

## ABSTRACT

Currently computer networks have become an integral part in the world of telecommunications. Many companies use computer networks to communicate and exchange data with corporate branches, corporate partners or by employees who were there in the field. Using channel-based company formerly leased lines or frame relay circuits to connect the central office with branch offices there. It is not efficient and flexible again today considering the cost is quite expensive to rent a channel leased lines and access can only be done from a closed network, so difficult that a mobile user. Virtual Private Network to be the right solution to solve the problem. VPN allows to establish communication over a public network as if communicating in a private network. Data security is assured by the use of encryption and authentication. This final project implementation TLS based VPN L2TP, which VPN technology is a fusion of technology TLS VPN site-to-site transport which secures the session using a L2TP protocol.

Implementation is done by building a VPN server and the VoIP server. Analysis is performed to determine the effect of the use of VPN to the performance of VoIP services and the effect on some kinds of attacks against performance on the VoIP service. Service used is the VoIP service.

From the measurement results obtained by the L2TP tunnel setup delay by an average of 2.035 seconds for authentication using an SSL certificate. On the use of a VPN will add the header for a minimum of 104 bytes and a maximum of 356 bytes compared to the normal shipping is only 40 bytes. The addition of headers and encryption and authentication processing delay causes a decrease in the performance of VoIP in terms of delay, packet loss, jitter and throughput. The use of AES provides higher performance than 3DES. From the security test result obtained that the system is secure based on 3 aspect, confidentiality, integrity, and availability.

Key words: VPN, TLS/SSL, L2TP, QoS.