

BAB V

KESIMPULAN DAN SARAN

1.1 Kesimpulan

Berdasarkan hasil implementasi dan analisis pengujian yang dilakukan, sehingga dapat disimpulkan sebagai berikut:

1. Hasil Pengujian simulasi *failover connection* secara *real time* menunjukkan status berhasil dari skenario *MPLS-L3VPN* menuju ke rute *DMVPN* yang diterapkan dalam membangun *VPN* cadangan tanpa membangun infrastruktur baru.
2. Pada Parameter *QoS (Quality of Services)* yang terdiri dari *throughput*, *delay*, *jitter* dan *packet loss* menurut ITU-T G.114:
 - a. *Delay* pada pengujian memiliki nilai yang sangat baik di bawah standar yaitu *150 ms*, selain itu skenario *Failover Process* mendapatkan kenaikan nilai *delay* sebesar *40,8 ms* yang sebelumnya *8,7 ms* pada skenario *MPLS-L3VPN* sedangkan skenario *DMVPN* nilai yang didapatkan *36,9 ms*.
 - b. *Jitter* pada pengujian memiliki nilai yang sangat baik juga yaitu di bawah *20 ms* sesuai standar *ITU*, terlihat pada hasil yang didapatkan pada skenario *MPLS-L3VPN*, *Failover Process* dan *DMVPN* yaitu *0,0208 ms*, *0,0307 ms* dan *0,0263 ms*.
 - c. *Packet loss* pada pengujian memiliki nilai yang sangat baik dari maksimal yang direkomendasikan yaitu $<0.5\%$, sedangkan nilai terbesar pada pengujian adalah pada skenario *Failover Process* sebesar *0,3%* dan kedua skenario lainnya mendapatkan nilai sama sebesar *0,2%*.
 - d. Parameter terakhir yaitu *Throughput* dengan total jumlah *bit* paket yang berhasil diterima, nilai terbesar pada hasil pengujian adalah skenario *MPLS-L3VPN* sebesar *339 bps*, skenario *DMVPN*

sebesar 293,8 *bps* dan skenario *Failover Proccess* sebesar 212,5 *bps*.

3. Perbedaan kualitas *QoS* yang didapatkan oleh *MPLS* lebih baik daripada *DMVPN*, disebabkan *IPSec* yang belum diimplementasikan pada *MPLS-L3VPN* sedangkan *DMVPN* diterapkan. Merferensikan pada penelitian sebelumnya yaitu *MPLS* dengan mengimplementasikan *IPSec* akan menurunkan performa terhadap *VoIP application* (Bensalah, El Kamoun, & Bahnasse, 2017), serta *DMVPN* dengan *IPSec* menyebabkan latensi dan penurunan kualitas *VoIP application* selama pembentukan *tunnel DMVPN* (Bahnasse & El Kamoun, 2017).

1.2 Saran

Berdasarkan permasalahan dan pembangunan *failover VPN* peneliti memiliki beberapa saran untuk disampaikan antara lain:

1. Pada pengujian selanjutnya dalam menganalisis performa *DMVPN*, peneliti memberikan saran dalam menganalisis *QoS* untuk *VoIP* dan aplikasi *real-time* lainnya
2. Diharapkan simulasi selanjutnya dilakukan terhadap perangkat nyata atau dapat di uji coba ke dalam jaringan *WAN* publik pada studi kasus ke perusahaan.
3. Peneliti merekomendasikan *pentesting* terhadap *IPSec DMVPN* terkait kriptografi yang di integrasikannya, sehingga *administrator* dapat menentukan dan mengevaluasi konfigurasi enkripsi maupun menanggulangi resiko terjadi pencurian data.