

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan zaman teknologi informasi dan telekomunikasi maka semakin banyak kebutuhan akan kecepatan jaringan internet. Terutama untuk menghubungkan jaringan yang satu dengan jaringan yang lain, dimana kedua tempat jaringan tersebut letaknya saling berjauhan, maka untuk menghubungkan keduanya agar terjadi suatu koneksi yang lebih aman dan efisien maka dibutuhkan teknologi MPLS. Pada penelitian [9] VOIP dengan melakukan tunnelling. Evaluasi dilakukan dengan mengukur kualitas layanan VOIP baik tanpa menggunakan MPLS maupun dengan menggunakan MPLSVPN Berdasarkan hasil penelitian dapat disimpulkan bahwa dengan penerapan VPN pada jaringan MPLS mampu meningkatkan Quality of Service (QoS) protokol routing OSPF pada jaringan VoIP tetapi tidak ada konfigurasi autentikasi. Pada Penelitian [8] VoIP yang dilewatkan melalui jaringan MPLSVPN lebih baik performansi nya daripada trafik VoIP yang dilewatkan melalui jaringan IP biasa. Sehingga kualitas suara yang dihasilkan oleh jaringan VoIP over MPLS lebih baik daripada VoIP dengan jaringan IP biasa. Lalu pada penelitian ini menggunakan *Routing Protocol Authentication* yang merupakan metode autentikasi yang dibuat untuk memberikan autentikasi pada tiap informasi menggunakan MD5 hash function yang dikonfigurasi pada router tetapi algoritma yang digunakan cukup aman tetapi masih bisa terdeteksi dari sisi penyerang karena kunci yang digunakan kurang aman tetapi performansi QOS nya lebih baik. Lalu pada penelitian [2] menganalisis mengenai keamanan VOIP pada jaringan MPLSVPN dengan mengimplementasikan tunnelling Isec namun metode yang digunakan membuat kinerja dari VOIP tersebut menurun. Berikut dibawah ini merupakan tabel perbandingan dari beberapa jurnal yang digunakan untuk penelitian ini :

Tabel 1.1 Perbandingan Studi Literatur MPLSVPN

Jurnal	Penulis	Autentikasi	Tools	Jenis Serangan
[1]	Denny Wijanarko, 2017	X	X	(tidak ada serangan)tetapi memakai MPLSVPN
[2]	Ceisar Maulana Shabirin, 2018	MD5	LOKI	Spoofing & Sniffing
[3]	Andi Taufik Saputra, 2010	IP SEC Tunneling	X	DoS (Denial Of Service)
Penelitian yang di Usulkan	Marina Saraswati	SHA	LOKI, Wireshark	Injection ipv4,Spoofing & Sniffing

Maka dari itu pada penelitian ini akan membahas masalah keamanan jaringan MPLS dari sisi *integrity*. Lalu akan dilakukan simulasi serangan *Injection Ipv4*, *Spoofing*, *Sniffing* pada topologi jaringan yang sudah terkonfigurasi menggunakan *authentication* pada routing protocolnya Dalam penelitian kali ini akan digunakan fungsi Hash Algoritma SHA sebagai autentikasi yang akan dikonfigurasi di tiap header nya.untuk membuktikan apakah kunci yang di enkripsi menggunakan fungsi Hash algoritma SHA dapat menahan dari serangan yang diberikan dan tetap menghasilkan performansi QoS dan kinerja VOIP yang baik.

1.2 Tujuan dan Manfaat

Tujuan dari penelitian ini yaitu antara lain sebagai berikut :

1. Membangun dan menjelaskan cara kerja MPLS-L3 VPN dengan menggunakan routing protocol autentikasi
2. Menjelaskan kinerja jaringan MPLS terhadap layanan VOIP dengan parameter QOS yang diukur Throughput, Delay, Packet Loss, Jitter
3. Melakukan serangan injection ipv4 , spoofing , sniffing pada jaringan MPLS-L3 VPN

Manfaat dari penelitian ini yaitu antara lain sebagai berikut :

4. Memperdalam dan memantapkan penguasaan terhadap ilmu yang telah didapat selama penulis mengikuti *study* di jurusan D3 Teknologi Telekomunikasi
5. Memperkaya wawasan tentang beberapa keilmuan khususnya bagi penulis sendiri umumnya untuk para pembaca

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut.

1. Bagaimana kinerja jaringan mpls-l3vpn tanpa routing protokol autentikasi dan diberi serangan?
2. Bagaimana kinerja jaringan mpls-l3vpn menggunakan routing protokol autentikasi dan di beri serangan?
3. Bagaimana kualitas komunikasi voip yang sudah dilakukan dan menggunakan jaringan mpls-l3vpn yang menggunakan routing protokol ter-autentikasi?

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini, sebagai berikut.

1. Kinerja jaringan MPLS-L3VPN dengan menggunakan Routing Protokol Autentikasi dan Tanpa autentikasi
2. Penggunaan Algoritma SHA sebagai keamanan pada jaringan

3. Membahas serangan Injection ipv4, Spoofing, Sniffing yang di implementasikan pada jaringan
4. Pengujian dilakukan hanya menggunakan jaringan lokal IPv4. dan Routing Protokol OSPF untuk pengujian algoritma SHA
5. Pengukuran kualitas komunikasi VOIP hanya di lakukan pada protocol RTP

1.5 Metodologi

Metode yang digunakan dalam penyelesaian tugas akhir ini sebagai berikut.

a. Metode penelitian

yang digunakan adalah metode eksperimen. Pada penelitian ini akan dilakukan implementasi untuk melihat bagaimana QoS OSPF pada MPLS VPN dengan autentikasi dan tanpa autentikasi pada jalur utama dan jalur backup. Penelitian ini dilakukan dengan menggunakan simulator GNS3

b. Parameter Penelitian

Parameter penelitian ini mengacu pada parameter-parameter yang akan diamati. Parameter-parameter yang diamati yaitu, throughput, delay, jitter, dan packet loss dan uji keamanan pada jaringan

c. Metode Pengumpulan data

Metode pengumpulan data yang digunakan adalah metode observasi, yaitu dengan melakukan pengamatan terhadap hasil implementasi yang berupa grafik maupun tabel yang didapat dari software analisis Wireshark.

d. Metode Analisa

Metode analisa yang digunakan adalah metode perbandingan. Metode perbandingan merupakan kegiatan yang melakukan perbandingan terhadap hasil dari implementasi. Hasil dari implementasi antara jaringan yang menggunakan autentikasi dan tanpa autentikasi.

1.6 Sistematika Penulisan

Dalam penulisan tugas akhir terdiri atas lima bab, dengan keterangan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan proyek akhir, seperti pengertian MPLS L3-VPN, konsep/prinsip kerja MPLS-L3 VPN, prinsip kerja MPLS-L3VPN , jenis – jenis serangan dan lain sebagainya

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Pada bab ini membahas tentang deskripsi tugas akhir, alur pengerjaan tugas akhir, perancangan sistem, serta implemenmtasi dan analisis jaringan MPLS-L3 VPN.

BAB IV SIMULASI DAN ANALISIS

Pada bab ini membahas tentang simulasi dan analisis perencanaan.

BAB V PENUTUP

Pada bab ini membahas tentang kesimpulan dari pengerjaan tugas akhir dan saran untuk pembaca yang akan mengambil penelitian dengan topik yang sama.