ABSTRACT

Virtual Private Network (VPN), developed at large companies expanding their business network, but they still want to be able to connect local networks (private) between branches with its business partners who are in distant places. The company also wanted to provide facilities for their employees that wants to connect to local networks of their companies for data exchange from everywhere.

Virtual Private Network becomes the right solutions to solve the problem. VPN allows to establish communication through the public network, viewed seems to communicate in a private network. Security assured with the use of data encryption and authentication. This final project discuss the implementation of L2TP/IPSec VPN, which is defined in RFC 3193 standard, a VPN technology which is a combination of L2TP and IPSec, securing the L2TP packet over IPSec tunnel. And the applications that passed are video and voice communications that was supported by QoS guarantees with DiffServ (Differentiated Service). Implementation is done by building a VPN server and Radius server that integrated to handle user authentication also building router that support DiffServ by using Mikrotik. Analysis was done to measure the time needed for tunnel setup and performance when using VoIP communication applications.

From the measurement results obtained by the tunnel setup delay L2TP/IPSec pre shared key for an average of 2.1119 seconds and 2.3207 seconds for the certificate. By using of a VPN will cause a decrease in performance in terms of delay, packet loss and throughput due to additional header. Use of DiffServ capable of providing higher performance than without using Diffserv with improvements packet loss from 78.096% to 0.94%, throughput from 18145 bps to 85064 bps and delay from 81 ms to 20.1 ms at maximum background traffic.

Keywords: VPN, L2TP/IPSec, Radius, DiffServ