Introduction

Currently, business processes in many companies have used information technology, especially in computer networks. The company also utilizes a computer network with secure features and consistently maintains high network availability to keep its business processes running. Large companies, especially those with many branches, use a Virtual Private Network (VPN) to maintain network security, especially aspects of confidentiality, data integrity, and origin authentication. However, the VPN being used is still a regular VPN that requires configuration and maintenance costs that are quite high. To that end, Cisco introduces Dynamic Multipoint Virtual Private Network (DMVPN) technology that companies can use to communicate and transfer secure data between branch offices and the central office [1].

DMVPN is a VPN design concept that combines technologies such as Multipoint Generic Routing Encapsulation (mGRE), Next Hop Resolution Protocol (NHRP), IPSec Encryption [2]. DMVPN has advantages compared to regular VPN, which is that regular VPN has complex configurations where an administrator needs to configure each site-to-site individually, and if there is a new site added, the configuration needs to be added as well. With DMVPN, if a site is added, the configuration is only done on the newly added site. For this reason, DMVPN technology is suitable for companies that frequently increase the number of branch offices because it can increase flexibility, reduce configuration complexity and reduce operational and maintenance costs. In DMVPN it is also possible between branch offices to communicate without having to go through the HUB Server.

In addition to the confidentiality, data integrity, and origin authentication aspects provided by DMVPN, a consistently available network is required to ensure that the ongoing business processes within the company continue to operate. The redundancy method on the device can be a solution for the availability aspect of the network. Network redundancy is a process to ensure network availability on devices with alternative devices in case of network failure. A protocol that can perform redundancy on a computer network is First Hop Redundancy Protocol (FHRP) [3].

FHRP is a computer network protocol designed to handle network failures by providing a redundant link between two routers. The main FHRP protocols that are frequently used are the Virtual Router Redundancy Protocol (VRRP), Hot Standby Redundancy Protocol (HSRP), and Gateway Load Balancing Protocol (GLBP) [3]. VRRP is the IETF standard protocol in RFC 5798 (Obsoletes: RFC 3768) for HSRP and GLBP is a proprietary protocol owned by Cisco [4].

In the research by Alam, Towhidul, et al [5] a secure network design and implementation have been performed using DMVPN with one of the First Hop Redundancy Protocols (FHRP), namely HSRP. Based on this research, it was found that HSRP, as one of the FHRP protocols, can be used in DMVPN networks. Therefore we conducted this research to test and compare the performance of other FHRP protocols, namely VRRP and GLBP on the DMVPN network with the evaluation metric used in this research are network convergence time and Quality of Service (QoS).