# ABSTRAK

Semakin tingginya kebutuhan akan jaringan internet membuat terjadinya pengembangan untuk jaringan internet. Diantaranya *high speed internet access* dan *secure network*. Jaringan dengan tingkat keamanan yang tinggipun menjadi suatu keharusan untuk diperhatikan, kebocoran informasi data yang dilewatkan melalui jaringan adalah hal yang sangat dihindari, sehingga dapat disimpulkan akses internet cepat juga sangat membutuhkan kamanan jaringan yang memadai. MPLS (*Multi Protocol Label Switching*) adalah suatu metode *forwarding* yang mempersingkat waktu pembacaan *destination address* paket sehingga paket lebih cepat diteruskan ke *hop* selanjutnya. Karena itulah muncul juga MPLS VPN, dengan mengandalkan skalabilitas dan *traffic engineering* sebagai keamanan sisi *confidentiality*[10]. Bagaimana dengan informasi sistem peroutingan, maka kita dapat menggunakan *Routing Protocol Authentication* yang merupakan metode autentikasi yang dibuat untuk memberikan autentikasi pada tiap informasi *routing* yang berada di dalam paket. Sehingga mencegah adanya serangan pada paket informasi peroutingan[2].

Pada tugas akhir ini akan dibahas masalah keamanan pada sisi *integrity* dari *man-in-the-middle-attack*, menggunakan sistem autentikasi di setiap *peer* MPLS, dengan menggunakan teknologi *Routing Protocol authentication*.

Dari pengujian dapat disimpulkan bahwa informasi peroutingan sangat mudah untuk didapatkan sehingga membutuhkan autentikasi pada tiap *header*-nya yang kemudian dienkripsi dengan fungsi *hash* MD5. Dengan adanya autentikasi ini dibutuhkan waktu untuk melakukan *cracking* agar dapat mengirim paket *spoof* dari penyerang ke arah router sehingga penyerang dikenali sebagai bagian dari jaringan yang seharusnya. Dan MD5 sendiri masih mampu untuk melindungi paket, dengan menggunakan *key* atau *password* yang kuat dan dijaga kerahasiaannya.

**Kata Kunci :** MPLS, *routing protocol authentication, man-in-the-middle,* MPLSVPN.