BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dalam bidang komputer membuat manusia menyadari akan pentingnya kebutuhan fasilitas yang disediakan oleh teknologi tersebut, khususnya dalam bidang pekerjaan. Membuat suatu instansi, baik pemerintah maupun swasta harus dapat melakukan proses pengelolahan sistem informasi yang cepat, tepat, dan aman. Berbicara soal keamanan informasi, ini masih sering terjadinya pembobolan informasi dan pencurian data-data instansi yang dilakukan oleh para *Hacker* yang tidak bertanggung jawab. Yang menginginkan sebuah informasi dari data-data tersebut. Cara atau sistem yang dapat diterapkan untuk melakukan keamanan data pada jaringan komputer tersebut adalah menggunakan metode *DHCP Snooping* dan *Extended Access List (ACL).*

Metode pertama adalah *DHCP Snooping* merupakan fitur keamanan *layer 2* yang digunakan untuk membatasi *DHCP Server palsu* yang tidak sah atau tidak dikenali untuk memberikan informasi berbahaya kepada *Client* berupa alamat *Ip Address* yang salah. *DHCP Snooping* menentukan port *switch* mana yang dapat merespon permintaan dari DHCP *(DHCP Request)*. Dan diberi semua jalur lalulintas yang terhubung ke *Network* melalui DHCP Server yang asli serta memblok port-port yang tidak terdaftar pada DHCP Server asli. Peran DHCP pada sebuah jaringan sangatlah penting sekarang ini karena permintaan client yang banyak, penggunaan DHCP sangat membantu untuk memberikan alamat IP *(internet protocol)* secara otomatis kepada *client*, ketika memanfaatkan DHCP berarti *IP Address* secara lengkap akan diberikan kepada

client secara otomatis, pemberian IP secara otomatis ini sering juga disebut dengan IP Dinamic. [1]

Metode kedua adalah *Extended Access List (ACL).* Merupakan salah satu bagian dari metode *Access Control List. Extended Access List* dapat menyaring lalu lintas data suatu jaringan dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan. *Extended Access List* juga menjamin keamanan untuk setiap komputer sehingga jalur komunikasi serta hak akses setiap komputer dapat berjalan dengan baik. Extended access list memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, Extended access list memiliki beberapa *protocol-protokol* yang berfungsi untuk melakukan trafik pada jaringan. TCP *(WWW, FTP, Telnet, SMTP, POP3), UDP (DNS), dan ICMP (Ping).* [2]

Untuk melakukan analisis perbandigan dua metode diatas maka peneliti memerlukan *Virtual Local Area Network (Vlan,)* agar tidak terbatas pada kondisi fisik melainkan peneliti bisa lebih bisa *fleksibel* dalam mendesign dan merancang sebuah *Topologi Jaringan* yang akan di pasangkan *Metode DHCP Snooping dan Metode Extended Access List.* Untuk melakukan penelitian perbandingan metode pada masalah tentang keamanan jaringan pada Vlan. *Virtual lan (vlan)* adalah model jaringan yang secara logis membagi jaringan menjadi beberapa *Vlan* yang berbeda. *Vlan* tidak terbatas pada kondisi jaringan fisik seperti *Lan.* Vlan dapat dikonfigurasi dalam praktek tanpa harus memeriksa kondisi perangkat. Akibatnya, Vlan memiliki *fleksibilitas* dalam manajemen jaringan dan memungkinkan *administrator* jaringan untuk memartisi jaringan mereka sesuai dengan kemampuan jaringan dan persyaratan keamanan.

Untuk melakukan penerapan Virtual Lan *(Vlan)* serta melakukan analisis metode diatas maka, penerapan prototipe jaringan serta mensimulasikannya peneliti menggunakan *Cisco Packet Tracer 7.3.0*. Dimana *Cisco Packet Tracer* ini akan membantu peneliti dalam perancangan *system* keamanan jaringan dengan memilih *device* yang sesuai yang akan di gunakan dalam perancangan *Vlan* dan untuk melakukan analisis perbandigan metode nantinya.

Berdasarkan latar belakang masalah diatas, maka dilakukanlah penelitian "Perbandigan Simulasi Keamanan Dengan Metode DHCP Snooping Dan Extended Accesss List" dengan menggunakan metode DHCP Snooping Dan Extended Access List sebagai metode yang akan diuji kinerjanya, dimana tiap metode tersebut memiliki fitur keamanan yang berbeda disetiap sistem keamanannya, sehingga dengan menggunakan sistem keamanan yang berbeda apakah akan berdampak pada kinerja jaringan. Pada penelitian ini peneliti menggunakan cisco packet tracer untuk membuat jaringan vlan untuk melakukan pengujian, pengujian ini dilakukan untuk mengetahui proses tingkatan keamanan pada masing-masing metode yang diujikan pada simulasi yang dilakukan untuk mengetahui metode mana yang cocok dijadikan sebuah *security* yang baik dalam melakukan penyaringan lalulintas data, menjamin keamanan data dalam sebuah jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, ditemukan beberapa rumusan masalah sebagai berikut :

1. Bagaimana proses perancangan simulasi jaringan vlan yang akan digunakan untuk penerapan metode ?

2. Bagaimana cara menguji kinerja masing-masing metode yang dilakukan analisis ?
3. Apakah terjadi perbedaan kinerja jaringan saat diterapkan keamanan jaringan dari dua metode tersebut pada jaringan vlan ?
4. Bagaimana hasil analisis pengujian kinerja dari masing masing metode yang dilakukan pada vlan ?

1.3 Batasan Masalah

Beberapa batasan masalah dalam ruang lingkup pembahasan dalam penelitian adalah sebagai berikut :

1. Menggunakan *Software Cisco Packet Tracer versi 7.3.0* untuk melakukan desain simulasi pada vlan.
2. Menggunakan *Router Mikrotik RB941-2nd* untuk penerapan *Vlan.*
3. Tahap pengujian kinerja Metode dilakukan pada *Topologi Jaringan* yang di rancang.
4. Pengujian analisis perbandigan dua metode meliputi keamanan terhadap lalulintas data serta konektivitas.
5. Tes menggunakan *Ping, Icmp, Websitite.*
6. Pengujian kinerja dilakukan pada sisi *Client.*
7. Penelitian ini hanya membahas tentang *security* jaringan dari dua *Metode* saja yaitu *DHCP Snooping dan Extended Access List*

1.4 Maksud Dan Tujuan Penelitian

Adapun maksud dari penelitian ini adalah :

1. Sebagai persyaratan dalam mencapai gelar sarjana pada jenjang Strata 1 Informatika di Universitas Amikom Yogyakarta.
2. Melakukan perbandigan kinerja dua metode keamanan jaringan pada vlan

Tujuan dari penelitian adalah :

1. Memanfaatkan teknologi berupa *Software Cisco Packet Tracer* untuk melakukan studi analisis dua metode
2. Memberikan hasil pengujian kinerja perbandingan pada masing-masing metode
3. Menambah pemahaman tentang keamanan jaringan menggunakan metode *DHCP Snooping dan Extended Access List*

1.5 Manfaat Penelitian

Hasil dari penelitian ini akan menjadi acuan informasi yang dapat digunakan dalam pemanfaatan teknologi keamanan jaringan berupa perbandingan kinerja dua metode pada VLAN yang diterapkan pada simulasi.

1.6 Metode Penelitian

Peneliti menggunakan metode penelitian dalam memperoleh data-data adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Pengumpulan data yang dilakukan untuk kegiatan penelitian dalam Menyusun laporan ini yaitu :

1. Studi Pustaka

Pengambilan data menggunakan metode studi pustaka yaitu dengan cara mempelajari dan meneliti literatur-literatur dari sumber buku-buku, jurnal ilmiah maupun dari internet yang berkaitan dengan topik penelitian.

1.6.2 Analysis

Tahap ini merupakan tahap awal dengan melakukan Analisa kebutuhan seperti *software* dan *hardware*. Serta menganalisa permasalahan yang muncul dalam membuat topologi jaringan Vlan untuk diterapkan metode dalam jaringan vlan.

1.6.3 Design

pada tahap *disegn* ini akan membuat topologi jaringan dengan mengambil dari data-data analisis yang sudah didapatkan ditahap sebelumnya. Tahap ini meliputi penggambaran desing topologi jaringan vlan dan jalur perkabelan dibuat lebih jelas.

1.6.4 Simulation Prototyping

Pada tahap ini peniliti akan membuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Packet Tracer.

1.6.5 Implementation

Pada tahap ini akan dilakukan implementasi keamanan pada jaringan secara lan berbasis vlan menggunakan semua data-data dari hasil tahap sebelumnya.

1.6.6 Monitoring

Tahap *monitoring* merupakan salah satu tahap penting dalam penelitian karena merupakan tahap melakukan pengamatan langsung terhadap peforma kinerja dari masing-masing metode yang diterapkan dengan cara melihat hasil yang didapatkan dari tiap-tiap metode berupa nilai *security, dhcp offer, dhcp acknoledgeman, dhcp request.*

1.6.7 Result

Pada tahap ini dilakukan analis hasil berupa anakisa data-dat peforma dari kinerja masing-masing metode sesudah melewati tahap-tahap pengujian. Data-data tersebutlah yang akan menjadi hasil dari perbandigan kinerja metode keamanan jaringan secara *vlan*.

1.7 Sistematika

Sistematika penulisan terdiri dari 5 bab meliputi :

BAB I PENDAHULUAN

Pada Bab ini membahas latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, metode pengumpulan data dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan tentang tinjauan Pustaka untuk menjadi landasan untuk mendukung dalam pembuatan penelitian ini terlaksa dan juga sebagai referensi.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas tentang kebutuhan sistem, data topologi untuk perancangan jaringan dalam pembuatan penelitian.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan bagaimana langkah membuat perbandingan dua metode pada vlan serta melakukan percobaan keamanan jaringan agar mendapatkan analisis hasil dari setiap metode.

BAB V PENUTUP

Pada Bab terakhir ini berisikan kesimpulan yang didapatkan dari keseluruhan penyusunan penelitian, serta saran dari peneliti untuk pengembangan penelitian lebih lanjut.