# BAB 1. PENDAHULUAN

## 1.1 Latar Belakang

Saat ini keamanan menjadi hal yang sangat penting, terutama dalam bidang teknologi informasi. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Biasanya keamanan pada *network* lebih banyak berfokus pada penggunaan *firewall, proxy,* atau berbagai cara untuk mengatasi serangan *Layer* 3. Kemananan semacam ini menggunakan sebuah asumsi bahwa serangan akan selalu dilakukan dari *network* eksternal. Diasumsikan bahwa tidak ada yang seorangpun yang melakukan serangan "jarak dekat"(Sofana, 2012:362). Sebenarnya *network* juga harus terlindungi dari berbagai serangan *Layer* 2. Misalkan saja, seorang karyawan yang ingin menambahkan perangkat di salah satu *switch* tanpa meminta izin Administrator berupa Laptop agar mendapat akses kedalam *network LAN* dan merubah konfigurasi *switch* tersebut dengan bebas sehingga berakibat jaringan menjadi lambat dan *user* lain tidak mendapatkan *bandwith* yang semestinya serta administrator harus mengkonfigurasi ulang perangkat jaringan utama yaitu *switch* dan *router*.

Ketika hal tersebut terjadi maka akan menyulitkan administrator untuk merombak topologi fisik suatu *LAN* dan mengkonfigurasi perangkat *network* yang sudah ditentukan, agar perangkat yang baru mendapatkan akses kedalam *network LAN*. Biasanya media fisik *network* akan ditanamkan pada pipa khusus yang sukar dibongkar dan ditata ulang. Sehingga tidak dapat secara fleksibel mengelompokkan kembali beberapa komputer yang lokasinya berjauhan (misal beda ruangan atau gedung), tanpa melalui proses bongkar pasang *hardware*. *VLAN* (*Virtual LAN)* dapat mengatasi keterbatasan ini. *VLAN* dapat secara fleksibel mengatur ulang "layout'' *network* secara virtual. Artinya tidak perlu membongkar media *network* dan mencabut kabel-kabel *switch*. Cukup mengatur ulang menggunakan *software* untuk menentukan komputer mana saja yang akan di kelompokkan. *Manageble switch* merupakan perangkat *switch* yang dalam penerapannya dapat dikonfigurasi lebih lanjut sesuai fitur-fitur yang tersedia,

*switch manageable* sering digunakan untuk menerapkan jaringan *Virtual LAN* dan *Inter Virtual LAN* dengan sistem keamanan yang lebih baik dibandingkan perangkat *switch unmanage*. Secara teknis jika *VLAN* sudah terbentuk, didalam praktiknya *VLAN* semacam ini masih belum bermanfaat. Sebab masing- masing *VLAN* tidak dapat berkomunikasi dengan *VLAN* yang berbeda *ID (VLAN Identity*). Di sinilah pentingnya *router. Router* dapat menghubungkan beberapa *VLAN* seperti menghubungkan beberapa *subnet* yang berbeda. Hal ini sering disebut dengan istilah *Inter-VLAN*.

Dari permasalahan tersebut diusulkan sistem yang dapat menangani pengelompokan kembali perangkat jaringan tanpa melalui proses bongkar pasang *hardware* dalam *LAN* dengan menggunakan teknologi *Inter-VLAN* (*Virtual LAN)*. Sekaligus adanya sistem *remote* yang aman yang mempermudah administrator dalam mengkonfigurasi perangkat jaringan utama.

## 1.2 Rumusan Masalah

Pemasalahan yang dirumuskan adalah bagaimana membangun suatu jaringan yang menerapkan teknologi *Inter-VLAN* dan adanya sistem yang dapat memudahkan administrator yang aman dalam menkonfigurasi jaringan tanpa harus langsung berhadapan dengan perangkat jaringan.

## 1.3 Batasan Masalah

Adapun batasan masalah yang diangkat pada penelitian ini adalah sebagai berikut :

1. Membangun jaringan yang menerapkan teknologi *Inter-VLAN*
2. Menggunakan *TACACS+ Server* sebagai *AAA* (*authentication authorization accounting*) *Remote Access.*

## 1.4 Tujuan

Adapun tujuan dari penelitian ini yaitu sebagai berikut :

1. Dapat membangun sistem *remote access* yang dapat digunakan oleh *administrator*.

2. Mampu membangun keamanan pada jaringan *Inter-VLAN*.

## 1.5 Manfaat

Manfaat dari penelitian ini adalah sebagai berikut.

1. Memudahkan *administrator* jaringan untuk mengatur jaringan
2. Memberikan keamanan dalam menggunakan *remote access* terhadap perangkat jaringan.
3. Memudahkan dalam memantau kondisi jaringan.
4. Dapat mengetauhi catatan atau *log administrator* dalam mengakses jaringan.