ABSTRACT

To be able to communicate to a computer network, every host on the network must have an IP address. One of those method is using DHCP protocol. DHCP protocol allows client to get an IP address from DHCP server automatically. But, basically DHCP doesn't have any security function to prevent attacking activity on a network. One of this attacking activity is the presence of unauthorized DHCP server who give IP addresses to clients of a service. DHCP Snooping, which usually found on Layer 2 devices, can be used as an alternative security method to overcome this kind of attacking activity.

In this study, DHCP Snooping is used to prevent an unauthorized DHCP server from giving IP addresses to clients of a service. The reliability of proposed method is tested by various scenarios. From each scenario, there will be some output parameter such as the percentage IP allocation of authorized server, elapsed time, response time, and throughput.

The result shows that DHCP Snooping can be used as an alternative security function to prevent the presence of unauthorized server on a system. DHCP Snooping improves IP allocation from legal server up to 81%. But, it works perfectly when the number of clients are less or equal to 300. The use of DHCP Snooping in this study increases Elapsed Time by 34% and Response Time increase significantly. The use of DHCP Snooping in this study also affects the Throughput by giving 89% decrement.

Keywords: *DHCP Snooping, Elapsed Time, illegal server, IP allocation, Response Time*