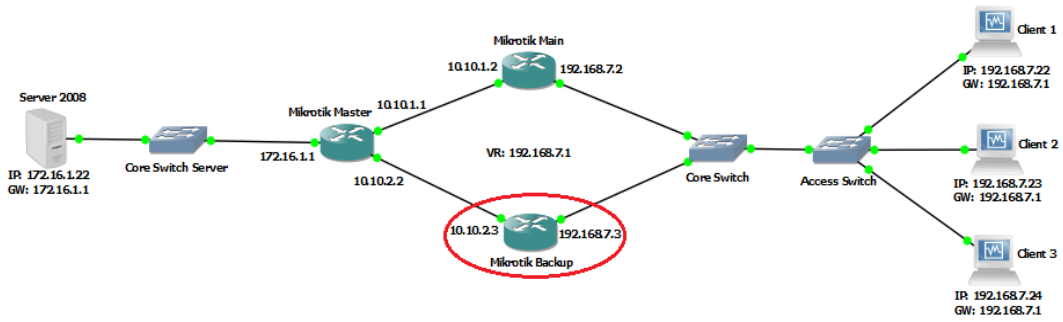
Pada Gambar 3.19 merupakan alur ketika terjadi kegagalan *link* atau perangkat yang diatasi oleh protokol redudansi VRRP.

3.7.1 Tujuan Perancangan Sistem

Perancangan sistem merupakan suatu proses yang menentukan bagaimana suatu sistem dapat berjalan dengan baik. Pada tahapan ini memberikan gambaran arsitektur dari infrastruktur yang digunakan untuk membangun protokol redudansi VRRP pada jaringan *client-server.*

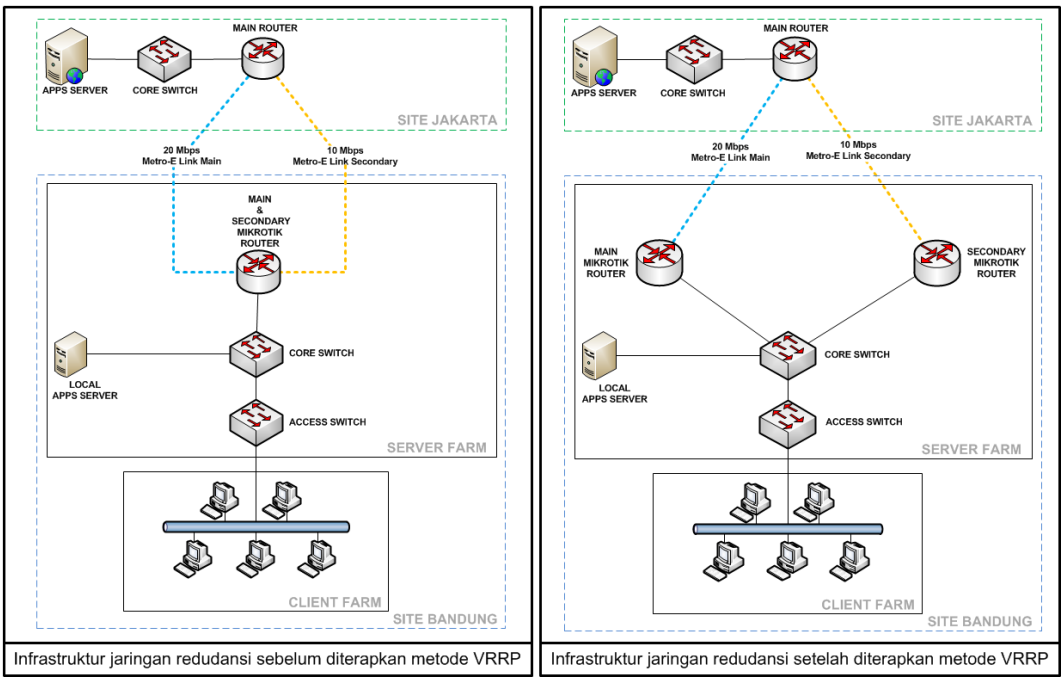
3.7.2 Perancangan Arsitektur

Perancangan arsitektur disimulasikan bertujuan agar memberikan gambaran arsitektur dari infrastruktur yang digunakan dalam membangun protokol redudansi VRRP pada jaringan *client-server*.



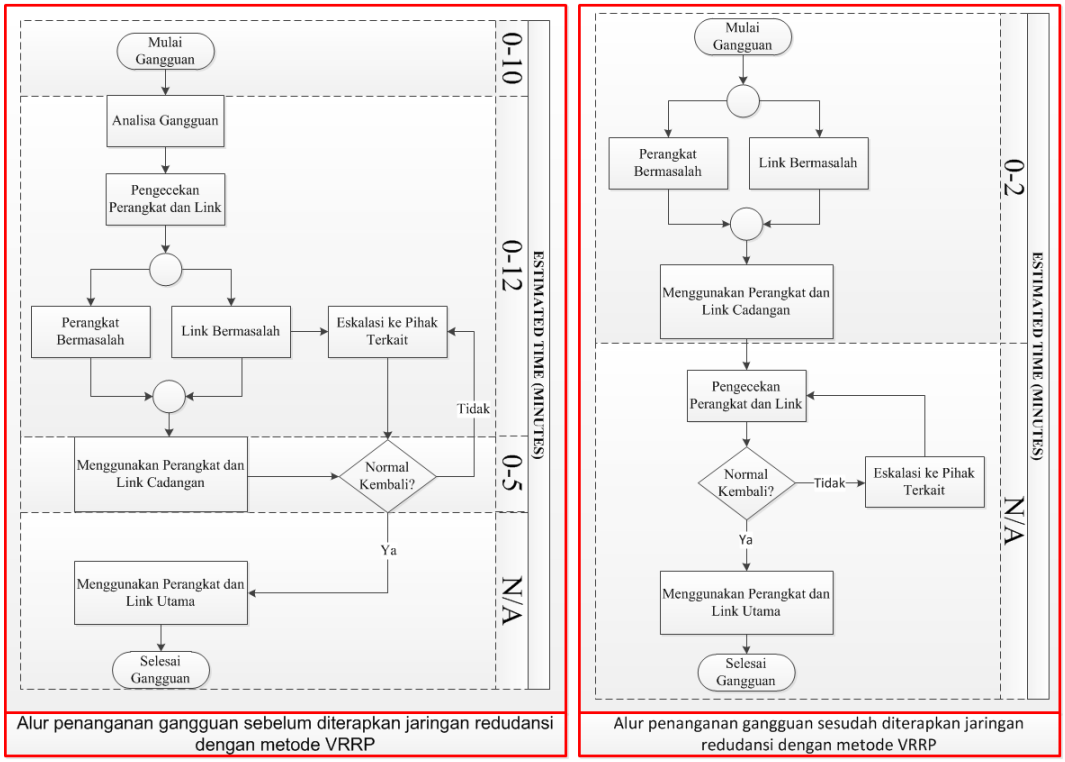
Gambar 3.20 Arsitektur Simulasi Jaringan Client-Server dengan Protokol Redudansi VRRP

Pada Gambar 3.20 merupakan Arsitektur Jaringan Client-Server dengan Protokol Redudansi VRRP, dimana dalam kondisi normal *client* yang memiliki satu IP segmen jaringan yang sama melakukan akses terhadap *server* melewati *switch* 1 lalu mengarah ke Mikrotik *Main* menggunakan OSPF *routing*, dilanjutkan ke Mikrotik *Master*, *Switch* 2 dan akhirnya sampai ke *Server*. Pada kondisi dimana Jaringan utama atau Mikrotik *Main* mengalami kegagalan, dengan cepat jaringan cadangan atau Mikrotik *Backup* akan mengambil alih.



Gambar 3.21 Perbandingan Infrastruktur

Pada Gambar 3.21 menunjukan mengenai perbandingan infrastruktur sebelum dan setelah penerapan protokol jaringan redudansi VRRP pada PT. Infomedia Nusantara.



Gambar 3.22 Perbandingan Alur Penanganan Ketika Terjadi Gangguan

Pada Gambar 3.22 dijelaskan mengenai perbedaan alur penanganan ketika terjadi gangguan sebelum diterapkan jaringan redudansi dengan metode VRRP dan sesudah diterapkannya jaringan redudansi dengan metode VRRP.