# Abstrak

Meningkatnya kebutuhan alamat IP mendorong adanya migrasi dari IPv4 ke IPv6. Berbagai pengujian dilakukan dengan tujuan tidak ada kendala dalam migrasi, terutama masalah performansi jaringan dan keamanan jaringan. VPN merupakan suatu metode untuk mengamankan paket data yang melewati jaringan publik. *Protocol* yang digunakan dalam implementasi *Virtual Private Network (VPN)* ini adalah *protocol IP Security (IPSec)* yang bekerja di *layer network*. IPSec memiliki dua buah *mode* dalam implementasinya, yaitu *transport mode* dan *tunnel mode*. *Tunnel mode* dapat diimplementasikan untuk membangun VPN *host to host* dan *gateway to gateway*. Sedangkan *transport mode* hanya dapat diimplementasikan untuk membangun VPN *host to host*. *Protocol IPSec* memiliki dua buah *security protocol* yaitu *Authentication Header (AH)* dan *Encapsulation Security Payload (ESP)* yang bisa digunakan.

Setiap protokol yang digunakan memiliki panjang header yang berbeda sesuai dengan fungsinya untuk enkapsulasi paket data. Semakin panjang *header* protokol yang mengenkapsulasi suatu paket data dan semakin besarnya proses komputasi untuk melakukan enkripsi dan otentikasi, maka waktu yang dibutuhkan semakin bertambah. Hal ini mempengaruhi performansi suatu jaringan dengan menurunnya nilai *throughput*.

**Kata kunci :** IPv4, IPv6, VPN, IPsec, *Tunnel mode, Transport mode.*