BAB I
PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan tekonologi dan komunikasi ini membuat hampir semua kebutuhan manusia menggunakan jaringan internet sebagai sarana bentuk penyampaian informasi. Hal ini disebabkan oleh kemajuan, kehandalan dan ketersediaan pada infrastruktur jaringan dari penyedia jasa layanan jaringan internet yang menjadi penunjang masyarakat untuk dapat berkomunikasi melalui internet. Internet menjadikan berbagai kebutuhan baik dari sisi belajar mengajar, *video conference*, voip, dan sebagainya itu membutuhkan jaringan yang kompleks, dibalik jaringan yang kompleks tentunya ada perancangan khusus agar semua kegiatan tersebut dapat berjalan dengan baik[1].

Seiring semakin meningkatnya jumlah kebutuhan dan pengguna jaringan komputer tentu pengembangan dalam sebuah jaringan pun tidak dapat dihindari. Hadirnya teknologi *Virtual Local Area Network* (VLAN) ini dapat mengatasi keterbatasan sub-*network* pada jaringan komputer tanpa harus memperhatikan lokasi perangkat, di mana VLAN dapat bekerja dengan mengelompokan beberapa *network* dalam satu perangkat yang sama dan juga dengan adanya *port trunk* memungkinkan untuk membawa beberapa VLAN dalam satu *port* yang sama. Vlan *Ttrunking Protocol* (VTP) merupakan sebuah cara yang dilakukan untuk menyebarkan konfigurasi VLAN melalui *port trunk*, di mana dalam penerapan VTP terdapat *switch* yang difungsikan sebagai server dan switch yang digunakan sebagai *client* sebagai penerima dari konfigurasi VLAN.

Namun selain mempermudah pengguna dalam melakukan kegiatan, berbagai bentuk serangan bahkan ancaman baik secara langsung maupun tidak langsung akan memberikan dampak pada aktifitas yang terjadi pada jaringan internet tersebut. Hal yang menjadi rentan terhadap serangan seorang *hacker* bisa menyusup kedalam sebuah sistem karena sebuah sistem mempunyai keamanan yang kurang mumpuni. Seorang penyusup memeliki

beberapa tujuan seperti untuk merubah data, memasukan virus, dapat mencuri data ataupun hanya sekedar unjuk gigi saja, oleh karena itu perlu adanya perlindungan dari sebuah sistem untuk melindungi dari segala macam ancaman yang ada yang umumnya dilakukan secara manual oleh seorang sistem administrator jaringan. Sebuah sistem dapat dikatakan aman apabila hanyak orang-orang yang berwenang saja yang dapat mengakses hal tersebut dan semua data yang ada pada sebuah sistem hanya dapat dikendalikan sepenuhnya oleh orang-orang yang mempunyai hak tersebut[2].

Sebagai bentuk perlindungan dan keamanan dari ancaman seorang *hacker* maupun orang tidak mempunyai wewenang yang dapat menyebabkan kasus kejahatan pencurian data tersebut dapat diterapkan salah satu metode dengan menggunakan *Acces Control List* (ACL), yang berfungsi sebagai pembatasan yang mengizinkan ataupun memblokir antara satu jaringan VLAN satu terhadap jaringan VLAN yang lainya ataupun membatasi hak akses dari jaringan VLAN yang diizinkan atupun tidak diizinkan untuk mengakses jaringan publik (internet)[2][3].

Berdasarkan pemaparan latar belakang di atas, maka dalam penyusunan skripsi penulis melakukan penelitian yang berjudul "ANALISIS PENERAPAN *ACCESS CONTROL LIST* (ACL) SEBAGAI PEMBATASAN HAK AKSES PADA JARINGAN VLAN BERBASIS VLAN *TRUNKING PROTOCOL* (VTP)".

1.2 RUMUSAN MASALAH

1. Bagaimana merancang jaringan *Virtual Local Area Network* (VLAN) berbasis *Vlan Trunking Protocol* (VTP) dengan keamanan *Access Control List* (ACL).
2. Bagaimana perfomansi *Access Control List* (ACL) sebagai pembatasan hak akses terhadap jaringan VLAN satu dengan VLAN yang lainya, jaringan publik (internet) dengan parameter QoS *throughput*, *packet loss*, *dellay* dan *jitter*.

1.3 BATASAN MASALAH

1. Sistem keamanan ini dibuat pada jaringan *Virtual Local Area Network* (VLAN).
2. Teknik perancangan VLAN menggunakan Vlan *Trunking Protocol* (VTP).
3. Menggunakan GNS3 sebagai simulator untuk perancangan jaringan.
4. Menggunakan *router* mikroTik sebagai *core router* dan *gateway* untuk jaringan lokal.
5. Menggunakan Cisco IOU sebagai *multilayerswitch.*
6. Menggunakan OS Ubuntu 18.04 sebagai OS untuk pengujian.
7. Menggunakan Windows versi 7 sebagai sistem operasi untuk client pada VLAN.
8. Menggunakan metode *Access Control List* (ACL) yang digunakan sebagai pembatasan hak akses untuk keamanan jaringan.
9. Melakukan pengujian QoS sebelum dan sesudah ACL diterapkan untuk menentukan perfomansi dari keduanya.

1.4 TUJUAN

1. Mengetahui cara merancang jaringan *Virtual Local Area Network* (VLAN) berbasis *Vlan Trunking Protocol* (VTP) dengan keamanan *Access Control List* (ACL).
2. Mengetahui perfomansi *Access Control List* (ACL) sebagai pembatasan hak akses terhadap jaringan VLAN satu dengan VLAN yang lainya, jaringan publik (internet) dengan parameter QoS *throughput*, *packet loss*, *dellay* dan *jitter*.

1.5 MANFAAT

Penilitian ini diharapkan dapat memporel manfaat, yaitu

a. Bagi pengguna

   Dapat memberi kepuasan terhadap pengguna jaringan dengan sebuah sistem yang lebih aman dengan ditetapkanya *Access Control List* (ACL).

b. Bagi penulis

Manfaat bagi penulis yaitu memperoleh pengetahuan tentang keamanan jaringan komputer serta mampu mengimplementasikan *Access Control List* (ACL) untuk keamanan jaringan komputer.

1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian serta sistematika penulisan. Bab 2 membahas tentang penelitian terdahulu dan teori pendukung dalam melakukan penelitian yang bersumber dari buku, *ebook*, Jurnal, *website* yang terdiri dari studi pustaka, pengertian jaringan komputer, keamanan jaringan, perangkat jaringan pengertian dan penjelasan sistem kerja dari *Virtual Local Area Network* (VLAN) serta *Access Control List* (ACL), penjelasan mengenai aplikasi simulator jaringan GNS3. Pada bab 3 membahas tentang alur penelitian, skenario jaringan dan topologi jaringan. Bab 4 membahas tentang analisa dan pembahasan dari hasil penelitian yang sudah dilakukan. Selanjutnya bab 5 membahas tentang kesimpulan dan saran sebagai penunjang untuk penelitian selanjutnya.