BAB II
LANDASAN TEORI

2.1 Router

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing.* Proses *routing* terjadi pada lapisan ketiga (lapisan jaringan seperti internet protocol) dari stack protocol tujuh-lapis OSI.

Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa subnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda atau berbeda arsitektur jaringan. Router umumnya dipakai untuk jaringan berbasis teknologi protokol TCP/IP, router jenis ini dinamakan IP Router. Internet merupakan contoh utama dari jaringan yang memiliki IP Router.

Umumnya router ada dua jenis, yaitu router statis dan router dinamis,
Router statis atau static router merupakan router yang memiliki tabel routing statis yang disetting dengan cara manual oleh para administrator jaringan. Sedangkan router dinamis atau rynamic router merupakan router yang memiliki dan membuat tabel routing dinamis dengan membaca lalu lintas jaringan dan juga dengan saling berhubungan dengan router lainnya.*Redundant Router* adalah pergantian kerja router master ke router bakcup dikarenakan router master terjadi kegagalan koneksi atau down.

Fungsi Router :

- Membaca alamat logika / ip address source & destination untuk menentukan routing dari suatu LAN ke LAN lainnya.
- Menyimpan routing table untuk menentukan rute terbaik antara LAN ke WAN.
- Perangkat di layer 3 OSI Layer.
- Bisa berupa "box" atau sebuah OS yang menjalankan sebuah daemon routing. Interfaces Ethernet, Serial, ISDN BRI.

2.2 Routing

Routing adalah proses untuk memilih jalur (path) yang harus dilalui oleh paket. Jalur yang baik tergantung pada beban jaringan, panjang datagram, type of service requested dan pola trafik. Pada umumnya skema routing hanya mempertimbangkan jalur terpendek *(the shortest path).*

Terdapat 2 bentuk routing, yaitu:

a. Direct Routing (direct delivery); paket dikirimkan dari satu mesin ke mesin lain secara langsung (host berada pada jaringan fisik yang sama) sehingga tidak perlu melalui mesin lain atau gateway.

b. Indirect Routing (indirect delivery); paket dikirimkan dari suatu mesin ke mesin yang lain yang tidak terhubung langsung (berbeda jaringan) sehingga paket akan melewati satu atau lebih gateway atau network yang lain sebelum sampai ke mesin yang dituju.

   Router merekomendasikan tentang jalur yang digunakan untuk melewatkan paket berdasarkan informasi yang terdapat pada Tabel Routing.

   Informasi yang terdapat pada tabel routing dapat diperoleh secara static routing melalui perantara administrator dengan cara mengisi tabel routing secara manual ataupun secara dynamic routing menggunakan protokol routing, dimana setiap router yang berhubungan akan saling bertukar informasi routing agar dapat mengetahui alamat tujuan dan memelihara tabel routing.

Tabel Routing pada umumnya berisi informasi tentang:

a. Alamat Network Tujuan

b. Interface Router yang terdekat dengan network tujuan

c. Metric, yaitu sebuah nilai yang menunjukkan jarak untuk mencapai network tujuan. Metric tesebut menggunakan teknik berdasarkan jumlah *lompatan (Hop Count).*

2.2.1 Protokol Routing

John Gage, chief researcher dari Sun Microsystems (1984:6) mengatakan routing protocol menjelaskan bagaimana router yang ada saling berkomunikasi satu dengan yang lain , dan digunakan untuk memelihara / mengupdate isi dari routing table .

Macam – macam Routing :

a. Static Routing Static

Routing ini merupakan cara paling simple untuk mengisi routing table yang ada di router , tapi dengan menggunakan static routing ini biasa nya di gunakan pada jaringan – jaringan yang kecil di mana hanya ada beberapa ip yang harus di masukan ke dalam routing table .

b. Dynamic Routing

Dynamic Routing adalah fungsi dari routing protocol yang saling berkomunikasi untuk melakukan update pada routing table , berbeda dengan static routing di mana admin harus secara manual memasukan routing table , dengan manggunakan dynamic routing ini admin tidak perlu untuk mengupdate jika terjadi perubahan dalam routing table , karena dalam dynamic routing ini dapat melakukan periodic update . Oleh sebab itu dynamic routing ini biasa di gunakan untuk jaringan yang kompleks .

Terdapat dua macam algoritma dalam Dynamic Routing :

• Distance Vector

Algoritma Distance Vector routing table di update secara periodic, sehingga router mendapatkan informasi dari router lain dan dilakukan terus menerus sampai semua router mendapatkan routing table yang baru, sehingga 16 jika terjadi perubahan pada jaringan router – router yang ada dalam *Autonomous System* yang sama akan mendapat routing table yang baru. Algoritma ini sering di sebut Bellman – Ford.

• Link-State

Algoritma Link-State biasa di sebut dengan *Algoritma Dijkstra* atau *Algoritman Shortest Path Firs* (SPF) , memiliki perbedaan dengan *Distance Vector* di mana *Link-State* memiliki informasi yang lebih spesifik dan memiliki informasi jarak antar router yang ada . Namun dalam penggunaan Link-State ini

membutuhkan resource yang cukup banyak , karena memilik informasi yang spesifik untuk di olah makan membutuhkan processor yang cepat , memory yang besar , serta bandwith yang lebar untuk mengaksesnya.
Yang termasuk Dynamic Routing adalah :

► RIP (Routing Information Protocol)

RIP adalah routing protocol dynamic yang menggunakan algoritma distance vector , di mana RIP menggunakan protocol UDP untuk mengirimkan informasi routing atar router . Protocol RIP ini menggunakan perhitungan Hop-Count sebagai routing metric

► IGRP *(Interior Gateway Routing Protocol)*

IGRP adalah routing protocol yang diciptakan oleh perusahaan Cisco untuk menutupi kekurangan dari RIP , di mana dalam protocol IGRP ini menggunakan *Autonomous System* (AS) yang dapat menentukan routing berdasarkan system interior atau exterior . *Administrative Distance* untuk IGRP adalah 100.

► EIGRP *(Enhanced Interior Gateway Routing Protocol)*

EIGRP adalah routing protocol yang hanya bisa di gunakan pada device Cisco atau yang biasa di sebut sebagai proprietary protocol pada cisco. Dimana EIGRP ini merupakan pengembangan dari protocol IGRP , dan EIGRP menggunakan *Diffusing Update Algorithm* (DUAL) dengan bertukar informasi "*Hello Packet*" untuk memastikan keberadaan router yang ada di sekitar nya .
EIGRP memilik tiga table dalam menyimpan informasi, yaitu :
o Neighbor Table

Neighbor Table merupakan table yang paling penting di atara table – table yang lain nya di mana di dalam neighbor table ini akan menyimpan list tentang router – router tetangga nya dimana setiap ada device baru yang akan di pasang , address dan interface akan langsung di masukan ke dalam table ini .

o Topology Table

Table ini ini di buat untuk memenuhi kebutuhan dari routing table dalam satu *Autonomous System* (AS) yang sama.

o Routing Table

Dalam routing table ini menyimpan rute terbaik yang akan di lalui untuk sampai ke tujuan , di mana informasi tersebut di ambil dari toplogy table .

► OSPF *(Open Shortest Path First)*

OSPF merupakan routing protocol yang hanya dapat bekerja di dalam jaringan internal suatu organisasi atau perusahaan tertentu . Selain itu OSPF merupakan protocol yang dapat di gunakan di perangkat manapun yang compatible dengan protocol ini . OSPF merupakan routing protocol yang menggunakan konsep hirarki, yang arti nya OSPF membagi – bagi jaringan menjadi beberapa tingkatan.

► BGP *(Border Gateway Protocol)*

BGP adalah sebuah system antar *Autonomous Routing Protocol* , pada umum nya BGP ini digunakan untuk pertukaran informasi routing untuk internet dan merupakan protocol yang digunakan antar penyedia layanan internet (ISP).

2.3 System Operasi

System operasi adalah sekumpulan rutin perangkat lunak yang berada diantara program aplikasi dan perangkat keras. System operasi memiliki tugas yaitu mengelola seluruh sumber daya system komputer dan sebagai penyedia layanan.

System operasi menyediakan *System Call* (berupa fungsi-fungsi atau API=*Application Programming Interface*). System Call ini memberikan abstraksi tingkat tinggi mesin untuk pemrograman. System Call berfungsi menghindarkan kompleksitas pemrograman dengan memberi sekumpulan instruksi yang lebih mudah dan nyaman, system operasi juga sebagai basis untuk program lain dimana program aplikasi dijalankan diatas system operasi, program-program itu memanfaatkan sumber daya system komputer dengan cara meminta layanan

system operasi mengendalikan sumber daya untuk aplikasi sehingga penggunaan sumber daya system komputer dapat dilakukan secara benar dan efisien.
System operasi yang dikenal antara lain :

- Windows (95, 98, ME, 2000, XP, VISTA, SERVER, Windows7)
- Linux (Red Hat, Slackware, Ubuntu, Fedora, Mikrotik, Debian, OpenSUSE)
- UNIX
- FreeBSD (Berkeley Software Distribution)
- SUN (SOLARIS)
- DOS (MS-DOS)
- Machintosh (MAC OS, MAC OSX)

2.4 Gateway

Gateway adalah pintu gerbang sebagai keluar-masuknya paket data dari local network menuju router network. Tujuannya agar client pada local network dapat berkomunikasi dengan internet. Router dapat disetting menjadi Gateway dimana ia menjadi penghubung antara jaringan local dengan jaringan luar.

2.5 Proxy Server

Proxy Server adalah sebuah fasilitas untuk menghubungkan diri ke internet secara bersama-sama. Memenuhi permintaan user untuk layanan Internet (http, FTP,Telnet) dan mengirimkannya sesuai dengan kebijakan. Bertindak sebagai gateway menuju layanan. Mewakili paket data dari dalam dan dari luar. Menangani semua komunikasi internet – ekternal. Bertindak sebagai gateway antara mesin internal dan eksternal. Proxy server mengevaluasi dan mengontrol permintaan dari client, jika sesuai policy dilewatkan jika tidak di deny/drop. Menggunakan metode NAT.

2.6 VLAN *(Virtual Local Area Network)*

Vlan merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti jaringan LAN , di mana dalam VLAN ini suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik suatu device.

Dengan menggunakan VLAN akan membuat pengaturan suatu jaringan menjadi lebih fleksibel di mana dapat di buat segmen yang bergantung pada organisasi atau departemen.

Keuntungan menggunakan VLAN :

a. Mengontrol Broadcast

Dengan menggunakan VLAN , secara default port – port yang tidak berada pada VLAN yang sama tidak dapat berkomunikasi dengan demikian makan broadcast dapat di atur oleh admin.

b. Meningkatkan kinerja jaringan

Dengan menggunakan VLAN , otomatis semua port – port yang memiliki VLAN yang sama saja yang dapat melakukan komunikasi , maka hanya VLAN yang sudah terdaftar yang bisa melalui switch tersebut , dengan itu akan meningkatkan kinerja jaringan tersebut .

c. Fleksibilitas dan skalabilitas.

Dengan menggunakan VLAN , tiap host yang memiliki VLAN yang sama bisa saling berkomunikasi tanpa harus masuk ke switch yang sama bisa dengan switch lain , dengan syarat VLAN harus sama dan harus terhubung dengan switch sebelum nya (Fleksibilitas) Dengan menggunakan VLAN, maka tidak perlu takut kehabisan port yang ada, di mana dengan menambahkan switch lain dan di daftarkan dengan VLAN yang sama maka akan dapat berkomunikasi lagi walaupun berbeda switch tapi dalam satu VLAN yang sama (Skalabilitas).

d. Keamanan jaringan.

Dengan menggunakan VLAN , sudah di atur sedemikian rupa sehingga akan meningkatkan security jaringan VLAN tersebut , karena beda VLAN tidak dapat saling berkomunikasi.

e. Mempermudah management jaringan

Dengan menggunakan VLAN , akan mempermudah seorang admin jaringan untuk memontioring dan memaintenance sebuah jaringan , karena sudah di kelompokan masing – masing VLAN sesuai dengan fungsi nya

2.7 Model TCP IP dan OSI Layer

Masalah yang paling utama dalam komunikasi antar komputer dari vendor yang berbeda adalah karena menggunakan protocol dan format data yang berbeda – beda , untuk mengatasi masalah ini International *Organization for Standardization* (ISO) membuat suatu arsitektur komunikasi yang di kenal dengan *Open System Interconnection* (OSI) model yang menjadi standart untuk menghubungkan komputer dari vendor yang berbeda – beda .

Manfaat dari adanya OSI layer yaitu :

- Membuat peralatan vendor yang berbeda dapat saling bekerjasama
- Membuat stadarisasi yang didapat dipakai vendor untuk mengurangi kerumitan perancangan
- Standarisasi interfaces
- Modular enginneering
- Kerjasama dan komunikasi teknologi yang berbeda
- Memudahkan pelatihan network.

Setiap layer bertanggung jawwab secara khusus pada proses komunikasi data. Misal, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, sementara layer lainnya bertanggungjawab untuk mengoreksi terjadinya "*error*" selama proses transfer data berlangsung. Pada tabel 2.7.1 merupakan penjelasan mengenai lapisan – lapisan OSI.

Table 2.7.1 Layer OSI

Nama	Diskripsi
Application Layer	Interface protocol TCP/IP dengan user
a. SMTP *(Simple mail transfer Protocol)*	Bertanggung jawab atas perpindahan pesan pesan email dari satu server ke server lainnya
b. FTP *(File Transfer Protocol)*	Mentransfer satu / banyak *file* dari satu komputer ke komputer lain
Transport Layer	mengadakan komunikasi antara dua komputer
a. TCP *(Transmission Control Protocol)*	***1) Connection-oriented*** dua aplikasi pengguna TCP haris melakukan *handshaking* terlebih dahulu ***2) Reliable*** proses deteksi kesalahan paket dan retransmisi. ***3) Byte strem service*** Paket-paket diurut kembali (*sequence*)
b. UDP *(User Datagram Protocol)*	1) Tidak *reliable* karena tidak bergaransi 2) Tidak ada *retransmision* jika pengiriman paket mengalami kegagalan 3) Penerima tidak mengirimkan tanda terima 4) Paket-paket tidak diurut kembali seperti asalnya *5)* Bersifat *multicasting* atau *broadcasting*
Internet Layer	proses pengiriman paket ke alamat yang tepat
a. IP *(Internet Protocol)*	1) menyampaikan paket data ke alamat yang tepat 2) pemecahan (*fragmentation*) dan penyatuan dari paket *3)* routing
b. ARP *(Address Resolution Protocol)*	translasi IP *address* yang diketahui menjadi MAC *address*
c. RARP *(Reverse Address Resolution Protocol)*	translasi MAC *address* yang diketahui menjadi IP *address*
d. ICMP *(Internet Control Message Protocol)*	mengirimkan pesan dan melaporkan kegagalan pengiriman data
Network Access Layer	mengirim dan menerima data ke dan dari media fisik

Peranan dari tabel OSI Layer sebagai berikut :

► Application Layer

Application Layer merupakan Layer paling atas pada model TCP/IP, yang bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol *Dynamic Host Configuration Protocol* (DHCP), *Domain Name System* (DNS), *Hypertext Transfer Protocol* (HTTP), *File Transfer Protocol* (FTP), Telnet, *Simple Mail Transfer Protocol* (SMTP), *Simple Network Management Protocol* (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi Stack Protocol, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka *Windows Sockets* (Winsock) atau NetBios over TCP/IP (NetBT).

► Transport Layer

Transport Layer berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat connection-oriented atau broadcast yang bersifat connectionless. Protokol dalam lapisan ini adalah *Transmission Control Protocol* (TCP) dan *User Diagram Protocol* (UDP).

► Internet Layer

Internet Layer berfungsi untuk melakukan pemetaan (*routing*) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. 47 Protokol yang bekerja dalam lapisan ini adalah Internet Protocol (IP), *Address Resolution Protocol* (ARP),*Internet control Message Protocol* (ICMP), dan *Internet Group Management Protocol* (IGMP)

► Network Access Layer

Network Access layer bertanggung jawab menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, dan menjaga antrian trafik di jaringan. Data pada layer ini berbentuk paket.

2.8 Switching

Switching adalah suatu proses elektronik yang dapat di pakai untuk menghubungkan jalur komunikasi . Jaringan switching adalah jaringan yang mengalokasikan sebuar sirkuit yang dedicated antara nodes dan terminal untuk di gunakan oleh pengguna untuk berkomunikasi.

Beberapa faktor yang menyebabkan terjadinya proses switching:

a. Interupsi system

   Di sebabkan oleh kejadian eksternal dan tak bergantung proses yang saat itu sedang berjalan.

b. Trap

   Trap merupakan interupsi karena terjadinya kesalahan atau kondisi pengecualian (*Exception condition*) yang di hasilkan oleh proses yang sedang berjalan , seperti usaha illegal untuk mengakses suatu file.

c. Supervisor call

   Yaitu panggilan meminta atau mengaktifkan bagian system operasi. Contoh: Proses pemakai running meminta layanan masukan/keluaran seperti membuka file. Panggilan ini menghasilkan transfer ke rutin bagian system operasi. Biasanya, penggunaan system call membuat proses pemakai blocked karena diaktifkan proses kernel (*system operation*).

2.9 QOS (*Quality of Service*)

Parameter QoS menggolongkan kualitas transfer yang diberikan oleh suatu koneksi yang diperoleh dengan membandingkan unit data pada sisi masukan dan keluaran interface.

Parameter QoS antara lain:

a. Delay

Delay didefinisikan sebagai total waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Besarnya delay maksimum yang direkomendasikan oleh ITU untuk aplikasi suara dan data 0 s/d 150 ms delay tersebut masih dapat di terima. Dan apabila delay di atas 400 ms tidak dapat diterima untuk layanan.

b. Throughput

Jumlah data per satuan waktu yang dikirim untuk suatu terminal tertentu di dalam sebuah jaringan,dari suatu titik jaringan, atau dari suatu titik ke titik jaringan yang lain. Throughput maksimal dari suatu titik atau jaringan komunikasi menujukkan kapasitasnya.Secara matematis throughput dapat dituliskan sebagai berikut :

$$throughput = \frac{\text{jumlah bit success delivered}}{\text{total waktu pengiriman}}$$

c. Jitter

Jitter atau variasi kedatangan paket diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpuanan ulang paket-paket diakhir perjalanan.

d Packet Loss

Packet loss adalah perbandingan seluruh paket IP yang hilang dengan seluruh paket IP yang dikirimkan antara pada source dan destination. Salah satu penyebab packet loss adalah antrian yang melebihi kapasitas buffer pada setiap node. Beberapa penyebab terjadinya packet loss yaitu:

- Congestion disebabkan terjadinya antrian yang berlebihan dalam jaringan
- Node yang bekerja melebihi kapasitas buffer
- Memory yang terbatas pada node.
- Policing atau kontrol terhadap jaringan

2.10 Redundant Routing Protocols

Berikut beberapa metode untuk redundant routing protokol, yaitu

- VRRP *(Virtual Router Redundancy Protocol)*
- FHRP *(First Hop Redundandy Protocol)*
- HSRP *(Hot Standby Router Protocol)*
- GLBP *(Gateway Loadbalancing Protocol)*

2.10.1 *VRRP* (*Virtual Router Redundancy Protocol*).

Virtual Router Redundancy Protocol merupakan suatu system untuk meningkatkan keandalan jaringan dengan menggunakan host standby *router*.

Protokol ini selalu memonitor kondisi router aktif dan siap menyediakan alamat ip jika router aktif tidak tersedia *mikrotik router OS. VRRP* telah

memenuhih RFC2338 , sehingga kompatibel dengan router komersial lainya, dengan keterbatasan hanya 255 virtual router per interface.

- Virtual Router

Image router tunggal yang diciptakan melalui operasi satu atau lebih router yang menjalankan *VRRP*.

- *VRRP* Instance

Program yang menerapkan *VRRP* yang berjalan pada sebuah router. Sebuah instance router tunggal *VRRP* bisa menyediakan kemampuan *VRRP* untuk lebih dari satu router virtual.

- Virtual Router ID (VRID)

Tanda pengenal numeris untuk sebuah virtual router khusus. VRID harus unique pada sebuah segmen jaringan yang tersedia.

- Virtual Router IP

Alamat IP yang berpasangan dengan sebuah VRID yang host lainnya bisa gunakan untuk mendapatkan layanan jaringan darinya. VRIP dikelola oelah *VRRP* instance yang menjadi milik dari sebuah VRID.

- Virtual MAC Address

Untuk media yang menggunakan pengalamatan MAC (seperti Ethernet), *VRRP* instance menggunakan sebuah alamat MAC yang sudah ditentukan sebelumnya untuk semua tindakan *VRRP* dari pada menggunakan alamat adapter MAC yang sebenarnya. Hal ini memisahkan operasi dari virtual router dari router yang sebenarnya yang menyediakan fungsi routing. VMAC diturunkan dari VRID.

- Master

Sebuah instance *VRRP* yang melakukan fungsi routing untuk virtual router pada suatu waktu. Hanya satu master yang aktif pada suatu waktu untuk sebuah VRID yang diberikan. Master juga merujuk pada sebuah kondisi dari *VRRP* FS ketika *VRRP* instance sedang beroperasi sebagai master (yaitu kondisi Master/Master State).

- Backup

Sebuah instance *VRRP* untuk sebuah VRID yang aktif namun tidak dalam kondisi master. Berapapun jumlah backup bisa ada untuk sebuah VRID. Backup

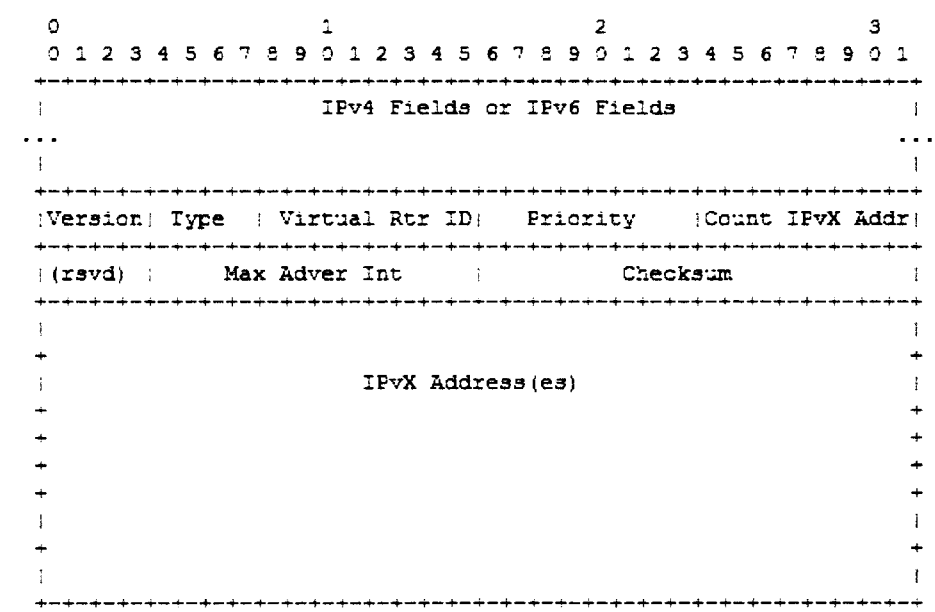
siap untuk untuk mengambil peran sebagai master jika master saat ini gagal. Backup juga merujuk pada kondisi FSM *VRRP* ketika instance *VRRP* sedang beroperasi sebagai backup (yaitu "*backup state*").

- Priority

Nilai prioritas yang diberikan untuk *VRRP* Instance yang berbeda, sebagai cara untuk menentukan router mana yang akan mengambil peran sebagai master jika master saat itu gagal. Priority adalah sbeuah angka dari 1 sampai 254 (0 dan 255 dipakai). Semakin besar angka, semakin tinggi prioritas.

- Owner

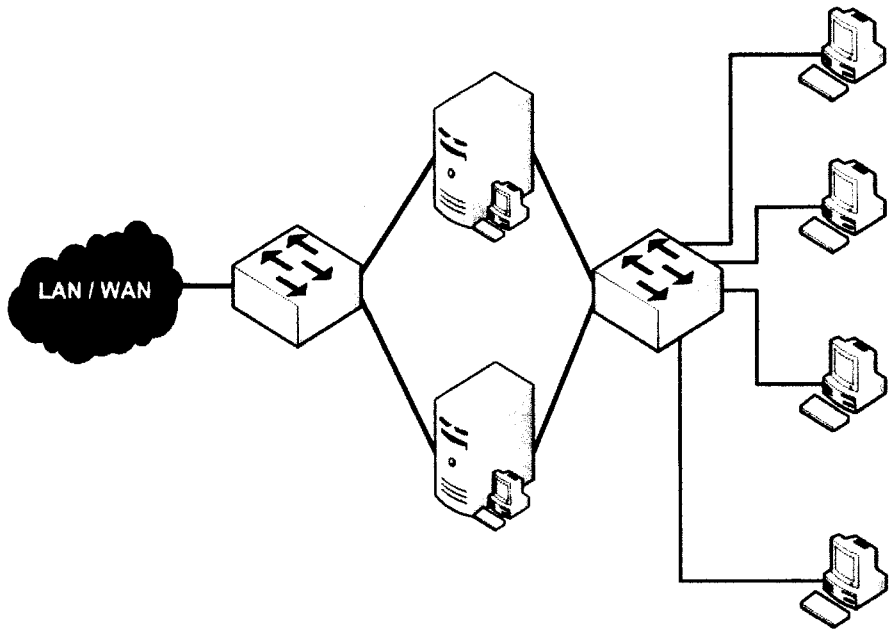
Jika alamat IP virtual sama karena alamat IP apapun dikonfigurasi pada sebuah interface dari router , router tersebut adalah owner dari alamat IP virtual. Prioritas dari *VRRP* Instance ketika VIP owner adalah 255, nilai tertinggi dan sudah dipakai.



Gambar. 2.10.1 *VRRP* Packet Format.

System *VRRP* memilih router yang digunakan berdasarakan prioritas router. Pada saat router di dalam virtual router ini hanya satu yang berada pada mode master dan lainnya dalam kondisi slave. Router pada kondisi master selalu mengirimkan inforasi *VRRP* ke semua router yang berada pada posisi backup. Jika

selama 3 selama inforasi BRRP tidak ada, maka backup router berdasarkan prioritas memproklamasikan master menggunakan RFC2338.

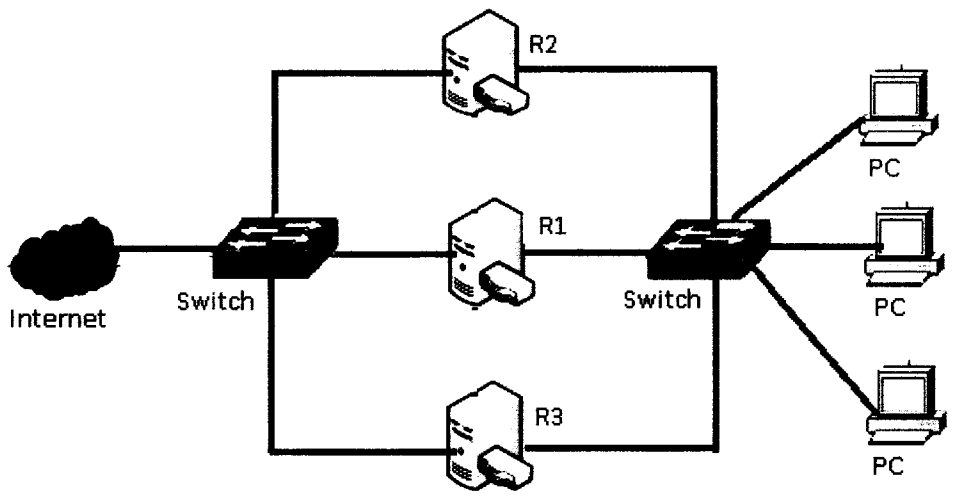


Gambar. 2.10.2 Model System *VRRP* untuk *Redundant Router*

Pada gambar 2.9.1 merupakan rancangan *VRRP* pada umumnya atau secara garis besarnya,

Adapun *protocol stack VRRP* terdiri dari

a. *Source Address*, merupakan IP *address* utama dari *interface* dimana paket akan dikirim.
b. *Destination Address*, merupakan IP *multicast address* dimana semua router dengan rancangan *VRRP* menerima *multicast* ini.
c. *Time To Live,* semua paket *VRRP* dengan *Time To Live* tidak sama 255 maka ditolak.
d. *Protocol,* menunjukkan protocol yang digunakan.



Gambar 2.10.3 Model *System VRRP* menggunakan 1 Master 2 Backup

Pada gambar 2.10.3 merupakan perancangan system *VRRP* menggunakan 3 router, 1 router sebagai router master (R1) dan 2 router sebagai backup nya (R2 dan R3).

Ilustrasi konsep *VRRP* pada gambar 2.9.2

- IP *VRRP* diset 10.1.1.1 pada masing-masing router
- R1 diset sebagai router master dengan priority tertinggi misal 255. Dengan IP 10.1.1.3
- R2 diset sebagai router backup dengan priority misal 200. Dengan IP 10.1.1.4
- R3 diset sebagai router backup dengan priority misal 190. Dengan IP 10.1.1.5
- Apabila R1 terjadi kegagalan koneksi atau down maka R2 secara otomatis menggantikan router master karena nilai priority nya lebih tinggi dibanding R3.

Cara Kerja *VRRP* (*Virtual Router Redundancy Protocol*)

Host yang ditunjukan di gambar 2.9.2 dikonfigurasi dengan IP Address Router Virtual sebagai default gateway. Seperti disebutkan diatas, master meneruskan paket yang ditujukan untuk remote subnet dan menanggapi permintaan ARP.Seperti dalam contoh ini master juga adalah virtual router pemilik interface IP Address, juga menanggapi permintaan ICMP dan datagram IP yang ditujukan untuk interface router IP address virtual tersebut. Backup tidak meneruskan paket atas nama interface router virtual, juga tidak merespon permintaan ARP.

Jika master tidak tersedia/mati maka backup akan menjadi master dan mengambil alih tanggung jawab untuk meneruskan paket dan menanggapi request ARP. Tetapi karena Master baru ini bukan IP address pemilik maka tidak menanggapi request ping ICMP dan alamat IP datagram. Setiap VRRP Router yang merupakan penyewa dikonfigurasi dengan prioritas antara 1 dan 254. Menurut standar VRRP, sebuah pemilik memiliki prioritas 255. Dalam gambar 2.10.3 di atas RS1 dikonfigurasi untuk VRRP, terlihat IP address router virtual dan membandingkannya dengan IP address dari interface sendiri yang dikonfigurasi untuk VRRP di VRID. Karena RS1 memiliki IP address router virtual itu menyatakan dan mengirim pemberitahuan ke semua router VRRP lainnya bahwa dirinya adalah master.Dalam hal ini proses untuk menentukan master berbeda, proses ini membandingkan 2 kriteria. Pertama, Router dengan prioritas tertinggi menjadi Master. Kedua jika prioritas sama, IP address tertinggi menang dan menjadi Master. Memahami paket VRRP adalahkunci untuk mengetahui proses penawaran.

Keuntungan dari *VRRP* :

a. Redudancy.

VRRP memungkinkan untuk mengkonfigurasi beberapa router sebagai default gateway router, yang mengurangi kemungkinan satu titik kegagalan dalam sebuah jaringan.

b. Load Sharing.

VRRP dapat dikonfigurasi sedemikian rupa sehingga lalu lintas ke dan dari klien LAN dapat digunakan bersama oleh beberapa router, sehingga dapat membagi beban lalu lintas yang tersedia secara lebih merata di antara router.

c. Multiple Virtual Router.

VRRP mendukung hingga 255 virtual router (*VRRP* group) pada sebuah *router physical interface*. Beberapa dukungan router virtual memungkinkan untuk melaksanakan redudancy dan load sharing dalam topologi LAN.

d. Multiple IP Addresses.

Virtual Router dapat mengelola beberapa IP address, termasuk secondary ip address. Oleh karena itu, jika memiliki beberapa subnet yang dikonfigurasi pada Ethernet interface, *VRRP* dapat dikonfigurasikan pada setiap subnet.

e. Preemption.

Skema redundansi dari *VRRP* memungkinkan untuk membuat terlebih dahulu virtual router cadangan yang telah mengambil alih virtual router master yang gagal dengan prioritas yang lebih tinggi dari virtual router cadangan yang tersedia.

f. Authentication.

Pesan *VRRP* digest 5 (MD5) algoritma otentikasi melindungi *VRRP*-spoofing terhadap perangkat lunak dan menggunakan standar industri algoritma MD5 untuk meningkatkan kehandalan dan keamanan.

g. Advertisement Protokol.

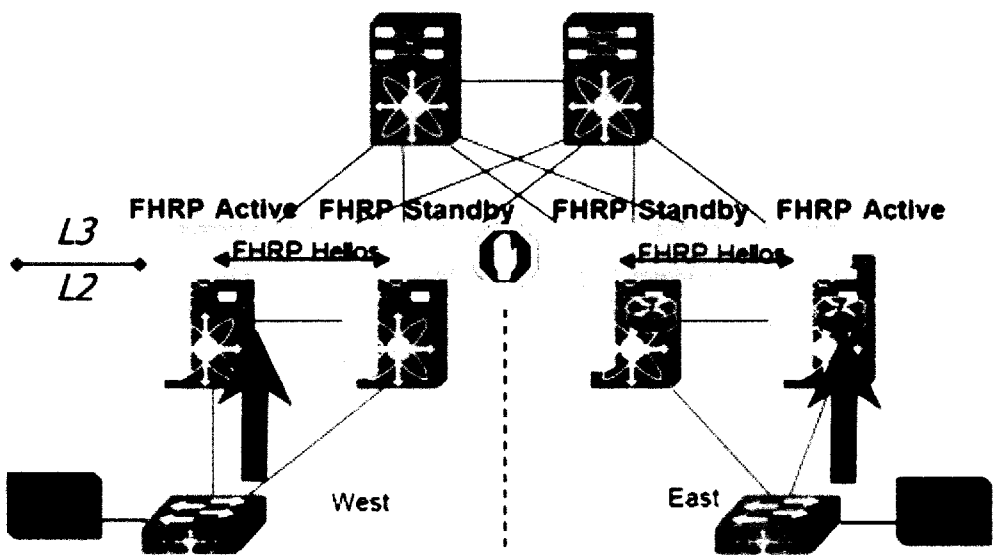
VRRP menggunakan *Internet Assigned Numbers Authority* (IANA) dengan standard multicast address-nya (224.0.0.18). Skema pengalamatan ini meminimalkan jumlah router yang harus melayani multicasts dan memungkinkan peralatan tes untuk mengidentifikasi secara akurat paket *VRRP* pada segmen.

h. *VRRP* Object Tracking.

VRRP Object Tracking menyediakan cara untuk memastikan router virtual master terbaik dari router *VRRP* untuk *VRRP* group dengan mengubah prioritas ke status Object Tracking seperti interface atau IP route states.

2.10.2 FHRP (*First Hop Redudancy Protocol*)

FHRP merupakan suatu Protocol yang berguna untuk Network agar selalu dalam kondisi ON dengan cara menyediakan jalur (Link) *Redudancy* pada dua atau lebih perangkat *Phisiccally* yang di konfigurasi menjadi satu perangkat virtual, salah satu perangkat akan menjadi jalur active (utama) dan yang lain Standby atau jalur cadangan (Backup Link) apabila jalur utama Down, misal: dua perangkat menjadi satu interface virtual jadi pada dua perangkat tersebut akan sepakat hanya ada satu gateway pada dua Link (jalur) dan pada Link tersebut ada yang active dan backup.



Gambar 2.10.4 FHRP *(First Hop Redudancy Protocol)*

Proses detail pada konfigurasi Protocol FHRP adalah sebagai berikut:

1.Forwarding / Active Router mengirim Hello packet ke Standby Router tiap beberapa detik

2.Secara Default Router yang menyala duluan akan menjadi Forwarding Router

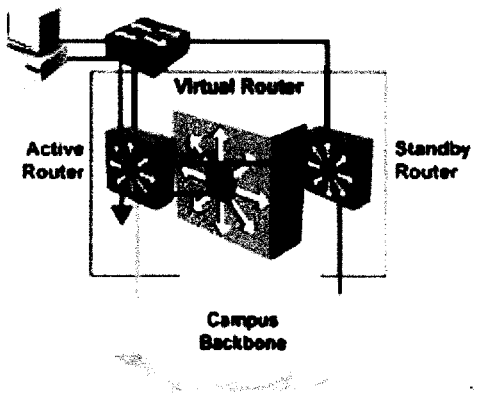
3.Apabila Active Router lagi Down dan tidak mengirim Hello paket ke Standby Router maka otomatis Standby Router Active dan menjadi forwarding Ruter.

4.Secara Default apabila mantan Active Router UP lagi maka dia akan menjadi Standby Router dan posisinya sudah di ambil alih, (kecuali nilai Priority masih Tertinggi maka akan menjadi Active Router lagi).

2.10.3 HSRP (*Hot Standby Router Protocol*)

HSRP adalah metode standar untuk memberikan ketersediaan jaringan yang tinggi dengan menyediakan First-hop redundancy untuk IP host pada LAN IEEE 802 dikonfigurasi dengan default gateway IP address. Sebuah jaringan dengan High availability menyediakan sarana alternatif yang mana semua infrastructure paths dan key server dapat diakses setiap saat. *Hot Standby Router rotocol* (HSRP) adalah salah satu fitur perangkat lunak tersebut yang dapat dikonfigurasi untuk menyediakan Layer 3 redundansi untuk network host.

Ini memungkinkan dua router interface untuk bekerja sama untuk menyajikan penampilan satu virtual router atau default gateway untuk host di LAN. Jadi dengan kata lain ketika salah satu router yang terconfigure dalam HSRP nya down maka Link pada jaringan tersebut tetap berjalan, dikarenakan ip gateway yang di kenal host adalah ip nya virtual router.



Gambar 2.10.5 HSRP (*Hot Standby Router Protocol*).

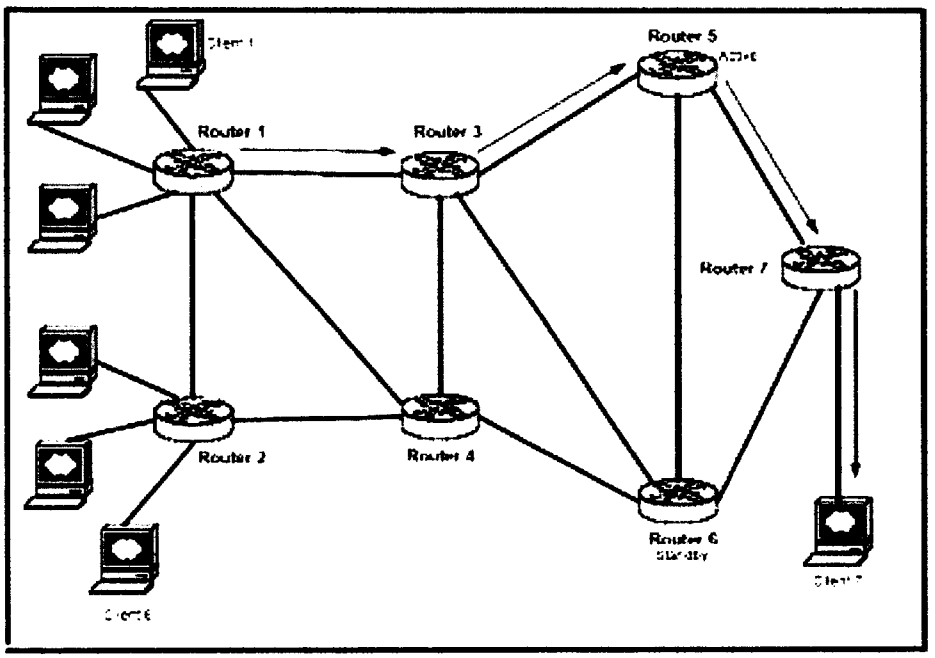
HSRP mendefinisikan sebuah Standby Router, dengan satu router sebagai Active Router. HSRP menyediakan gateway redundancy dengan sharing IP dan MAC address antara redundant gateway yang tergabung dalam HSRP yang sama.

Term (Istilah)	**Definition (Definisi)**
Active Router	Router yang meneruskan paket-paket untuk virtual router
Standby Router	Router cadangan Bila Active Router Down
Standby Group	The set of routers participating in HSRP that jointly emulate a virtual router

2.10.4 GLBP (*Gateway Loadbalancing Protocol*)

Load balancing adalah sebuah konsep yang gunanya untuk menyeimbangkan beban atau muatan. Seperti itulah prinsip kerja dari *Gateway Load Balancing Protocol* (GLBP). Intinya adalah membagi kerja Router yang besarnya sama atau seimbang. *Gateway Load Balancing Protocol* (GLBP) melindungi trafik data dari kerusakan router atau jalur data. GLBP melindungi trafik dengan cara routerrouternya diberi sebuah default gateway yang sama sedangkan yang membedakan pada virtual MAC nya dari masing-masing router.

Pada Gambar 2.10.6 Router 5 sebagai router active, sedangkan router 6 berperan sebagai router standby apabila terjadi congesti. Sebuah router dipilih sebagai active router yang nantinya akan membawa paket melalui virtual IP address dalam group tersebut.



Gambar 2.10.6 GLBP (*Gateway Loadbalancing Protocol*)

Cara Kerja GLBP (*Gateway Loadbalancing Protocol*)

- GLBP *Active Virtual Gateway*

GLBP Group memilih satu gateway yang akan menjadi active virtual gateway (AVG) untuk group tersebut. Anggota group lain membackup AVG tersebut untuk menghindari jika AVG tersebut sewaktu-waktu tidak terpakai lagi. Gateway lainnya menganggap hubungan perjalanan paket mengirim ke virtual MAC address ditentukan oleh AVG. Gateway yang mengetahui active virtual MAC address selanjutnya. AVG bertanggung jawab untuk menjawab request dari Address Resulution protocol (ARP) untuk meminta Virtual IP address. Load sharing terjadi ketika AVG membalas ARP request dengan virtual MAC address yang berbeda.

- GLBP *Virtual Gateway Redundancy*

Menjalankan Virtual Gateway Redundancy pada GLBP sama dengan HSRP. ateway yang berwenang untuk memutuskan adalah AVG sedangkan Gateway lainnnya ebagai standby virtual gateway dan gateway yang tersisa ditempatkan di tempat yang udah diperhatikan. Jika terjadi kerusakan pada AVG, maka standby virtual gateway kan menerima tanggung jawab sebagai Virtual IP address. Standby Virtual Gateway yang baru akan ditempatkan di tempat yang mudah diperhatikan.

- GLBP *Virtual Forwarder Redundancy*

Virtual Forwarder Redundancy sama seperti *Virtual Gateway Redundancy* dengan suatu AVF. Apabila AVF mengalami gangguan, maka *Secondary Virtual Forwarder* (SVF) akan menerima status dan bertanggung jawab pada Virtual MAC Address. AVF yang baru akan menjadi primary virtual forwarder untuk sebuah nomor forwarder yang berbeda.