BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat pesat dengan beragamnya teknologi informasi yang disematkan sangat mempengaruhi pola bisnis dan strategi bisnis perusahaan terutama komunikasi data yang menjadi kebutuhan utama bagi sebuah perusahaan saat ini. Adapun menurut Munir (2010) bahwa teknologi informasi dan komunikasi meliputi berbagai aspek yang melibatkan teknologi, rekayasa dan teknik pengelolaan yang digunakan dalam pengendalian dan pemrosesan informasi serta penggunaannya, komputer dan hubungan mesin (komputer) dan manusia, dan hal yang berkaitan dengan sosial, ekonomi dan kebudayaan. Penggunaan akan komunikasi data tentu tidak hanya sebatas area lokal saja, namun perusahaan cenderung mempunyai banyak area-area kantor cabang yang tersebar di lokasi tertentu.

Virtual Private Network (VPN) merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengoneksikan kantor pusat, kantor cabang dan lain-lain menggunakan infrastruktur telekomunikasi dan metode enkripsi (Kevin, 2001). Teknologi infrastuktur *WAN* seperti *X.25*, *ATM* dan *Frame Relay* memberikan jalur transmisi antar berbagai lokasi. Meskipun *ATM* merupakan teknologi terbaru yang memberikan *Throughput* tinggi dan sedikit *delay* akan tetapi meminimalisirkan *flow* dan *error controls*-nya sehingga tidak sedikit terjadi *overload*. sedangkan *flow* dan *error controls* pada *X.25* terdapat pada *link-to-link* berdampak *overload* yang tinggi dan *Frame Relay* terdapat pada *end-to-end* berdampak *overload* yang sedang. Jaringan *ATM* dan *Frame relay* lebih efisien daripada *X.25* berdasarkan kehandalan, kualitas dan menyediakan *multiprotocol* (Mir & Sharma, 2014). Adapun kekurangan ketiga teknologi *WAN* tersebut yaitu tidak adanya suatu pengelolaan *Quality of Service (QoS)* dan saat ini digantikan sebagian besar oleh *MPLS VPN* dimana aplikasi seperti *ERP*, *Citrix*, *RDP*, *VoIP* dan video yang membutuhkan kualitas yang handal.

Dalam memenuhi kebutuhan komunikasi *VPN* yang menggunakan *MPLS VPN* sebagai media *WAN* tersebut, terkadang kegagalan sebuah konektifitas jaringan tidak dapat diperhitungkan waktu terjadinya ketika berhadapan dengan *hardware* jaringan dan kondisi alam. Redundansi pada *VPN* merupakan bentuk kesiagaan perusahaan dalam ketersediaan komunikasi antara area dengan mekanisme pergantian secara otomatis dari jalur utama ke jalur cadangan. Menurut Ahmed, Fathi, & Ashibani (2017), dalam memilih teknologi *VPN* secara *site-to-site* ada beberapa unsur penting yang disarankan untuk mendekati solusi kebutuhan perusahaan yaitu dengan mengetahui parameter-parameter sebagai berikut; *QoS requirement*, *Topology requirement*, *Security requirement* dan *Protocol support requirement*.

Berbagai solusi yang diperkenalkan dalam menyediakan *VPN* cadangan, antara lain teknologi infrastruktur *WAN* yaitu *MPLS VPN* dengan seluruh kelebihannya dan protokol *VPN* seperti *PPTP*, *L2TP*, *OpenVPN*, *DMVPN* dan *GETVPN*. Permasalahan dalam memilih teknologi *VPN* adalah bagaimana membangun redundansi dan tidak memerlukan penambahan infrastruktur baru, melainkan dapat memanfaatkan jalur *Internet* dengan mekanisme *routing distribution* agar dapat berpindah otomatis ke *VPN* cadangan. Berdasarkan relevansi masalah tersebut, *MPLS VPN* belum memberikan solusi dengan memanfaatkan infrastruktur *WAN* publik yang mana *MPLS* hanya menyediakan *WAN* tersendiri serta perusahaan juga memerlukan penambahan infrastruktur baru tanpa memanfaatkan sumber daya yang ada (Gupta & Singh, 2016). Sedangkan protokol *VPN* yang telah disebutkan, juga belum dapat mendukung mekanisme *routing distribution* agar dapat berpindah otomatis dari *VPN* utama. Berbeda dengan *DMVPN* dan *GETVPN* yang dapat mendukung kedua kekurangan tersebut, perbedaan dari teknologi ini adalah *DMVPN* dapat diimplementasikan pada *WAN* publik sedangkan *GETVPN* tidak dapat diimplementasikan (Cisco, 2017). *DMVPN* merupakan solusi yang dapat memberikan jawaban dari permasalahan dengan *tunneling* melalui *internet* menggunakan *mGRE* (*Multipoint Generic Routing Encapsulation*), performa komunikasi data pada *QoS application* yang handal, mendukung kecepatan pengiriman data yang aman dengan enkripsi *IPSec* yang

lebih cepat dibandingkan menggunakan *SSL*, dan menyesuaikan protokol yang ada di perusahaan seperti *routing protocol* dan *TCP/IP* agar dapat melakukan perpindahan ke *VPN* cadangan secara otomatis (Cisco, 2017). Sehingga, dalam perancangan *VPN* cadangan dari studi kasus *fail connection* dan mendukung *QoS application* yang memanfaatkan infrastuktur *Internet* sebagai medianya adalah teknologi *DMVPN*.

1.2 Perumusan Masalah

Identifikasi permasalahan dalam penelitian ini adalah jaringan perusahaan yang memerlukan komunikasi data antara dua area di berbagai lokasi yang hanya memerlukan konektifitas VPN yang handal secara redudansi dari VPN utama tanpa membangun infrastruktur baru. Beberapa solusi teknologi infrastuktur WAN dan protokol VPN belum dapat merelevansikan permasalahan pada studi kasus tersebut. DMVPN dengan mekanisme routing distribution dapat membangun jaringan VPN multiples sites memanfaatkan WAN publik sebagai VPN cadangan, didukung dengan hub and spoke, menyematkan topologi full mesh, dan dapat memberikan enkripsi komunikasi data ketika melalui jalur Internet tersebut. Pada penelitian ini, juga melakukan pengamatan dari pengaruh pergantian *VPN* utama ke *VPN* cadangan, yang mana tujuannya melihat kualitas parameter *QoS* menurut standar internasional *ITU-T G.411*.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Topologi jaringan yang disimulasikan merupakan skala kecil (*testlab*), dengan menggunakan 5 buah cisco *router* dan 1 buah cisco *ethernet switch* yang dibangun dengan skenario *site-to-site VPN*.
2. Perancangan jaringan *failover VPN* dirancang serelevan mungkin terhadap gambaran umum dari studi kasus, yakni kantor pusat dan kantor cabang

yang konektifitasnya diasumsikan *VPN* utama terhubung dengan jaringan *MPLS-L3VPN* dan infrastruktur lainnya adalah *Internet* sebagai implementasi *DMVPN*.

3. Penerapan protokol *routing* yang disimulasikan tidak berhubungan dengan jaringan riil perusahaan, namun mereferensikan pada penelitian sebelumnya.
4. Pengambilan data analisis kualitas QoS hanya mengacu pada *delay*, *jitter*, *packet loss* dan *throughput* yang sesuai standarisasi ITU-T G.114.

1.4 Tujuan

Tujuan pada penelitian ini adalah sebagai berikut:

1. Merancang *site-to-site VPN* pada simulasi dari kantor pusat ke kantor cabang melalui *Internet*, tanpa membangun infrastruktur baru dengan menggunakan *DMVPN*.
2. Menguji dan menganalisis tingkat pengaruh kualitas QoS ketika proses *failover VPN* berlangsung pada suatu transfer data *ICMP* dan hasil Video *streaming* sebagai salah satu solusi *VPN over internet*.

1.5 Manfaat Penelitian

Dengan dilaksanakan penelitian akan diperoleh sebagai berikut:

1. Memudahkan pengguna/perusahaan dalam komunikasi data dari kantor pusat ke kantor cabang dengan menggunakan infrastruktur *internet* yang handal.
2. Memudahkan perusahaan dalam mengetahui hasil penggunaan *DMVPN* melalui *internet* sebagai *VPN* cadangan.
3. Mendapatkan informasi dari hasil analisis kualitas *QoS* dari perancangan sistem *failover* secara *real time*.

1.6 Sistematika Penulisan

Dalam penulisan skripsi ini, untuk memudahkan dalam hal penyusunan, penulis membaginya ke dalam beberapa bab. Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang pelaksanaan penelitian secara umum. Pada bab ini akan dijelaskan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab ini berisi tinjauan terhadap penelitian-penelitian yang sudah dilakukan dan teori-teori yang berkaitan dengan topik yang sedang diteliti sebagai bahan acuan dalam melakukan penelitian. Dalam bab ini dijelaskan mengenai teori – teori secara umum mengenai dasar jaringan dan teori khusus yang berkaitan dengan sistem yang dibangun.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai metode penelitian yang digunakan untuk mewujudkan skenario *failover VPN over Internet*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi penjelasan mengenai hasil yang dicapai setelah mengimplementasikan skenario *failover VPN over Internet* dan pembahasan di dalamnya.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi penjelasan mengenai kesimpulan dari sistem yang dibangun dan saran yang didapat dari hasil penelitian dimana saran tersebut dapat digunakan untuk pengembangan fitur – fitur *failover VPN over Internet* lainnya.