

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

*Software Defined Network* (SDN) merupakan sebuah konsep pendekatan baru untuk mendesain, mengelola, dan mengimplementasikan arsitektur jaringan dimana aliran data dari sistem control dipisahkan dari *hardware* [2]. Banyaknya penggunaan jaringan internet menyebabkan keamanan pada jaringan internet merupakan hal yang sangat dibutuhkan pada saat ini. Banyak upaya yang dilakukan untuk memberikan pelayanan jaringan internet seperti peningkatan *bandwith*, memberikan keamanan pada jaringan internet seperti menggunakan *DHCP Snooping*. *DHCP Snooping* merupakan keamanan pada jaringan komputer dan internet yang digunakan untuk mencegah atau memfilter adanya *server* lain yang tidak dipercaya dalam memberikan akses jaringan kepada pengguna atau komputer *client* [1].

Pada penelitian yang dilakukan oleh [4] bahwa *DHCP Snooping* dapat digunakan sebagai fungsi pengamanan alternatif ketika terdapat *rouge server* di dalam sistem. Selain itu, penggunaan *DHCP Snooping* pada penelitian ini memberikan peningkatan 2 kali lipat terhadap parameter *Discover Response Time* [4]. Penelitian yang dilakukan oleh [16], bahwa *DHCP Snooping* dapat memfilter dan memvalidasi terhadap port yang terpercaya dan yg tidak terpercaya. Dengan menggunakan *DHCP Snooping* jaringan komputer akan lebih aman dan tidak terganggu dengan adanya *DHCP server* yang lain. Penelitian yang dilakukan oleh [17], bahwa mitigasi *DHCP* untuk mengurangi serangan adalah *DHCP Snooping* adalah teknik keamanan yang menentukan port mana saja yang mendapatkan IP *DHCP* dan membatasi lalu lintas *DHCP* dari sumber terpercaya dan tidak terpercaya.

Namun sejauh ini penelitian tersebut belum dilakukan mengenai jaringan SDN dan pengaruh controller lainnya dan hanya berfokus pada kinerja dari *DHCP Snooping*. Maka dari itu penulis akan melakukan penelitian dengan judul "*Analisis Kinerja DHCP Snooping pada Jaringan Software Defined Network*

(SDN)”, penelitian ini dilakukan agar dapat mengetahui performansi jaringan dan karakteristik dari *controller* terbaru.

## 1.2 Rumusan Masalah

Berdasarkan deskripsi latar belakang, maka dapat dirumuskan beberapa masalah dalam penelitian ini, yaitu:

1. Bagaimana merancang jaringan SDN ?
2. Bagaimana cara membangun *DHCP Rogue* pada jaringan SDN ?
3. Bagaimana penerapan *DHCP Snooping* pada SDN ?
4. Bagaimana kinerja *DHCP Snooping* pada SDN ?

## 1.3 Tujuan Penelitian

Adapun tujuan dari penelitian tugas akhir ini adalah untuk mengetahui hasil dari analisis kinerja *DHCP Snooping* pada jaringan SDN.

## 1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah, dapat memanfaatkan *DHCP Snooping* yang terdapat pada perangkat jaringan untuk mencegah adanya *server DHCP* palsu yang mencoba memberikan alamat IP kepada *client*.

## 1.5 Batasan Masalah

Penelitian ini memiliki batasan masalah agar pembahasan yang akan dilakukan tidak menyimpang dari topik pembahasan. Batasan masalah dari penelitian ini adalah:

1. Konfigurasi jaringan menggunakan 1 buah *DHCP server*, 1 buah perangkat *DHCP rogue*, dan 2 buah *DHCP client*.
2. Menggunakan VMware sebagai *virtual machine* yang menjalankan simulasi jaringan SDN
3. Pengalamatan IP dengan menerapkan *DHCP Server* dan menggunakan IPv4.
4. Pengujian dilakukan pada konfigurasi jaringan yang telah ditentukan
5. Menggunakan protokol *OpenFlow*.

## 1.6 Metode Penelitian

Metode penelitian yang penulis gunakan untuk dapat menyelesaikan Tugas Akhir ini yaitu:

### 1. Studi Literatur

Mengumpulkan, mempelajari, memahami teori-teori yang dibutuhkan dalam pembuatan tugas akhir ini dari buku-buku referensi, artikel, jurnal, dan sumber yang terkait.

### 2. Perancangan dan simulasi

Topologi yang akan dirancang berdasarkan teori yang didapat dari studi literatur dengan melakukan simulasi menggunakan *software Virtual Machine*.

### 3. Verifikasi

Proses verifikasi dilakukan dengan membandingkan hasil perancangan yang telah dilakukan di *software Virtual Machine*.

### 4. Analisis hasil simulasi

Menganalisis hasil kinerja DHCP *Snooping* pada jaringan SDN menggunakan Aruba Van *Controller*.

## 1.7 Sistematika Penulisan

Sistematika penulisan pada Tugas Akhir ini terdiri dari 5 bab, yaitu:

### BAB I PENDAHULUAN

Pada bab ini membahas mengenai latar belakang, rumusan masalah, tujuan, Batasan masalah, metode penelitian dan sistematika penulisan dari Tugas Akhir ini

### BAB II DASAR TEORI

Pada bab ini membahas teori dan konsep pendukung

### BAB III PERANCANGAN MODEL DAN SISTEM

Pada bab ini berisi *flow chart* penelitian, rancangan pemodelan sistem, perancangan skenario penelitian,

### BAB IV ANALISIS HASIL DAN SIMULASI

Pada bab ini membahas mengenai hasil

## BAB V PENUTUP

Pada bab ini berisi uraian tentang kesimpulan dari penelitian Tugas Akhir dan ditutup dengan saran untuk penelitian lebih lanjut.