

## ABSTRACT

*The hub and spoke architecture used by FlexVPN is one of the wide area network applications, making it prone to high delays and packet loss. FlexVPN uses IPsec tunneling so that it will have an impact on the resulting quality of service because it adds to the process on the router in the form of increasing the packet size sent for the encryption process. The addition of MPLS can be used as a solution because it can reduce the router's workload by streamlining the forwarding of each packet. This can happen because the working system inserts labels on IP packets so it doesn't read the routing table to send each packet. This study designed a FlexVPN over MPLS network model with tests involving file transfer services using the TCP and UDP transport protocols. The file sizes used include 20 MB, 40 MB, and 80 MB with the ISO file format. The TCP measurement results obtained the smallest delay of 0,526 ms, the smallest jitter of 0,021 ms, 0% packet loss, and the highest throughput of 14,45 Mbps. UDP measurements obtained the smallest delay of 1,182 ms, the smallest jitter of 0,006 ms, 0% packet loss, and the highest throughput of 2,042 Mbps. The conclusion is that the effect of the FlexVPN over MPLS network on file transfer services produces a better quality of service for the use of the transport protocol. rather than UDP which is connectionless.ng is connection oriented, namely TCP rather than UDP which is connectionless.*

**Keywords:** WAN, Hub and Spoke, FlexVPN, MPLS, TCP, UDP, QoS