# BAB 1
# PENDAHULUAN

## 1.1 LATAR BELAKANG

*Software Defined Wide Area Network* (SDWAN) merupakan bentuk aplikasi dari teknologi SDN yang diterapkan pada jaringan *Wide Area Network* (WAN). Jaringan WAN dapat menghubungkan beberapa jaringan lokal dengan jarak geografis yang cukup jauh. Penerapan teknologi SDN-WAN bermaksud untuk melakukan kontrol perpindahan jalur jaringan dengan area yang luas pada proses transfer paket data dengan pendekatan berbasis *Software* [1].

Namun, *link* koneksi dari penyedia jasa layanan *internet* terkadang mengalami kendala yang dapat menyebabkan terputusnya koneksi *internet* yang digunakan. Terputusnya koneksi pada jaringan dapat diakibatkan oleh kegagalan perangkat dan kegagalan *link*. Kegagalan perangkat jaringan berarti perangkat atau hardware yang digunakan pada jaringan mengalami masalah sehingga menyebabkan perangkat *router* tidak dapat meneruskan paket [2]. Apabila hanya terdapat satu *link internet* akan menyebabkan setiap perangkat *user* pada jaringan tidak dapat berkomunikasi.

Oleh karena itu, dibutuhkan solusi agar layanan *internet* dapat memberikan konektivitas yang berkelanjutan meski terkendala oleh gangguan pada jalur koneksinya. Salah satu solusinya yaitu dengan menambahkan jalur (*link*) *redundancy* yang digunakan untuk meningkatkan *reliability*. Kedua *link* tersebut diintegrasikan pada metode *failover*.

Pada *failover*, *Router* akan terbagi menjadi *Router* Utama dan *router* yang lain akan digunakan sebagai *Router* cadangan atau *Router Backup* untuk mengantisipasi apabila *router* utama mengalami gangguan. Ketika *router* utama Kembali normal, *router* utama akan kembali digunakan untuk terhubung ke *internet*. Protokol yang digunakan pada *failover* yaiu *Virtual Router Redundancy Protocol* (VRRP) dan *Hot standby router Protocol* (HSRP) yang termasuk kedalam protokol *First Hop Redundancy Protocol* (FHRP) [3].

Keuntungan dari metode *failover* adalah memiliki ketersediaan lebih tinggi tanpa harus melakukan konfigurasi ulang pada perangkat jaringan saat terjadi kegagalan pada *link* atau *router* utama [4]. Protokol VRRP merupakan standar IETF yang memiliki mekanisme *router* redundan untuk meningkatkan *reliability* jaringan. VRRP beroperasi dengan cara menyatukan beberapa *router* yang ada secara bersamaan menjadi sebuah *router* secara *virtual*. Protokol VRRP akan membutuhkan sebuah IP yang akan digunakan pada *virtual router* yang dihasilkan. [5]. Berbeda dengan protokol HSRP yang khusus digunakan pada *router* cisco, protokol VRRP bersifat *open-standard* yang artinya protokol VRRP dapat digunakan oleh banyak vendor [6]. Pada penelitian ini akan membahas mengenai penggunaan protokol VRRP yang dapat digunakan pada berbagai vendor termasuk pada *router* fortigate.

Fortigate merupakan perangkat *firewall* yang digunakan sebagai sistem keamanan. Fortigate diluncurkan oleh perusahaan yang bernama Fortinet. Fortigate berfungsi sebagai perangkat keamanan jaringan secara keseluruhan serta dapat berperan sebagai *gateway* dan *router* dari suatu jaringan LAN sehingga tak dibutuhkan lagi *router* ataupun perangkat tambahan load *balancing* apabila terdapat lebih dari satu koneksi WAN [7]. Dengan demikian, fortigate dapat memanfaatkan protokol VRRP yang menggunakan dua buah jalur komunikasi atau lebih.

Berdasarkan permasalahan di atas, maka penulis mengambil judul **"ANALISA *FAILOVER* PADA SDWAN MENGGUNAKAN PROTOKOL *VIRTUAL ROUTER REDUNDANCY PROTOCOL* (VRRP)"** sebagai tugas akhir.

## 1.2 RUMUSAN MASALAH

Rumusan masalah yang perlu dikaji lebih lanjut dari penelitian ini yaitu:

1) Bagaimana rancangan arsitektur SD-WAN pada Pnetlab dan mensimulasikan metode *failover* menggunakan protokol VRRP ?
2) Bagaimana performansi metode *failover* pada SD-WAN menggunakan protokol VRRP ?
3) Bagaimana performansi QoS yang diperoleh dari simulasi *failover* pada SD-WAN menggunakan protokol VRRP ?

## 1.3 BATASAN MASALAH

Beberapa batasan masalah dari penelitian ini adalah:

1) Implementasi metode *failover* menggunakan *protocol* VRRP
2) Implementasi *router* SD-WAN menggunakan fortigate
3) Penelitian hanya membahas metode *failover* pada *router* SD-WAN
4) Implementasi menggunakan dua buah *link* komunikasi
5) Penelitian menggunakan Pnetlab pada VMWare
6) Penelitian tidak membahas mengenai keamanan jaringan
7) Untuk parameter pengujian menggunakan nilai QoS dan *time response failover*

## 1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Mengetahui cara merancarng arsitektur SD-WAN pada Pnetlab dan mensimulasikan metode *failover* menggunakan protokol VRRP.
2) Mengetahui performansi metode *failover* pada SD-WAN menggunakan protokol VRRP.
3) Mengetahui performansi QoS yang diperoleh dari simulasi *failover* pada SD-WAN menggunakan protokol VRRP.

## 1.5 MANFAAT

Manfaat dari penelitian ini adalah untuk mengetahui penggunaan metode *failover* menggunakan protokol VRRP pada jaringan SD-WAN untuk meningkatkan *High Availability* jaringan.

## 1.6 SISTEMATIKA PENULISAN

Sistematika penulisan ini dibagi menjadi 3 bagian:

1. BAB I : PENDAHULUAN

   Bab 1 membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan.

2. BAB II : DASAR TEORI

Bab 2 merupakan dasar teori, berisi kajian pustaka dari penelitian sebelumnya serta teori yang akan dijadikan refrensi penulis untuk menyusun penelitian ini seperti konsep SDWAN, protokol VRRP dan materi pendukung lainnya.

3. BAB III : METODE PENELITIAN

   Pada bab 3 membahas mengenai cara penelitian yang mencangkup *hardware* dan *software* yang digunakan, topologi yang digunakan, spesifikasi perangkat yang digunakan dan diagram alur penelitian.

4. BAB IV

   Pada bab 4 menjabarkan tentang hasil data yang didapatkan serta analisa yang didapatkan berdasarkan data yang dihasilkan pada proses simulasi.

5. BAB V

   Pada bab 5 berisi kesimpulan hasil penelitian serta berisi saran untuk pengembangan tesis kedepannya.