ABSTRACT

The network architecture currently more widely used is the traditional network architecture that uses interconnection media such as switches or hubs to connect devices connected into a network. This architecture has limitations in handling large network scalability and data traffic density. In addition, conventional networks are less effective when used to develop network controller applications. Therefore, a new network architecture was created, namely, Software Defined Networking (SDN) as a form of meeting user needs to overcome these limitations by separating the control plane and data plane. In SDN there is a firewall called multi-tenancy, which is an architectural pattern that runs on the service provider's infrastructure. One of the features of SDN is network slicing which allows the separation of the network into several slices with resource isolation. This research aims to analyze the application of network slicing using FlowVisor in enforcing CPU switch isolation in Software Defined Networking (SDN) networks by implementing the OpenFlow protocol and POX controller. This research was conducted by simulating the network topology using Mininet. Several test scenarios were performed in this study, namely connectivity test, functionality test, resource utilization test, and measuring Quality of Services based on throughput, packet loss, delay, and jitter parameters with or without FlowVisor. The results showed that CPU and memory usage increased when FlowVisor was enabled, with a comparison of CPU usage without FlowVisor reaching 32.23% and using FlowVisor reaching 34.00%. Memory usage without FlowVisor reached 480% and using FlowVisor reached 560%. The tests conducted prove that FlowVisor in CPU switch isolation successfully separates resources between slices without disrupting the Quality of Services performance. However, there is an increase in CPU and memory usage when FlowVisor is enabled.

Keywords— network slicing, Software Defined Network (SDN), FlowVisor, Quality of Services (QoS)