# ABSTRAK

Saat ini jaringan komputer telah menjadi bagian yang tidak terpisahkan dalam dunia telekomunikasi. Banyak perusahaan menggunakan jaringan komputer ini untuk dapat berkomunikasi dan bertukar data dengan perusahaan cabang, perusahaan mitra maupun dengan pegawainya yang sedang ada di lapangan. Dahulu perusahaan menggunakan saluran berbasis *leased lines* atau sirkit frame relay untuk menghubungkan kantor pusat dengan kantor cabang yang ada. Hal tersebut tidak efisien dan fleksibel lagi saat ini mengingat biaya yang harus dikeluarkan yang cukup mahal untuk menyewa saluran *leased lines* dan pengaksesan hanya bisa dilakukan dari jaringan tertutup tersebut, sehingga menyulitkan *user* yang *mobile*.

*Virtual Private Network* menjadi solusi tepat untuk memecahkan masalah tersebut. VPN memungkinkan untuk membangun komunikasi melalui jaringan publik seolah-olah berkomunikasi dalam suatu jaringan *private*. Keamanan data terjamin dengan digunakannya enkripsi dan otentikasi. Tugas akhir ini membahas implementasi VPN berbasis L2TP/IPSec, yang didefinisikan dalam standar RFC 3193, yaitu teknologi VPN yang merupakan perpaduan dari L2TP dan IPSec dengan cara mengamankan paket L2TP melalui *tunnel* IPSec. Implementasi dilakukan dengan membangun VPN *server* dan Radius *server* yang terintegrasi untuk menangani otentikasi *user*. Analisis dilakukan untuk mengukur waktu yang diperlukan untuk *tunnel setup* dan performansi pada penggunaan aplikasi *file transfer protocol.*

Dari hasil pengukuran diperoleh hasil *tunnel setup delay* L2TP/IPSec untuk *pre shared key* rata-rata sebesar 2,123 detik dan 2,162 detik untuk *certificate.* Pada penggunaan VPN akan ditambahkan *header* sebesar minimal 104 byte dan maksimal 356 byte dibandingkan pada pengiriman normal yang hanya 40 byte. Penambahan *header* dan *delay processing* enkripsi dan otentikasi menyebabkan penurunan performansi dari segi *delay, packet loss dan throughputnya.* Penggunaan AES memberikan performansi yang lebih tinggi daripada 3DES, sedangkan performansi yang bagus diperoleh HMAC-MD5 di saat *background traffic* kecil dan HMAC-SHA-1 pada *background traffic* besar.

Kata kunci : VPN, L2TP, IPSec, L2TP/IPSec, Radius