

INTISARI

Perkembangan komunikasi data yang disematkan dalam proses aktifitas berbeda lokasi yang aman menjadi kebutuhan utama bagi sebuah perusahaan saat ini. VPN dapat menghubungkan antar area dengan metode enkripsi tertentu sebagai media pengamanannya. Infrastruktur Jaringan VPN tunggal tersebut tidak cukup memberikan redundansi terhadap kegagalan sebuah konektivitas jaringan yang tidak dapat diperhitungkan. Dengan menggunakan teknologi *Dynamic Multipoint Virtual Private Network* sebagai jalur cadangan VPN, perusahaan dapat berkomunikasi secara aman melalui jaringan internet tanpa membangun infrastruktur baru dengan performa baik. Teknologi tersebut dapat memudahkan dalam hal konfigurasi dibandingkan dengan solusi sejenis seperti *X.25*, *Frame Relay* dan *ATM* maupun, solusi dengan protokol VPN seperti *PP2P*, *L2TP*, *GETVPN* dan *OpenVPN*. Dalam memaksimalkan *high availability* komunikasi data perusahaan, diperlukan perancangan sistem redundansi VPN salah satunya menggunakan pemilihan protokol routing otomatis. Perancangan sistem redundansi menggunakan DMVPN dijalankan pada tiga skenario yang berbeda yaitu jaringan MPLS-L3VPN, proses pergantian *route* VPN, dan jaringan DMVPN dengan aplikasi video *conference* sebagai data pengujian menunjukkan perubahan kualitas trafik video lebih besar pada saat proses pergantian VPN, namun untuk *delay* MPLS 6% lebih kecil dari DMVPN sedangkan proses pergantian VPN terjadi kenaikan nilai yang signifikan. Parameter pengujian lainnya seperti *jitter*, *packet loss* dan *throughput* lebih banyak berpengaruh oleh pengukuran *delay*, sehingga diperoleh kesimpulan DMVPN dapat diimplementasikan sebagai redundansi dari MPLS-L3VPN dengan sistem pemilihan routing protocol pada skala jaringan *medium-enterprise*.

Kata kunci: Redundansi, VPN, Internet, *Routing Protocol*, DMVPN, MPLS-L3VPN

ABSTRACT

The development of data communication embedded in the process of different secure location activities is a major requirement for a company today. VPN can connect between areas with certain encryption methods as a secure medium. The single VPN network infrastructure is not enough to provide redundancy for the failure of network connectivity that cannot be calculated. By using Dynamic Multipoint Virtual Private Network technology as a VPN backup path, companies can communicate securely through the internet network without building new infrastructure with good performance. It can simplify configuration compared to similar solutions such as X.25, Frame Relay, and ATM as well as another solution with VPN protocols such as PP2P, L2TP, GETVPN, and OpenVPN. In maximizing the high availability of enterprise data communications, a VPN redundancy system design is needed, one of which uses automatic routing protocol selection. The redundancy system design using DMVPN is run on three different scenarios, namely MPLS-L3VPN network, VPN route change process, and DMVPN network with video conference application as testing data shows the change in video traffic quality is greater during the VPN change process, but for MPLS delay 6 % is smaller than DMVPN while the VPN turnover process has a significant increase in value. Other testing parameters such as jitter, *packet* loss, and throughput are more influential by delay measurement so that the conclusion of DMVPN can be implemented as a redundancy from MPLS-L3VPN with the routing protocol selection system on a medium-enterprise network scale.

Keywords: Redundancy, VPN, Internet, Routing Protocol, DMVPN, MPLS-L3VPN

