SNMP *Trap Messages Parsing* Perangkat Cisco *Wireless LAN Controller* (WLC) untuk Manajemen Perangkat *Access Point* (AP) Cisco

Nur Fajri Amali, M. Andri Setiawan
Jurusan Teknik Informatika-FTI, Universitas Islam Indoensia (UII)
Jl. Kaliurang KM. 14,5, Sleman, DIY, Indonesia
E-mail: 13523271@students.uii.ac.id

***Abstrak*—Dalam perspektif manajemen, sebuah organisasi yang menggunakan layanan internet *wireless* membuthkan informasi mengenai kondisi layanan yang diberikan, seperti informasi tentang jumlah suatu pengguna di suatu tempat yang terdapat fasilitas internet *wireless*. Salah satu cara untuk mendapatkan informasi tersebut dilakukan dengan *logging.* Logging adalah alat mendasar bagi administrator sistem untuk mengidentifikasi aktivitas yang tidak biasa saat mencoba mendiagnosis dan mengisolasi masalah, atau mencoba memastikan sistem berjalan sesuai konfigurasi [6]. Dalam melakukan logging terdapat beberapa macam protokol yang dapat digunakan, salah satunya adalah dengan menggunakan *Service Network Management Protocol* (SNMP). SNMP adalah sebuah protokol apikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi jaringan komputer [7]. Dengan menggunakan SNMP dapat diketahui segala informasi yang terjadi pada setiap alat yang menjadi SNMP Agent, salah satunya adalah Cisco WLC. Cisco WLC adalah salah satu alat yang digunakan oleh Badan Sistem Informasi (BSI) kampus Universitas Islam indonesia (UII) untuk melakukan kendali terhadap setiap Access Point (AP) yang terhubung di lingkungan kampus. Dengan menjadikan Cisco WLC ini menjadi SNMP Agent, penulis bisa melihat informasi-informasi yang di inginkan, seperti salah satunya informasi terkait authentikasi klien untuk daring. Dengan informasi Trap authentikasi klien yang akan diberikan oleh SNMP Agent, penulis dapat melakukan optimalisasi terhadap penempatan sejumlah AP yang mana AP tersebut memiliki tingkat pengguna yang lebih sedikit dibandingkan dengan AP yang lain dengan menghitung berapa banyak sebuah AP di auhentikasi oleh klien. Peneitian ini juga bisa mendapatkan informasi tentang mobilitas pengguna. Proses berjalan dengan mem-*forward* trap authentikasi kepada sebuah *host* yang menjadi sebuah SNMP Manager yang menjalankan proses untuk menerima Trap dari SNMP Agent, kemudian *host* melakukan *parsing* terhadap trap authentikasi yang masuk untuk mendapatkan informasi seperti *username,* tempat akses user, dan SSID. Hasil dari proses tersebut disimpan dalam sebuah file kemudian setiap rentang waktu 1 jam, data yang disimpan dimasukkan kedalam basis data agar bisa ditampilkan dalam web. Penelitian ini diusulkan untuk mengoptimalisasi penggunaan perangkat wireless di lingkungan kampus UII dan optimalisasi budget BSI sehingga bisa menghemat biaya pengeluaran untuk membeli lisensi perangkat lunak yang memiliki fungsi yang sama seperti pada penelitian yang dilakukan ini.**

Kata Kunci- Logging, Parsing, SNMP Trap, Cisco WLC, Cisco AP.

I. PENDAHULUAN

Perkembangan Dalam sebuah organisasi besar /perusahaan /universitas dimana terdapat banyak pekerja ataupun mahasiswa di dalamnya yang menggunakan sarana internet, pastilah terdapat beberapa hal yang dibutuhkan bagi pengelola jaringan internet di internal organisasi/ perusahaan/ universitas. Salah satu diantaranya seperti kebutuhan dimana pengelola membutuhkan informasi mengenai berapa banyak pengguna jaringan internet yang terhubung di semua tempat sehingga dapat memastikan layanan yang diberikan menjadi optimal dan bermanfaat dari sisi manajemen pengelolaan jaringan internet.

Dalam rangka melakukan manajemen jaringan internet dari sisi perangkat seperti *Access Point* yang digunakan sebagai sarana penghubung pengguna ke jaringan internet secara nirkabel, pengelola butuh mengetahui berapa pengguna yang terhubung ke tiap-tiap perangkat yang dipasang sehingga dengan informasi tersebut pengelola dapat melakukan optimalisasi perangkat. Apabila ditemukan perangkat yang ternyata memiliki jumlah pengguna yang sedikit atau bahkan tidak memiliki pengguna yang terhubung dalam hitungan hari atau minggu bahkan bulan, perangkat tersebut bisa dicabut atau dipindahkan ke tempat lain yang memiliki banyak pengguna internet nirkabel sehingga nantinya akan meningkatkan cakupan kapasitas yang dilayani tempat/ daerah tersebut dan akan tercipta suatu kondisi yang optimal dan menguntungkan dari perspektif manajemen perangkat

Universitas Islam Indonesia (UII) sebagai sebuah Universitas memiliki jumlah mahasiswa dan staff yang besar yang terbagi di beberapa fakultas. Setiap mahasiswa mempunyai sebuah akun yang dapat digunakan untuk mengakses internet nirkabel dimanapun selama di lingkungan UII. Badan Sistem Informasi (BSI) UII adalah sebuah badan yang mengatur seluruh layanan teknologi informasi di lingkungan UII. Dalam hal ini BSI adalah entitas yang mengatur manajemen jaringan internet sehingga BSI juga membutuhkan informasi tentang berapa banyak pengguna jaringan internet di suatu tempat.

Masalahnya yaitu BSI tidak mempunyai sebuah layanan informasi untuk mengetahui seberapa banyak pengguna

jaringan internet di suatu tempat tertentu di lingkungan UII sehingga di butuhkan sebuah cara untuk mendapatkan informasi tersebut, salah satunya adalah dengan menggunakan *logging* pada jaringan internet untuk mengetahui siapa saja yang terhubung ke dalam jaringan.

Logging adalah alat mendasar bagi administrator sistem untuk mengidentifikasi aktivitas yang tidak biasa saat mencoba mendiagnosis dan mengisolasi masalah, atau mencoba memastikan sistem berjalan sesuai konfigurasi [8].

Dalam melakukan logging terdapat beberapa macam protokol yang dapat digunakan, salah satunya adalah bisa dengan menggunakan *Simple Network Management Protocol* (SNMP). SNMP adalah sebuah protokol apikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi jaringan komputer [7].

Untuk melakukan optimalisasi berdasarkan masalah diatas, kita dapat melakukannya dengan menggunakan fasilitas *Logging Trap* yang tersedia pada semua perangkat *Access Point* Cisco dengan menanfaatkan protokol SNMP sehingga *Access Point* akan mengirimkan *Logging Trap* pada tiap – tiap perangkat tersebut ke sebuah *Controller* perangkat yang bernama Cisco *Wireless LAN Controller* (WLC), kemudian *Logging Trap* tersebut di *forward* ke sebuah SNMP Manager untuk kemudian digunakan untuk mengetahui informasi pengguna pada setiap perangkat *Access Point.*

Penelitian yang diususlkan ini dilakukan untuk membantu Badan Sistem Informasi (BSI) UII dalam rangka optimalisasi perangkat *Access Point (AP)* di seluruh lingkungan UII yang ter-*cover* dengan Jaringan Internet Wireless. Dengan adanya konsep ini BSI dapat menghemat biaya pengeluaran yang mungkin saja bisa digunakan untuk membeli aplikasi dari pihak ketiga atau mungkin aplikasi berbayar dari Cisco yang harganya sangat mahal yang berfungsi sama untuk optimalisasi perangkat *Access Point (AP).*

II. TINJAUAN PUSTAKA

A. Simple Network Management Ptococol (SNMP)

SNMP adalah sebuah protokol apikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi jaringan komputer [7].

SNMP beroperasi pada layer aplikasi pada TCP/IP *layer* atau Layer 7 pada model standar layer OSI *layer*. Secara umum SNMP berjalan pada port 161 dan 162 dimana port 161 digunakan untuk mengirim *requests* dari SNMP Manager ke SNMP Agent sedangkan port 162 digunakan untuk menerima notifikasi yang berasal dari SNMP Agent. SNMP bisa berjalan pada port 10161 dan 10162 ketika service yang dijalankan menggunakan *Transport Layer Security* (TLS)

Protokol ini merupakan protokol sangat dasar bagi para pengelola jaringan yang ingin mengetahui bagaimana performa sebuah jaringan yang sedang berjalan, karena dengan SNMP ini pengelola jaringan dapat mengetahui segala macam kondisi atau apa saja yang terjadi pada sebuah perangkat jaringan secara *realtime* sehingga ketika ada masalah atau pun gangguan pada perangkat pengelola dapat mengetahuinya saat itu juga. Daftar berikut adalah versi dari SNMP yang ada sekarang yaitu [7] :

a. SNMP Versi 1

SNMP Versi 1 (SNMPv1) adalah versi awal dari protokol SNMP dan di definisikan di RFC 1157 dan merupakan standar IETF historis. Keamanan SNMPv1 adalah berdasarkan *community* yang tidak lebih dari sekedar kata sandi dimana yang dimaksud *community* adalah teks biasa (string) yang memungkinkan aplikasi berbasis SNMP dapat mengakses informasi dari perangkat yang mengunakan *community* tersebut. Ada 3 *community* dalam SNMPv1 ini yaitu *read-only, read-write,* dan *trap*. Saat ini SNMPv1 merupakan versi utama dari SNMP yang di dukung oleh banyak *vendor.*

b. SNMP Versi 2

SNMP Versi 2 (SNMPv2) sering disebut *community-string-based* dan secara teknis SNMPv2 ini disebut dengan SNMPv2c, di definisikan dalam RFC 3416, RFC 3417, dan RFC 3418.

c. SNMP Versi 3

SNMP Versi 3 (SNMPv3) adalah versi terbaru dari SNMP. Perbedaan dari dua versi sebelumnya adalah keamanannya yang lebih terjamin dengan menambahkan dukungan fitur otentikasi yang kuat dan komunikasi yang bersifat privat.

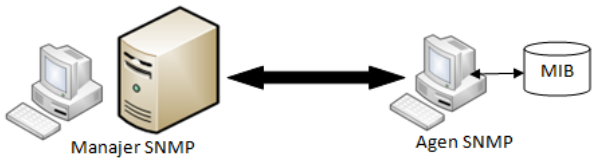
Pada SNMP terdiri dari 3 layanan dasar yaitu :

1. SNMP Manager

   SNMP Manager adalah server yang menjalankan beberapa jenis sistem perangkat lunak yang dapat mengangani tugas untuk jaringan. SNMP Manager sering disebut sebagai *Network Management Station* (NMS). NMS bertanggung jawab untuk menerima *Trap* dari SNMP Agent.

2. SNMP Agent

   SNMP Agent adalah perangkat lunak yang berjalan pada perangkat jaringan yang di kelola. SNMP Agent dapat menjadi sebuah program terpisah dari suatu sistem, ataupun bisa juga digabungkan kedalam sebuah sistem operasi, misalnya Cisco IOS Router. Pada saat ini sebagian besar perangkat jaringan sudah dilengkapi dengan perangkat lunak SNMP Agent yang sudah tertanam di dalam sistem operasi.

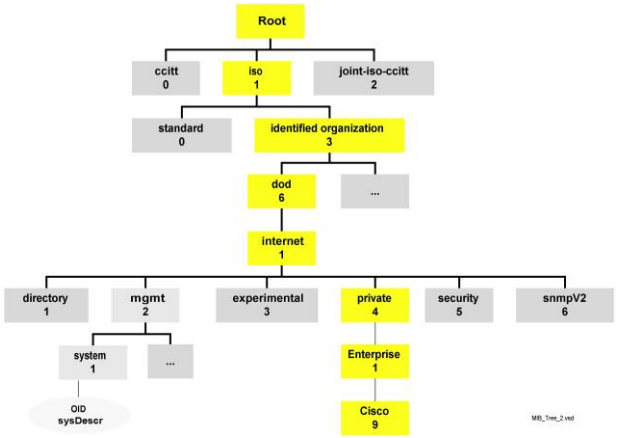


Gambar 1. SNMP manager dan SNMP Agen

3. Management Information Base (MIB)

   MIB pada SNMP dapat dikatakan sebagai tempat penyimpanan informasi yang dimiliki agen. MIB yang

terdapat pada SNMP didefinisikan secara hirarki dan setiap bagian mempunyai identifikasi objek (OID).



Gambar 2. Struktur MIB

B. *Wireless LAN Controller (WLC)*

Jaringan nirkabel telah menjadi suatu kebutuhan hari ini. Banyak lingkungan per usahaan membutuhkan penyebaran jaringan nirkabel dalam skala besar. Cisco sebagai perusahaan yang bergerak pada bidang jaringan telah menemukan sebuah konsep solusi yang dikenal dengan *Cisco Unified Wireless Network* (CUWN), yang membantu mempermudah pengelolaan penyebaran skala besar tersebut. WLC adalah perangkat yang mengasumsikan peran sentral di CUWN.

Konsep CUWN ini berarti mengatur semua entitas yang terhubung di dalam WLC hanya memiliki satu pusat kendali dimana WLC sendiri menjadi pusat kontrol terhadap semua entitas yang terhubung. Dengan menggunakan WLC, semua fungsi yang ada pada semua perangkat yang terhubung dapat diakses secara *remote* oleh WLC. WLC dapat memberikan perintah kepada perangkat-perangkat yang terpilih maupun dalam sebuah grup (terdiri dari beberapa AP) untuk memberlakukan pengaturan-pengaturan yang telah di konfigurasi pada WLC secara serempak.

Fungsi pada WLC ini sangat bermanfaat bagi sebuah organisasi yang mempunyai banyak AP yang di sebarkan pada tempat tertentu karena akan sangat memudahkan dari sisi manajemen perangkat yang terhubung.

C. *Access Point (AP)*

Access Point adalah sebuah perangkat jaringan yang berisi sebuah transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari clients remote. Dengan access points (AP) clients wireless bisa dengan cepat dan mudah untuk terhubung kepada jaringan LAN kabel secara wireless. Secara garis besar, access Point berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak Client dapat saling terhubung melalui jaringan (Network).

Access Point (AP) Cisco disebut atau juga dengan *Lightweight Access Point* (LWAPP) adalah suatu alat yang memungkinkan *user* terhubung ke dalam jaringan internet secara nirkabel. Secara umum AP ini menjadi sebuah entitas bagi WLC yang digunakan dalam penelitian. AP digunakan sebagai media yang di kontrol oleh WLC secara *remote* sehingga setiap konfigurasi dapat dilakukan dengan WLC tanpa perlu untuk mengakses AP secara langsung ke tempat dimana AP di pasang.

D. *Message Parsing*

Pada bidang ilmu komputer, Parsing adalah sebuah cara untuk menguraikan sebuah data yang biasanya tidak terstruktur tapi memiliki suatu informasi tertentu yang dapat dimanfaatkan untuk kepentingan analisis. Parsing biasanya dilakukan terhadap file log atau datasets yang berisi informasi-informasi suatu kejadian sistem yang dicatat secara *realtime* pada file tersebut.

Pada dasarnya parsing adalah memisahkan data menjadi kata per kata dalam sebuah file atau memilih sebuah informasi dari suatu file log atau dataset. Log adalah text biasa yang terdiri dari bagian-bagian yang konstan dan bagian yang bervariasi. Sebagai contoh misalnya terdapat log “Connection from 10.10.34.12 closed” dan “Connection from 10.10.34.13 closed”. Kata “connection”, “from”, dan “closed” dianggap sebagai bagian yang konstan (tetap) karena selalu sama, sedangkan bagian yang tersisa disebut sebagai *variable parts* karena nilainya yang dinamis (He et al., 2016). Bagian konstan telah ditentukan dalam *source code* oleh pengembang, dan komponen *variable parts* selalu menghasilkan nilai yang dinamis.

Secara umum log parsing adalah metode utama yang digunakan oleh penulis untuk mendapatkan data-data yang dibutuhkan dalam penelitian ini, metode ini sangat bermanfaat bagi penulis untuk melakukan pencarian dan pemilihan pada data log yang didapat dari WLC.

E. *RADIUS*

Remote Authentication Dial-In User Service (RADIUS) adalah protokol yang menyediakan layanan terpusat untuk *authentication, Authoriszation,* dan *Accounting* (AAA) untuk *dial-up*, *Virtual Private Network* (VPN) dan baru baru ini untuk akses ke jaringan nirkabel [2]. *Authentication* adalah proses mengidentifikasi dan memverifikasi kredensial pengguna. Beberapa metode dapat digunakan untuk mengotentikasi pengguna, namun yang paling umum yaitu menggunakan kombinasi antara *username* dan *password.* Begitu pengguna di otentikasi, otorisasi ke berbagai sumber dan layanan jaringan dapat diberikan. *Authorization* atau Otorisasi menentukan apa yang bisa dilakukan penguna, dan Accounting adalah tindakan untuk merekam apa yang sedang dilakukan oleh pengguna.

Protokol RADIUS pertama kali didefinisikan di RFC 2058 [2] pada bulan januari 1997, RFC ini berisi standar yang diajukan. Pada januari 1997 juga diperkenalkan RADIUS *Accounting* yang didefinisikan pada RFC 2059 [3] yang statusnya adalah sebatas informasional. Kemudian pada bulan juni 2000 di RFC 2865 [5] didefinisikan RADIUS draft standar. Klien RADIUS (dalam kasus ini adalah AP) mengirim pesan RADIUS yang berisi informasi identitas

pengguna dan parameter koneksi ke server RADIUS, kemudian server RADIUS mengotentikasi dan memberi wewenang / otorisasi kepada klien yang meminta *request* dan mengirim kembali respons pesan RADIUS.

Penelitian yang penulis lakukan menggunakan sebuah RADIUS server yang dijalankan pada komputer *host*. Penerapan RADIUS server yang paling populer adalah dengan menggunakan aplikasi FreeRADIUS sehingga penulis pun menggunakan aplikasi ini. Secara umum RADIUS ini bermanfaat sebagai sebuah server otentikasi pada penelitian ini, dimana penulis membutuhkan beberapa informasi kredensial berupa *username* dan *password* untuk digunakan pada setiap perangkat agar dapat terhubung ke jaringan nirkabel yang penulis buat. Hal ini dibutuhkan karena penulis mencoba untuk membuat *environment* yang sama seperti sistem yang sudah ada di BSI agar sistem yang akan penulis buat ini bisa berjalan dengan baik karena dikembangkan pada *environment* yang sama.

III. PERANCANGAN DAN IMPLEMENTASI SISTEM

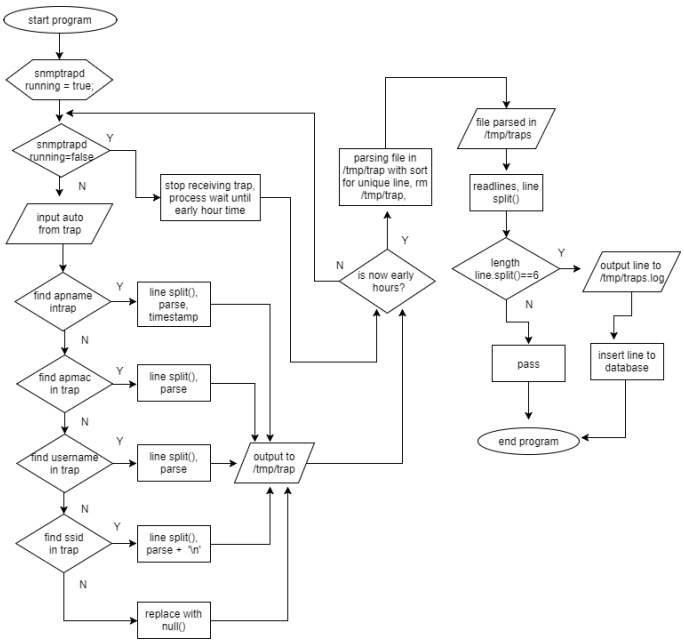
A. *Desain Interface*

Desain *interface* terbagi menjadi 4 *interface* penting yang merupakan menu dari halaman web yaitu dashboard, report, mobility dan settings.. fungsi dari halaman-halaman tersebut antara lain sebagai berikut:

1. *Dashboard* : Menu ini adalah menu utama dan menu saat pertama kali user login ke sistem. Dalam menu dashboar terdapat menu untuk memilih menampilkan 10 AP dengan pengguna terbesar, 10 AP dengan pengguna terkecil, 10 User teraktif dan juga Menu Mobilitas. Dalam menu ini dan semua menu lain terdapat sebuah *notification panel* yang terletak pada bagian kanan bawah yang menampilkan informasi tentang kapan sistem terakhir lagi meng-*update* data kedalam *database*, jumlah total data yang masuk ke *database* hari ini, jumlah total data yang masuk ke database dalam satu bulan ini dan total ukuran data di dalam database dalam hitungan *Mega Bytes* (MB).
2. *Report* : Menu digunakan untuk melihat laporan jumlah pengguna AP terbesar, AP terkecil, dan User Teraktif dalam waktu hari, minggu, bulan ini dan bulan sebelumnya.
3. *Mobility* : Menu ini digunakan untuk melihat perpindahan akses pengguna jaringan dengan car melakukan pencarian nama pengguna pada kolom search kemudian disertai dengan *role* yang diinginkan apakah ingin mengetahui perpindahan user untuk hari ini, dalam minggu ini atau dalam satu bulan ini.
4. *Settings*: Menu ini digunakan unruk merubah *password* yang digunakan untuk login oleh admin kedalam sistem.

B. *Alur Sistem*

Alur sistem / *flowchart* dari sistem yang dibangun oleh penulis adalah sebagai berikut.



Gambar 3. Alur sistem

Pada tahap perancangan ditentukan data berupa trap otentikasi yang akan dikirimkan oleh WLC kepada komputer host dan diolah dengan cara *parsing*. *Parsing* dilakukan dengan kode program yang ditulis dengan bahasa Python. Kemudian digunakan sistem operasi linux distro Ubuntu 14.04 *Long Term Support* (LTS) dan instalasi software pendukung seperti PHP5, MySQL sebagai basis data, dan *web* server apache2 untuk menjalankan sistem yang telah dibuat.

Gambar 4. Basisdata Sistem

Pembuatan sistem ini meliputi pembuatan program, pengambilan nilai variabel *trap* otentikasi, pengolahan data yang telah diambil, pembangunan sistem basis data, dan pembuatan sistem *web*. Dalam basisdata akan dibuat 2 tabel yang terdiri dari tabel authentikasi dan admin seperti Gambar 4. Diatas.

C. *Implementasi*

Tahapan ini adalah tahap memabangun sistem berdasarkan landasan teori sesuai dengan yang dipaparkan pada bab sebelumnya. Implementasi sistem dilakukan dengan menggunakan kode yang ditulis menggunakan bahasa

pemrograman Python dan juga menggunakan bahasa PHP. Sistem di implementasikan dengan menggunakan beberapa alat dan aplikasi sebagai berikut:

1. Cisco Wireless LAN Controller (WLC)
   WLC digunakan untuk membuat konfigurasi pada AP sehingga nantinya semua AP bisa dikendalikan secara *remote*, kemudian WLC juga digunakan untuk mengatur SNMP agar setiap *trap* yang dikirimkan oleh AP diteruskan kepada komputer *host*. Agar WLC dapat mengatur AP yang diinginkan, terlebih dahulu setiap AP yang dihubungkan harus diatur agar mengenali WLC ini, caranya pada AP harus diatur IP kontroller sesuai dengan IP yang digunakan di WLC, untuk AP akan dibahas pada poin B. Kemudian pada WLC harus diatur agar mengirimkan setiap *trap* dari AP yang terhubung ke komputer *host* (komputer yang penulis gunakan), caranya masukkan IP komputer *host* pada menu *trap receiver* kemudian masukan *community name* yang akan digunakan. *Community name* ini harus sama antara WLC dengan komputer *host* yang akan menerima *trap.*

2. 2 unit Csico AP
   AP digunakan sebagai media penyebar sinyal wifi terhadap konfigurasi yang telah dibuat pada WLC. AP juga berperan sebagai media penghubung antara *user* dengan jaringan. Pada penelitian yang dilakukan ini, AP hanya perlu diatur agar mengetahui alamat dari WLC yang digunakan sehingga secara otomatis nanti AP akan bergabung kedalam entitas yang diatur oleh WLC. Setelah AP diatur untuk mengenali WLC, AP dapat langsung di kontrol secara *remote* oleh WLC sehingga setiap ingin mengkonfigurasi AP cukup lewat WLC.

3. FreeRadius
   FreeRADIUS digunakan sebagai server RADIUS yang menangani proses otentikasi dari *user* untuk terhubung ke AP. Alurnya adalah setiap *user* yang akan terhubung ke AP untuk mengakses jaringan akan mengirimkan *request* ke FreeRADIUS, kemudian FreeRADIUS akan melakukan pengecekan terhadap *user*name dan password yang digunakan oleh *user* apakah *user* tersebut adalah valid dan kombinasi antara *user*name dan password tepat. Jika kondisi tersebut terpenuhi maka FreeRADIUS akan memberikan otorisasi kepada *user* tersebut untuk menggunakan akses ke jaringan.

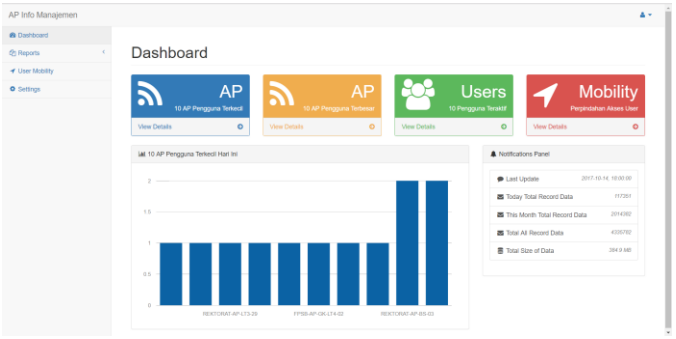
4. Dalo Radius
   Dalo RADIUS adalah aplikasi yang digunakan untuk manajemen *user* yang akan digunakan oleh RADIUS server. Dalam aplikasi ini tersedia menu untuk menambah, merubah, ataupun menghapus *user* dan aplikasi ini juga berfungsi sebagai manajemen layanan, misalnya untuk mengatur *policy user* dalam menggunakan jaringan. Aplikasi ini sangat membantu jika terdapat banyak *user* yang dalam sebuah organisasi/ perusahaan. Namun peneliti hanya menggunakan fungsi dasar saja yaitu menambah *user* untuk otentikasi agar *user* dapat terhubung ke dalam jaringan melalui AP.

IV. PENGUJIAN

Pengujian sisem dilakukan dengan menggunakan server *Virtual Private Server* (VPS) yang dibangun oleh BSI untuk menjalankan sistem yang sudah penulis buat. Hal yang berbeda pada pengujian ini dengan implementasi yang dilakukan oleh penulis terletak pada WLC yang digunakan. Jadi penulis hanya mengkopi kode program dan konfigurasi yang sudah dibuat pada komputer penulis untuk kemudian di jalankan pada server VPS (kecuali freeRADIUS), kemudian dari WLC yang digunakan oleh BSI dilakukan konfigurasi agar mengirimkan SNMP *trap* ke server VPS.

Pengujian berhasil dilakukan dan sistem sudah berjalan. *Trap* yang dikirimkan oleh WLC milik BSI berhasil masuk dan diproses *parsing* oleh kode yang sudah diimplementasikan pada server VPS dan data berhasil ditampilkan dengan menggunakan web yang dapat diakses dengan memasukkan alamat IP server VPS pada peramban. Berikut penulis perlihatkan salah satu tampilan hasil pengujian yang penulis lakukan pada sistem yang dijalankan di VPS pada menu dashboard:

A. Tampilan Menu Dashboard



Gambar 4. Tampilan menu Dashboard.

Setelah dilakukan pengujian pada menu dashboard, secara umum halaman tampak seperti pada BAB Desain Perancangan Sistem, hanya saja pada saat pengujian ini tentunta berbeda data, terdapat data yang berasal dari *trap* WLC yang digunakan oleh BSI UII. Data ini merupakan data asli yang berasal dari aktifitas pengguna dalam jaringan yang dikelola oleh BSI. Pengujian pada halaman dashboard menampilkan jumlah AP dengan pengguna terkecil, oleh karena itu data yang keluar pada kolom *frequency* pasti yg paling kecil.

Pada halaman ini terdapat sebuah *notification panel* dimana tampilan ini juga terdapat ketika *user* memilih menu 10 AP Pengguna Terbesar, 10 *User* Teraktif. *Notification panel* ini berjalan dengan baik dan menampilkan informasi berupa *last update* (data terakhir yang masuk ke sistem), *today total record data* (jumlah total *trap* yang diterima hari

ini), *this month total record data* (jumlah total *trap* yang diterima di bulan ini) dan *total size of data* (jumlah total ukuran data yang tersimpan di dalam basis data sistem) dalam hitungan *Mega Bytes* (MB).

B. Tampilan Menu Report

Pengujian pada tampilan menu *report* menunjukan data yang telah terkumpul berhasil dimasukkan kedalam *database* dan berhasil juga ditampilkan disini. Penulis melihat menu *Today* sudah bisa menampilkan data – data berupa AP dan *user* yang telah didapat dari proses *parsing* di sistem.

C. Tampilan Menu Mobility

Pengujian pada menu mobility berjalan sukses. Penulis mencoba memasukan id penulis kedalam kolom *search user*, kemudian sistem bisa menampilkan perpindahan akses penulis pada kolom *result.*

D. Tampilan Menu Settings

Pengujian pada menu *settings* berjalan dengan lancar. Pada menu *settings* terdapat kolom untuk merubah *password administrator*, penulis mencoba untuk merubah password dan hasilnya sukses dan password bisa dirubah. Begitu juga ketika penulis mencoba merubah password dengan memasukkan password yang salah pada kolom *old password*, maka *password* tidak berubah ketika penulis meng-klik tombol *change password*, begitu juga ketika penulis memasukkan kata yang berbeda pada kolom *new password* dan *confirm password*. Hal ini membuktikan bahwa pengujian pada menu *settings* berjalan sukses.

Berikut penulis rangkum kedalam tabel hasil dari pengujian yang penulis lakukan:

Tabel 1. Tabel hasil pengujian

Bagian Halaman	Fungsi	Hasil Pengujian
Menu Dashboard	Menampilkan menu – menu instan yang bisa dieksekusi untuk hari ini dalam tampilan kotak yang menarik dann juga menampilkan 10 AP dengan pengguna terkecil	Sukses
Menu Report	Menampilkan rangkuman keseluruhan informasi tentang 10 AP dengan pengguna terkecil, 10 AP dengan pengguna terbesar dan 10 *user* teraktif dalam hitungan hari, minggu, bulan ini dan bulan lalu	Sukses
Menu Mobility	Mencari informasi terkait perindahan tempat akses *user* dalam jaringan	Sukses
Menu Setting	Merubah *password* akses ke sistem untuk Administrator	Sukses

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Setelah dilakukan penelitian dan implementasi, simpulan yang dapat diambil dari kegiatan Tugas Akhir dengan judul "SNMP *Trap* Messages Parsing Perangkat Cisco Wireless LAN Controller (WLC) untuk manajemen perangkat Access Point (AP) Cisco" pada Badan Sistem Informasi (BSI) Universitas Islam Indonesia (UII) adalah:

a. Sistem berhasil berjalan dengan lancar dan data dapat ditampilkan pada aplikasi web yang sudah dibuat.

b. Secara umum setiap pesan log (dalam hal ini *trap*) dapat dimanfaatkan untuk mendapatkan informasi tertentu dengan teknik yang benar.

B. Saran

Dari sistem yang dibuat ini masih terdapat kekurangan dan kelemahan yang sebenarnya dapat dikembangkan lebih lanjut. Melalui hasil diskusi bersama Bapak Mukhammad Andri Setiawan selaku Deputi dari BSI UII, saran untuk pengembangan sistem ini yaitu:

a. Pengembangan sistem pada fitur mobilitas bisa dilakukan dengan cara menampilkan informasi yang masih berbentuk data pada tabel kedalam suatu *maps* yang mencakup wilayah UII sehingga mobilitas setiap *user* dapat dilihat lebih menarik berdasarkan pergerakan pada peta yang dibuat.

DAFTAR PUSTAKA

[1] Koo, Simon G. M., Rosenberg, Catherine., Chan, Hoi-Ho., and Lee, Yat Chung., *Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications*, West Lafayette, IN 47907-1285, USA.

[2] Rigney, C., Rubens, A., Simpson, W., and Willens, S., RFC 2058: *Remote Authentication Dial In User Service (RADIUS).* Available: www.ietf.org/rfc/rfc2058.txt, January 1997

[3] Rigney, C., RFC 2059: *Radius Accounting* [Online].Available: www.ietf.org/rfc/rfc2059.txt , January 1997.

[4] Rigney, C., Rubens, A., Simpson, W., and Willens, S., RFC 2138: *Remote Authentication Dial In User Service (RADIUS).* Available: www.ietf.org/rfc/rfc2138.txt, April 1997.

[5] Rigney, C., Rubens, A., Simpson, W., and Willens, S., *RFC 2865: Remote Authentication Dial In User Service (RADIUS).* Tersedia di: www.ietf.org/rfc/rfc2865.txt , June 2000.

[6] Eaton, Ian. 2003. *The Ins and Outs of System Logging Using Syslog.* Sydney: SANS Institute.

[7] R Mauro, Douglas., Schmidt, Kevin J., *"Essential SNMP Second Edition"*, O'Reilly Media, Sebastopol, 2005.

[8] Nawyn, Kenneth E. *A Security Analysis of System Event Logging with Syslog.* SANS Institute, 2003.

[9] He, Shilin., Zhu, Jieming., He, Pinjia., and R. Lyu, Michael., *Experience Report: System Log Analysis for Anomaly Detection.* Shenzhen, China: 2016 IEEE 27th International Symposium on Software Reliability Engineering, 2016.