Abstract

*Increasing needs of IP address urges to do migration proccess from IPv4 to IPv6. Hopefully, many testing are done in the migration will not get barrier especially network performance. Besides that, the network security becomes the main point in data communication problem. Virtual Private Network (*VPN*) is a method to make secure data packages which pass public network. Protocol which is used in this* VPN *implementation is IP Security protocol (IPSec) which works in network layer. IPSec has two modes in this implementation, transport mode and tunnel mode. Tunnel mode can be implemented for building* VPN *connection between host to host although among gateway to gateway. Whereas transport mode just can be implemented for building connection between host to host. IPSec Protocol has two security protocol such as Authentication Header (AH) and Encapsulation Security Payload (ESP) which can be used.*

Every protocol have their own length for different purpose in encapsulation data. The more length a header which encapsulate a packet data, and the more complex an encryption algorithm and authentication algorithm, it takes more time to process it. This will decrease the quality of network quality performance.

Keywords: IPv4, IPv6, VPN, *IP Security, Tunnel mode, Transport mode.*