ABSTRACT

The development of technology today has forced all of the elements of life to adapt to the technology, including the business sector. In the development of the business, it is not impossible to make company expansion. Along with the emergence of Internet technology at a cost that is affordable enough, it takes a technology that can guarantee the confidentiality of the data communication done. Therefore, there is a concept of a Virtual Private Network to meet those needs.

In the implementation, there are some Virtual Private Network technologies, such as PPTP, L2TP, IPsec, and several other methods. In this implementation and analysis study, IPsec method is chosen because it has a security framework that can be modified according to the desired security requirements. In addition, IPsec implementation is also much easier than the other protocols, and supports all operating modes. IPsec VPN's method is, applied to ADSL Internet line using Cisco 1841 routers using RFC 1843 Bridge method at Laboratory of Computer Network STTS network, and WIC-1ADSL module on a remote network that is located outside the STTS. Then, it will form an IPsec tunnel between the two networks. The test performed on a combination of the methods of encryption and hash which provided by the Cisco 1841 Router, such as DES, 3DES, AES, SHA, and MD5. Furthermore, the analysis was also performed to examine the relationship between the numbers of routers on the WAN with a VPN tunnel performance generated. This analysis used a statistical calculation method, the Analysis of Variance (ANOVA) and linear regression.

With this analysis study, some facts generated by statistical calculations are obtained. VPN performance is affected by the encryption method used, and the amount involved in the WAN router. In addition, the VPN degrade network performance by 44.4% from normal tissue. With a low enough cost, VPN is more feasible to be applied to small and medium enterprises.