BAB 2
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian Nurhazmi Hawari, Iskandar Fitri dan Andri Aningsih tahun 2019 [2] membahas tentang penggunaan VRRP pada *Backup Link Reviewed Layer Distribution Method.* Penelitian ini menghasilkan nilai *packet loss* dan *throughput* yang terjadi pada jaringan selama waktu pengamatan. Peneltian ini melakukan enam buah pengujian dengan masing-masing pengujian dilakukan selama 10, 20, 30, 40, 50 dan 60 menit. Besar *packet loss* yang dihasilkan dari penelitian ini yaitu masing-masing sebesar 0,43%, 0,21%, 0,20%, 0,10%, 0,8% dan 0,10%. Berdasarkan standar TIPHON, hasil tersebut termasuk ke dalam kategori sangat baik. Adapun besar nilai *throughput* yang dihasilkan yaitu masing-masing sebesar 275 bps, 280 bps, 282 bps, 279 bps dan 278 bps yang juga termasuk ke dalam kategori sangat bagus berdasarkan standarisasi TIPHON.

Penelitian Bella Listya Arisiha, Indrarini Dyah Irawati dan Muhammad Iqbal tahun 2020 [8] melakukan penelitian tentang penggunaan *failover protocol* VRRP dengan menggunakan MPLS (*Multi Protocol Label Switching*). Penelitian ini bertujuan untuk mengetahui nilai parameter QoS dari jaringan yang dibangun. Penelitian ini menggunakan tiga buah scenario pengambilan data, yaitu dengan melakukan pengukuran pada layanan *voice call*, video *call* dan layanan data jaringan dengan masing-masing scenario melakukan lima kali pengambilan data. Pada scenario *voice call*, pengukuran menghasilkan rata-rata nilai *throughput* 115 kbps, *packet loss* 2.47%, *delay* 9.02 ms dan *jitter* 7.21 ms. Pada scenario Pengukuran layanan video *call*, pengukuran menghasilkan nilai rata-rata *throughput* 1911 Kbps, *packet loss* 1.09%, *delay* 2.6 ms dan *jitter* 2.7 ms. Sedangkan pada skenario pengukuran layanan data, pengukuran menghasilkan nilai rata-rata *throughput* 1.2 Kbps, *packet loss* 0.6%, *delay* 3.27 ms dan *jitter* 3.12 ms.

Penelitian Riffat Hasan Saputra, Alif Subardono tahun 2020 [9], menganalisa pengaruh *failover* pada *Software Defined Network* dan konevensional.

Penelitian ini bermaksud untuk mengetahui pengaruh *failover* pada jaringan SDN dan konvensional dengan menambahkan konfigurasi load *balancing* metode ECMP pada perangkat *router* MikroTik RB951-2n. Penelitian ini menggunakan lima buah kasus yang berbeda dimana pada setiap kasus, Host-1 akan melakukan proses pengunduhan berkas dengan ukuran 1,5 GB dari situs ubuntu.com. Sedangkan Host-2 akan melakukan streaming video dari situs youtube.com dengan kualitas video yang dijalankan adalah 360p. Kasus pertama hanya menggunakan ISP-A yang diberi alokasi *bandwidth* sebesar 4 Mbps. Kasus kedua hanya menggunakan ISP-B dengan *bandwidth* sebesar 2 Mbps. Pada kasus ketiga menggunakan ISP-A dan ISP-B secara bersamaan tanpa melakukan uji *failover*. Kasus keempat menggunakan ISP A dan ISP B secara bersmaan dengan melakukan uji *faizlover* di tengah pengujian. Untuk kasus terakhir akan menggnakan dua jalur *gateway* dengan alokasi *bandwidth* yang sama yaitu 2 Mbps serta ditambahkan uji *failover*. Data dari nilai trafik *bandwidth* dicatat menggunakan graphing setiap lima menit terhitung sejak setiap kasus mulai dijalankan selama 40 menit untuk masing-masing kasus. Kelima kasus ini dilakukan pada jaringan SDN dan jaringan konvensional. Hasilnya, pada kasus 1 jaringan konvensional, trafik yang masuk pada jaringan lokal sebesar 3,77 Mbps. Sedangkan pada SDN, *bandwidth* yang masuk ke jaringan lokal sebesar 3,72 Mbps. Pada kasus 2, pada jaringan konvensioal *bandwidth* yang masuk pada jaringan lokal sebesar 2,03 Mbps dan pada SDN *bandwidth* pada jaringan lokal yaitu 2,09 Mbps. Pada kasus 3 jaringan konensional, jaringan lokal memiliki *bandwidth* sebesar 5,44 Mbps sedangkan pada SDN *bandwidth* yang diterima pada jaringan lokal yaitu sebesar 5,74 Mbps. Pada kasus keempat, dilakukan juga percobaan *failover* dengan memutus koneksi pada ISP A dan ISP B secara bergantian yang menyebabkan rata-rata *bandwidth* yang diterima menurun. Pada jaringan konvensional, rata-rata bandiwth pada jaringan lokal yaitu sebesar 4,27Mbps. Sedangkan pada SDN, jaringan lokal memiliki *bandwidth* sebesar 4,2 Mbps. Pada kasus kelima, jaringan konvensional memiliki *bandwidth* yang diterima oleh jaringan lokal sebesar 2,78 Mbps sedangkan pada jaringan SDN, besar *bandwidth* yang diterima jaringan lokal adalah 2,62 Mbps.

Penelitian Mugi Raharjo, Frengki Pernando dan Ahmad Fauzi tahun 2019 [10], menganalisa mengenai *failover* menggunakan protokol VRRP. Penelitian ini

bertujuan untuk meningkatkan *high Availability* jaringan pada perusahaan PT. Pelita Cengkareng Paper. Percobaan dilakukan dengan melakukan tes PING dari *client* ke *internet*, bersamaan dengan itu koneksi yang digunakan akan diputuskan. Uji coba ini dilakukan dengan dua skema, skema pertama tanpa menggunakan metode *failover* sedangkan skema kedua menggunakan metode *failover* dengan protokol VRRP. Hasilnya, pada skema pertama informasi ping menunjukkan keterangan *Destination host unreachable* karena tidak ada koneksi cadangan yang dapat mem*backup* koneksi ketika terputus. Sedangkan pada skema kedua, setelah *router* utama mengalami gangguan maka koneksi langsung dialihkan pada *router backup* sehingga koneksi dapat tetap berlanjut.

Penelitian Rachmat Adi Purnama dan Firmansyah tahun 2020 [11], meneliti penggunaan metode *failover* dengan menggunakan protokol VRRP. Pengujian dilakukan dengan melakukan *failover* dari *router master* ke *router backup* dan dari *router backup* ke *router master*. Hasilnya, pada *failover* dari *router master* ke *router backup* rata-rata *time response failover* yang dibutuhkan adalah 3,75ms dengan rata-rata *packet loss* yang terjadi sebanyak 3 packet. Sedangkan pada *failover* dari *router backup* kembali ke *router master*, rata-rata *time response failover* yang dibutuhkan sebesar 1,37ms dengan *packet loss* sebanyak 1,5 *packet*.

Adapun perbandingan penelitian yang penulis akan lakukan dengan kelima penelitian sebelumnya dapat dilihat pada tabel 2.1.

Tabel 2.1 Rangkuman Keterkaitan dengan Penelitian Sebelumnya

Penelitian Oleh	***Objective***	***Failover***	**Jaringan**	**Hasil Penelitian**
Nurhazmi Hawari, Iskandar Fitri dan Andri Aningsih **(**2019)	Meneliti mengenai penggunaan protokol VRRP	Menggunakan protokol VRRP	Konvensional	Nilai *packet loss* dan *throughput* yang didapat pada penelitian termasuk ke dalam kategori sangat bagus
Bella Listya Arisiha, Indrarini Dyah Irawati dan	Meneliti penggunaan Protokol VRRP	Menggunakan protokol VRRP	Konvensional	Jaringan memiliki performansi yang bagus berdasarkan pada parmeter

Penelitian Oleh	***Objective***	***Failover***	**Jaringan**	**Hasil Penelitian**
Muhammad Iqbal				QoS yang dihasilkan selama penelitian
Riffat Hasan Saputra, Alif Subardono (2020)	Meneliti pengaruh *failover* pada *Software Defined Network* dan konevensional	*Failover* diintegrasikan dengan load balancing Menggunakan ECMP pada *router* MikroTik RB951-2n	Konvensional dan SDN	Rata-rata efisiensi trafik dengan metode *failover* pada SDN lebih baik dari jaringan konvensional sebesar 0,5%
Mugi Raharjo, Frengki Pernando dan Ahmad Fauzi (2019)	Meneliti metode *failover* menggunakan protokol VRRP	Menggunakan protokol VRRP	Konvensional	*Failover* berfungsi dengan baik sehingga koneksi dapat tetap berjalan meski *link* utama terputus
Rachmat Adi Purnama dan Firmansyah (2020)	Meneliti penggunaan protokol VRRP	Menggunakan protokol VRRP	Konvensional	*Time response failover* dari *router master* ke *router backup* membutuhkan waktu lebih lama dari pada *time response failover* dari *router backup* ke *router master*
M Aldi Baihaqi	Meneliti penggunaan metode *failover p*ada SD-WAN	Menggunakan protokol VRRP	SD-WAN	Hasil yang diharapkan berupa performansi dari parameter QoS serta *time response failover* yang dihasilkan

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Jaringan computer adalah kumpulan beberapa perangkat seperti PC, printer, LAN Card, *Router* dan lain-lain yang membentuk sebuah jaringan yang terintegrasi satu sama lain [12]. Dua buah PC dapat dikatakan terkoneksi jika keduanya dapat saling mengirimkan data atau informasi. Masing-masing perangkat yang terhubung pada jaringan komputer disebut node [13].

1. *Local Area Network* (LAN)

Local area Network (LAN) merupakan jaringan sejumlah perangkat atau node yang memiliki lingkup lokas terbatas pada satu Gedung satu kompleks Gedung atau kampus [14] dengan tujuan berbagi resource (Resource Sharing). Dalam jaringan LAN, minimal perangkat yang digunakan terdapat dua buah perangkat agar dapat saling mengirimkan data antara keduanya dimana pada kedua perangkat tersebut harus memiliki kartu jaringan atau LAN Card.

2. *Metropolitan Area Network* (MAN)

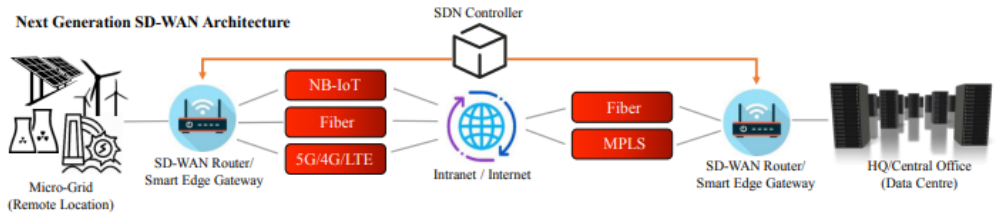
Metropolitan Area Network (MAN) merupakan versi LAN dengan ukuran atau cakupan wilayah yang lebih luas, namun cakpuan areanya lebih kecil dibandingkan dengan WAN. Pada biasanya teknologi yang digunakna pada MAN sama dengan teknologi pada LAN. MAN mampu menunjang komunikasi data berupa data dan suara. Bahkan, MAN juga dapat berhubungan dengan jaringan televisi kabel [15].

3. *Wide Area Network* (WAN)

Wide Area Network (WAN) merupakan kumpulan jarinagn LAN atau workgroup yang terhubung dengan alat telekomunikasi, biasanya menggunakan modem. untuk terhubung pada jaringan antar kantor pusat-cabang ataupun antar cabang. Jaringan WAN dapat terhubung dengan memanfaatkan jaringan umum (*internet*) namun dengan memperhatikan masalah keamanan [15].

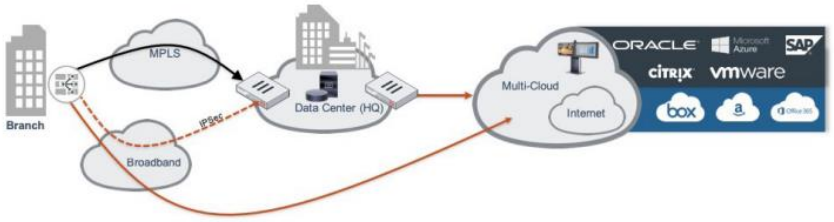
2.2.2 *Software Defined Wide Area Network* (SD-WAN)

SD-WAN merupakan bentuk implementasi *Software-defined Network* (SDN) pada *Wide Area Network* (WAN) [16]. SD-WAN mampu memberikan pelayanan dalam hal melakukan management WAN (*internet*) guna memperoleh performansi *traffic* yang cukup tinggi namun dengan harga yang rendah, sehingga diharapkan kebutuhan akan *internet* dapat dipenuhi serta dapat menggantikan private WAN yang memiliki *cost* yang lebih mahal [17]. Komunikasi antara *router edge* (*data plane*) dan *controller* (*control plane*) terhubung secara *secured tunnel*. Sebuah *controller* dapat memiliki beberapa *router edge* tergantung pada banyaknya jaringan *branch* atau cabang yang dimiliki [18].



Gambar 2.1 Arsitektur SD-WAN

Arsitektur SD-WAN, seperti pada Gambar 2.1, memiliki kemampuan untuk memastikan alokasi sumber daya, perutean jalur otomatis dan dinamis, yang mengoptimalkan keseimbangan beban dan ketahanan. SDWAN mengurangi *downtime* jaringan, meminimalkan hilangnya produktivitas dengan mendeteksi gangguan pada jaringan secara *real time*. Jika terjadi gangguan pada salah satu jalur komunikasi, *link* koneksi secara otomatis akan beralih ke *link* yang tersedia sehingga dapat menjaga jaringan tetap berjalan. [19].



Gambar 2.2 Arsitektur Fortigate SD-WAN

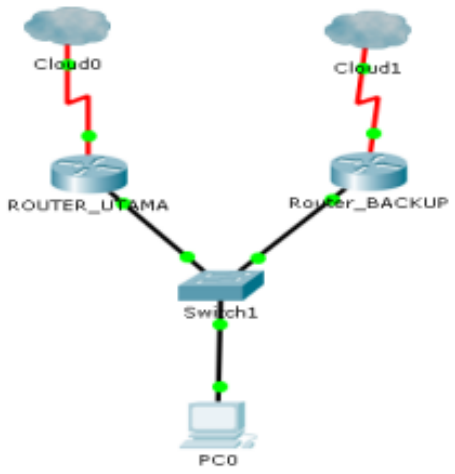
Gambar 2.2 menunjukkan arsitektur SD-WAN dengan menggunakan fortigate. Pada gambar tersebut, sebuah cabang dengan SD-WAN memiliki lebih dari satu koneksi. Jaringan WAN memiliki *link* koneksi yang memanfaatkan MPLS

dan juga koneksi broadband tunggal untuk menyediakan akses *internet* langsung dari cabang [20].

2.2.3 *FAILOVER*

failover merupakan teknik yang dapat memungkinkan penggunaan beberapa jalur komunikasi *internet* dengan menggunakan 2 atau lebih *router* untuk mencapai suatu *Network* tujuan dimana *router* terbagi menjadi dua, yaitu *router* yang digunakan sebagai utama dan *router* lainnya akan digunakan sebagai *router backup*. *Router backup* akan menggantikan fungsi dari *router* utama apabila *router* utama mengalami kendala[1]. Protokol pada *failover* yaitu Hop *Redundancy Protocol* (FHRP). FHRP merupakan protokol yang digunakan untuk melindungi default *gateway* pada sub jaringan dengan cara membuat dua atau lebih *router* menyediakan cadangan *link* koneksi. Apabila *router* aktif mengalami gangguan pada koneksi, *router* cadangan akan mengambil alih *link*, hal ini terjadi dalam selang waktu beberapa detik [6]. Terdapat tiga protokol pada FHRP yaitu *Virtual Router Redundancy Protocol* (VRRP), *Hot standby* Routing *Protocol* (HSRP), and *Gateway Load Balancing Protocol* (GLBP) [21].

2.2.4 *VIRTUAL ROUTER REDUNDANCY PROTOCOL* (VRRP)



Gambar 2.3 VRRP dengan Dua Buah *Link* Koneksi

Gambar 2.3 merupakan contoh topologi pada metode *failover* dengan menggunakan dua buah *router* yang terhubung pada 2 buah cloud yang berbeda. VRRP adalah salah satu protokol yang dapat digunakan pada metode *failover*.

VRRP memungkinkan satu atau lebih *virtual router* menjadi *gateway router* pada suatu jaringan LAN, yang memungkinkan dua atau lebih *router* di *multiaccess link* untuk menggunakan *virtual ip address* yang sama. VRRP digunakan pada jaringan LAN untuk mengantisipasi kegagalan dari *router* yang dijadikan sebagai *router* utama [5].

Dua atau lebih *krouter* harus dikonfigurasikan dengan ID *router virtual* dan alamat IP *virtual* yang sama sehingga keduanya dapat secara otomatis bergabung dengan domain VRRP yang sama. Prioritas harus ditetapkan ke setiap *interfaces* tersebut di domain VRRP dengan nilai prioritas yang berbeda. *Interface* dengan prioritas tertinggi akan menjadi *router* utama sedangkan *interfaces* diberi prioritas lebih rendah dan menjadi *router* cadangan. Jika *router* utama gagal, VRRP secara otomatis mengalihkan ke *router* di domain dengan prioritas tertinggi berikutnya.

2.2.5 Packet *Network* Emulator Tool Lab (PNETLab)

PNETLab dapat digunakan melakukan praktik laboratorium jaringan komputer secara *virtual* sehingga dapat mengatasi masalah keterbatasan perangkat praktikum. PNETLab juga memungkinkan *user* untuk berbagi sumber daya sehingga pekerjaan menjadi lebih cepat untuk dikerjakan secara bersamaan. Pada PNETLab akan diim*port* beberapa image *router* dan perangkat lainnya yang dibutuhkan dalam membuat topologi jaringan [22].

2.2.6 D-ITG

Distributed *Internet Traffic* Generator (D-ITG) adalah mampu membangkitkan *traffic* pada level paket secara akurat pada topologi jaringan. Pada D-ITG dapat dihasilkan sebuah log *file* hasil simulasi dari pengiriman trafik pada topologi jaringan. D-ITG memungkinkan untuk menyimpan informasi baik di sisi penerima maupun sisi pengirim. Dengan demikian dimungkinkan untuk mengambil informasi tentang pola lalu lintas yang dihasilkan [23].

2.2.7 *WIRESHARK*

Wireshark berfungsi untunk menangkap informasi *traffic* yang berjalan pada topologi jaringan sedetail mungkin sehingga jaringan dapat dianalisa dengan

menyesuaikan parameter-parameter yang ada [24]. *Wireshark* dapat merekam *traffic* yang berjalan termasuk protokol yang bekerja pada topologi tersebut sehingga dapat diamati protokol VRRP berjalan atau tidak

2.2.8 *Quality of Service* (QOS)

Quality of Service (QoS) adalah suatu cara untuk menentukan kualitas jaringan. QoS merupakan bentuk usaha guna mendefinisikan karakteristik dan sifat dari suatu jaringan. Parameter Qos yang dinilai berupa parameter seperti *delay*, *jitter* atau packetloss. Jaringan dapat melakukan penggunaan *bandwidth* yang bervariasi untuk memenuhi permintaan [25].

1. *Throughput*

Throughput merupakan kemampuan dari suatu jaringan dalam mentransmisikan data perdetik Satuannya yaitu *bit* per *second* (bps). Rumus perhitungan *throughput* seperti pada persamaan 2.1 [26]. Untuk menentukan klasifikasi nilai *throughput* yang didapat dapat berpatokan pada standarisasi TIPHON seperti yang terlihat pada tabel 2.2.

$$\text{Throughput} = \frac{Jumlah\ data\ yang\ dikirim}{Waktu\ pengiriman\ data} \quad \textbf{(2.1)}$$

Tabel 2.2 Kategori *Throughput*

Kategori	Besar *Throughput (%)*	Indeks
Sangat Bagus	<100	4
Bagus	<75	3
Sedang	<50	2
Jelek	<25	1

2. *Delay*

Delay merupakan waktu rata-rata yang dibutuhkan oleh paket untuk terkirim dari node sumber ke node tujuan. *Delay* mempengaruhi kualitas layanan (QoS) karena menunjukkan bahwa paket membutuhkan waktu untuk mencapai tujuannya dalam waktu yang lebih lama seperti yang ditunkukkan pada persamaan 2.2 [27]. Untuk menentukan klasifikasi nilai *delay* yang didapat dapat berpatokan pada standarisasi TIPHON seperti yang terlihat pada table 2.3.

$$\text{Delay rata} - \text{rata} = \frac{Total\ Delay}{Total\ paket\ yang\ diterima} \quad \textbf{(2.2)}$$

Tabel 2.3 Kategori *Delay*

Kategori	Besar *Delay*	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Jelek	>450ms	1

3. Jitter

Jitter merupakan variasi *delay* pada proses transmisi yang terjadi karena adanya perbedaan waktu atau interval kedatangan antar paket yang diterima oleh node tujuan. Cara mengatasi permasalahan *jitter* yaitu paket data yang datang dihimpun terlebih dahulu pada *jitter* buffer selama waktu tertentu hingga paket dapat diterima pada sisi receiver dengan urutan yang benar. Perhitungan *jitter* dapat dilihat pada persamaan 2.3 [25]. Untuk menentukan klasifikasi nilai *jitter* yang didapat dapat berpatokan pada standarisasi TIPHON seperti yang terlihat pada tabel 2.4.

$$Jitter = \frac{total\ variasi\ delay}{total\ paket\ yang\ diterima} \quad \textbf{(2.3)}$$

Tabel 2.4 Kategori *Jitter*

Kategori	*Jitter*	Indeks
Sangat Bagus	0 ms	4
Bagus	0 ms s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
Jelek	125 ms s/d 225 ms	1

4. *Packet loss*

Packetloss merupakan persentase data yang gagal dikirim dari total data yang ditransmisikan. *Packet loss* dapat terjadi karena adanya kemacetan pada saluran transmisi akibat padatnya *traffic*. Perhitungan *packet loss* dapat dilihat pada

persamaan 2.4 [25]. Untuk menentukan klasifikasi nilai *packet loss* yang didapat dapat berpatokan pada standarisasi TIPHON seperti yang terlihat pada table 2.5.

$$Packet\ loss = \frac{paket\ data\ yang\ dikirim - paket\ data\ yang\ diterima}{paket\ data\ yang\ dikirim} \text{ x } 100\% \quad \textbf{(2.4)}$$

Tabel 2.5 Kategori *packet loss*

Kategori	*Packet loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1