SNMP TRAP MESSAGES PARSING PERANGKAT CISCO *WIRELESS LAN CONTROLLER* (WLC) UNTUK MANAJEMEN PERANGKAT *ACCESS POINT* (AP) CISCO

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat

untuk Memperoleh Gelar Sarjana

Teknik Informatika

Disusun Oleh:

N a m a : Nur Fajri Amali

NIM : 13523271

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2017

LEMBAR PENGESAHAN DOSEN PEMBIMBING

SNMP TRAP MESSAGES PARSING PERANGKAT CISCO *WIRELESS LAN CONTROLLER* (WLC) UNTUK MANAJEMEN PERANGKAT *ACCESS POINT* (AP) CISCO

TUGAS AKHIR

Disusun Oleh:

N a m a : Nur Fajri Amali

NIM : 13523271

Yogyakarta, 19 September 2017

Pembimbing,

(Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D.)

LEMBAR PENGESAHAN PENGUJI

SNMP TRAP MESSAGES PARSING PERANGKAT CISCO *WIRELESS LAN CONTROLLER* (WLC) UNTUK MANAJEMEN PERANGKAT *ACCESS POINT* (AP) CISCO

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Informatika
di Fakultas Teknologi Industri Universitas Islam Indonesia
Yogyakarta, 02 Oktober 2017

Tim Penguji

Ketua

Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D. _____

Anggota 1

Ari Sujarwo S.Kom., MIT(Hons) _____

Anggota 2

Kholid Haryono S.T., M.Kom. _____

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Teknologi Industri
Universitas Islam Indonesia

(Hendrik, S.T., M.Eng.)

LEMBAR PERNYATAAN KEASLIAN HASIL TUGAS AKHIR

Yang bertanda tangan dibawah ini,

Nama : Nur Fajri Amali

NIM : 13523271

Tugas akhir dengan judul:

SNMP TRAP MESSAGES PARSING PERANGKAT CISCO *WIRELESS LAN CONTROLLER* (WLC) UNTUK MANAJEMEN PERANGKAT *ACCESS POINT* (AP) CISCO

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 05 Oktober 2017

(Nur Fajri Amali)

HALAMAN PERSEMBAHAN

Segala puji bagi Alllah Subhanahu Wa Ta'ala, Tuhan semesta alam yang telah memberikan ridho, rahmat serta hidayahnya atas kekuatan, ilmu, pengetahuan, dan pengalaman yang amat luas kepada saya, sehingga tak henti hentinya saya selalu senantiasa bersyukur atas apa yang telah diberikan kepada saya serta selalu memohon ampun atas setiap kesalahan yang telah saya lakukan baik disadari maupun tidak.

Shalawat dan salam senantiasa terlimpahkan kepada Nabi agung Muhammad Shallalahu 'Alaihi Wasalam yang telah memberikan cahaya yang terang benderang bagi akhlak dan kehidupan manusia sehingga menuntun kepada jalan kebenaran .

Tugas akhir ini saya persembahkan untuk semua yang saya cintai dan saya sayangi serta saya hormati.

Kepada orang tua saya, Ayahanda Asro Suwito serta Ibunda Rodiyah yang selalu memberikan dukungan moral dan moril serta selalu mendoakan saya di setiap waktu sujudnya selama saya hidup sampai sekarang saya meyelesaikan Tugas Akhir ini.

Kepada Keluarga, Sahabat dan Teman- Teman semua yang selalu berbagi suka dan duka setiap saat, semoga ini menjadi sedikit kebanggaan kepada kalian semua. Penulis menyadari bahwa ini saja tidak cukup untuk membalas budi dan kebaikan mereka semua. Semoga dengan prestasi kecil ini penulis bisa membuat bangga terutama kepada orang tua tercinta, Aamiin.

HALAMAN MOTTO

Dan (ingatlah juga), tatkala Tuhanmu memaklumkan. "Sesungguhnya jika kamu bersyukur, pasti Kami akan menambah (ni'mat) kepadamu, dan jika kamu mengingkari (ni'mat-Ku), maka sesungguhnya azab-Ku sangat pedih".

(Q.S Ibrahim: 7)

"Ya Rabbku, lapangkanlah untukku dadaku, dan mudahkanlah untukku urusanku, dan lepaskanlah kekakuan dari lidahku, supaya mereka mengerti perkataanku"

(QS. Thoha: 25-28)

"Tidak ada tuhan selain Engkau, Maha Suci Engkau. Sungguh aku termasuk orang-orang yang zalim."

(QS. Al-Anbiya': 87)

KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh.

Alhamdulillahirabbil'alamiin, puji syukur atas kehadirat Allah Subhana Wa Ta'ala yang telah melimpahkan rahmat dan hidayah-Nya. Sholawat serta salam tidak lupa kita haturkan kepada junjungan kita Nabi besar Muhammad SAW sehingga penulis dapat menyelesaikan tugas akhir ini yang berjudul "***SNMP Trap Messages Parsing* Perangkat Cisco *Wireless LAN Controller* (WLC) Untuk Manajemen Perangkat *Access Point* (AP) Cisco**" dapat diselesaikan dengan baik.

Laporan tugas akhir ini, disusun untuk memenuhi syarat memperoleh gelar Sarjana Strata-1 (S1) di jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia. Tugas akhir ini juga sebagai sarana untuk mempraktekkan secara langsung ilmu dan teori yang telah diperoleh selama menjalani masa studi di jurusan Teknik Informatika Universitas Islam Indonesia.

Tugas akhir ini dapat tersusun berkat bantuan, dorongan, bimbingan serta kerja sama dengan baik dari berbagai pihak. Penulis menyampaikan terimakasih dan penghargaan setinggi-tingginya kepada:

1. Orang tua penulis yang selalu medoakan dan memberikan dukungan baik moral dan moril kepada penulis.
2. Keluarga besar saya, terimakasih atas segalanya.
3. Mukhammad Andri Setiawan, S.T., M.Sc., Ph.D., sebagai dosen pembimbing tugas akhir yang telah memberikan pengarahan serta dorongan sehingga tugas akhir ini selesai.
4. Nandang Sutrisno, S.H., M.Hum., LLM., Ph.D. Selaku Rektor Universitas Islam Indonesia.
5. Hendrik, S.T., M.Eng. selaku Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

6. Sahabat-sahabat saya selama menempuh sarjana khususnya informatika angkatan 2013 (Eternity).
7. Kepada semua pihak yang tidak bisa saya sebutkan satu persatu yang telah benyak membantu secara langsung maupun tidak langsung, semoga Allah membalas kebaikan semua.

Tugas akhir ini tidak lepas dari kekurangan dan ketidaksempurnaan dikarenakan terbatasnya kemampuan penulis, oleh karena itu kritik dan saran membangun sangat dibutuhkan. Akhirnya penulis berharap semoga laporan tugas akhir ini memberikan manfaat bagi semua pihak yang terkait, *Aamiin*.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

SARI

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.

Penelitian 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.

Hasil pengujian menunjukan bahwa sistem berjalan dengan baik, dan sistem dapat menampilkan informasi yang diterima di *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, SNMP Trap, Cisco WLC, Cisco Access Point*

TAKARIR

Interface	: Tampilan dalam sistem dengan menggunakan web
Forward	: Melanjutkan dan mengirimkan kembali data
Layer	: Lapisan struktur dalam teori tentang lojik internet
Cover	: Lingkup area yang dicakup
Maps	: Peta suatu lokasi
Host	: Pengguna / yang mengoperasikan proses sistem
Wireless	: Jaringan internet nirkabel
Budget	: Anggaran untuk suatu keperluan
Request	: Permintaan dari proses
Service	: Layanan yang sedang dijalankan
Realtime	: Yang terjadi saat ini
Environment	: Lingkungan sistem
Container	: Tempat untuk menyimpan data
Unique	: Tidak sama dengan yang lain
Resource	: Sumber daya pada komputer
Command	: Baris perintah yang dijalankan untuk di eksekusi
Daemon	: Sebuah proses yang berjalan di latar belakang dalam sistem operasi linux
Acknowledgement	: Transmisi yang dikirimkan oleh pihak station penerima dalam jaringan kepada pihak pengirim bahwa data yang dikirimkan telah diterima dengan sempurna tanpa ada kesalahan

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam sebuah organisasi besar, perusahaan, atau 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, atau 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 atau 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 (Nawyn, 2003).

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 (R Mauro & Schmidt, 2005).

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).*

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, penulis merumuskan masalah sebagai berikut:

a. Bagaimana mendapatkan data serta membuat sebuah sistem untuk mendapatkan informasi jumlah pengguna di suatu tempat tertentu yang mengakses jaringan dalam periode waktu tertentu dan menampilkannya kepada pengelola.

1.3 Batasan Masalah

Dalam pengerjaaan skripsi ini terdapat beberapa batasan masalah agar pengerjaan lebih terarah:

a. Jenis perangkat *Access Point* yang digunakan adalah perangkat dari Cisco
b. Hanya untuk perangkat yang terhubung dengan sistem yang ada di Badan Sistem Informasi (BSI) Universitas Islam Indonesia.
c. Hanya untuk mengetahui *Access Point* mana saja yang memiliki pengguna terkecil dan terbesar dari semua *Access Point* milik BSI.
d. Data ditampilkan dengan menggunakan visualisasi dalam bentuk grafik.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai penilitian ini adalah:

a. Optimalisasi penggunaan perangkat *Access Point* (AP) di seluruh lingkungan UII yang terhubung dengan Sistem di Badan Sistem Informasi (BSI) UII.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

a. Penghematan biaya pengeluaran untuk bidang Teknologi oleh Badan Sistem Informasi yang mungkin bisa di alihkan untuk keperluan yang lain.

1.6 Metodologi Penelitian

Adapun metode penelitian yang penulis gunakan untuk melakukan penelitian ini diantaranya adalah:

a. Persiapan pembuatan program, yang termasuk dalam persiapan ini adalah diawali dengan penyusunan proposal, kemudian menyediakan aplikasi-aplikasi yang dibutuhkan untuk melakukan penelitian.

b. Studi literatur untuk mendapatkan literatur yang berkaitan dengan masalah SNMP *Trap Messages* baik yang berupa buku, artikel, jurnal ilmiah, maupun tugas akhir.

c. Pengumpulan data yang meliputi kegiatan-kegiatan sebagai berikut:

   1. Observasi, yaitu pencarian data atau informasi dengan melakukan pengujian langsung menggunakan perangkat terkait seperti *Access Point Cisco, Cisco WLC,* dan *Cisco Switch.*
   2. Metode Penelitian Kepustakaan (*Libray Research Method*), yaitu mengumpulkan data yang berhubungan dengan topik permasalahan dari judul yang penulis buat. Metode penelitian kepustakaan dilakukan dengan cara membaca buku-buku, makalah, *browsing* melalui Internet melihat *website*, bahan kuliah maupun artikel-arikel untuk mendapatkan landasan teori yang mencukupi.

d. Analisis data yang dilakukan dengan cara menganalisis data berupa pesan SNMP *Trap* yang telah di dapatkan dengan pengujian langsung perangkat Cisco.

e. Perancangan sistem yang terdiri dari perancangan basis data dan perancangan tampilan program aplikasi (*interface*).

f. Pembuatan sistem yang prosesnya ini dilakukan dengan pembuatan tampilan sistem, pembuatan basis data, dan penyusunan *coding* program.

g. Pengujian sistem yang telah dibuat, diuji dengan mengaktifkan perangkat, mengolah data, dan mengeluarkan data yang sudah di Analisis sehingga menghasilkan sebuah informasi.

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang permasalahan, identifikasi masalah, menentukan batasan masalah yang akan dibahas, menjabarkan tujuan dan manfaat dari penelitian ini, asumsi metodologi penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi berbagai teori yang digunakan sebagai landasan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini. Bahasan dalam bagian ini mengenai pembahasan teori dasar yang digunakan dalam penelitian, terkait logging,

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang objek dan jenis penelitian, data dan sumber data, teknik pengumpulan data.

BAB IV DESAIN PERANCANGAN SISTEM

Bab ini akan berisi mengenai analisis terhadap kebutuhan sistem yang dibangun, dan perancangan sistem yang akan dibangun dalam penelitian ini berupa rancangan antarmuka dan alur proses.

BAB V IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi hasil implementasi serta penjelasan sesuai dengan perencanaan yang telah dibuat sebelumnya. Pengujian dilakukan untuk memastikan bahwa hasil akhir yang dibuat sesuai dengan kebutuhan dan karakteristik pengguna.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang menjelaskan tujuan penelitian dapat tercapai serta menjelaskan kelebihan dan kekurangan yang terdapat pada sistem yang telah dibuat. Sementara saran, berisi hal-hal yang dapat dikembangkan lagi kedepannya mengenai kekurangan yang masih terdapat pada sistem tersebut.

BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

Bagian ini menjelaskan teori-teori dasar yang berkaitan dengan pembuatan sistem. Sistem yang akan dibuat oleh penulis menggunakan konsep yang sudah ada di bidang teknologi. Penulis akan menggunakan SNMP, *Wireless LAN Controller* (WLC), *Access Point* (AP), *Messages Parsing* dan *RADIUS*. Penulis akan membahasnya dimulai dari SNMP.

2.1.1 Protokol Simple Network Management Protocol (SNMP)

The Internet Engineering Task Force (IETF) adalah sebuah organnisasi yang bertanggung jawab untuk menentukan standar protokol yang mengatur lalu lintas internet, termasuk salah satunya adalah *Simple Network Management Protocol* (SNMP), selain itu IETF juga menerbitkan *Requests for Comments* (RFCs) yang merupakan spesifikasi untuk banyak protokol yang ada di dunia IP (R. Mauro & Schmidt, 2005).

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 (R. Mauro & Schmidt, 2005).

SNMP beroperasi pada layer aplikasi pada TCP/IP *Layer* atau *Layer* 7 pada model standar 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:

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.

Dalam SNMP terdapat *Protocol Data Unit* (PDU), pada SNMPv1 terdapat 5 PDU sementara dalam SNMPv2 terdapat 7 PDU. Jenis-jenis PDU dari SNMP seperti berikut:

1. GetRequest

GetRequest merupakan sebuah permintaan yang dikirim oleh manajer ke agen untuk mengambil nilai dari satu atau lebih variabel MIB yang diminta.

2. SetRequest

SetRequest merupakan sebuah permintaan yang dikirim oleh manajer ke agen untuk mengatur satu atau lebih variabel MIB yang ditentukan di PDU dengan nilai yang di tentukan di PDU.

3. GetNextRequest

GetNextRequest merupakan sebuah permintaan yang dikirim oleh manajer ke agen untuk mengambil variabel MIB berikutnya yang ditentukan di PDU. Hal ini dapat dilakukan karena dalam satu PDU bisa untuk menampung beberapa permintaan.

4. GetBulkRequest

GetBulkRequest merupakan versi optimal dari GetNextRequest, dimana permintaan manajer ke agen adalah perulangan dari perintah GetNextRequest sehingga banyak nilai dari variabel MIB dapat di minta sekaligus ke agen.

5. GetResponse

GetResponse merupakan sebuah PDU yang dikirim oleh agen berfungsi untuk mengembalikan nilai GetRequest, SetRequest, GetNextRequest, GetBulkRequest, dan InformRequest yang diminta oleh manajer.

6. *Trap*

Trap adalah pesan yang dikirim oleh agen tanpa diminta oleh manajer untuk memberitahukan tentang kejadian penting yang terjadi pada agen.

7. InformRequest

InformRequest merupakan sebuah PDU yang memberikan *acknowledgement* atas permintaan yang sebelumnya di minta apakah hasil dari permintaan sudah diterima atau belum.

Pada SNMP terdiri dari 3 layanan dasar yaitu :

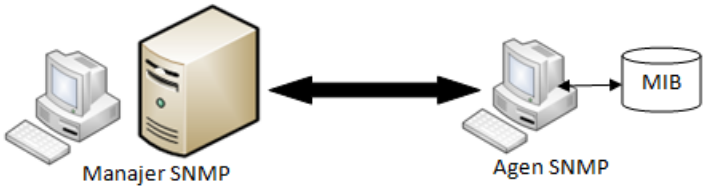
a. SNMP Manager

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.

b. 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.

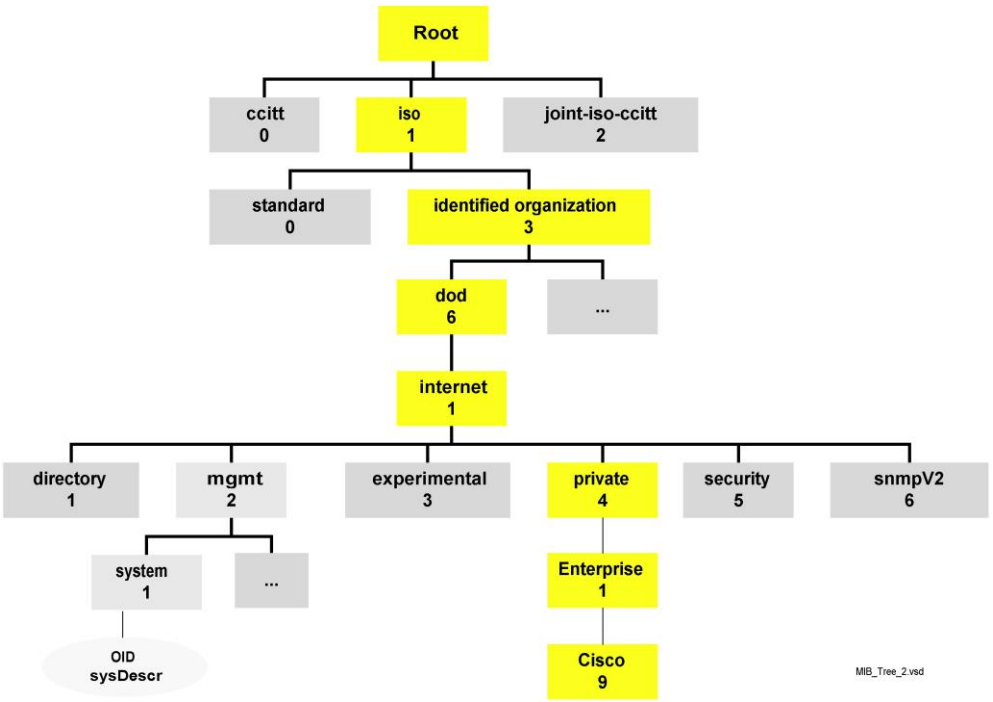


Gambar 2.1 SNMP manager dan SNMP Agen

c. 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).

MIB untuk setiap perangkat berbeda – beda berdasarkan vendor yang mengeluarkan atau memproduksi perangkat. Berikut ini adalah struktur MIB untuk perangkat dari vendor Cisco:



Gambar 2.2 Struktur MIB Perangkat Cisco

Pada dasarnya SNMP bekerja dengan mengirimkan pesan *Trap* dari SNMP Agen ke SNMP Manager. Mekanisme ini seperti mengirim sebuah log informasi dengan kode yang memiliki makna tertentu yang dapat diartikan oleh sebuah SNMP Manager. Kode berikut adalah kode – kode dari OID SNMP yang akan penulis gunakan landasan untuk memperoleh informasi dari *trap* yang dibutuhkan disajikan dalam Tabel 2.1 berikut:

Tabel 2.1 Tabel OID

OID	Makna
iso.3.6.1.4.1.9.9.513.1.1.1.1.5.0	OID *Access Point*
iso.3.6.1.4.1.9.9.599.1.3.1.1.8.0	OID MAC *Address Access Point*
iso.3.6.1.4.1.9.9.599.1.3.1.1.27.0	OID Pengguna *WiFi*
iso.3.6.1.4.1.9.9.599.1.3.1.1.28.0	OID SSID dari *WiFi* yang digunakan oleh pengguna

SNMP menjadi protokol yang terus dikembangkan karena banyak perangkat jaringan yang mendukung layanan SNMP ini seperti *Router, Switch, Server, Workstation,* dan *Printer.*

Secara umum dengan protokol SNMP ini peneliti menggunakannya untuk memperoleh data log dari dari alat yang digunakan, salah satunya seperti Cisco WLC yang nanti akan digunakan sebagai kontroller. WLC akan berberpan sebagai alat yang akan mengirimkan log data kepada *host.* SNMP digunakan oleh komputer *host* untuk menerima *trap* yang dikirimkan oleh WLC sehingga nantinya data yang dikirimkan (berupa *trap*) oleh WLC dapat diolah oleh komputer *host.*

2.1.2 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.

2.1.3 Access Point (AP)

Access Point (AP) adalah sebuah perangkat jaringan yang berisi sebuah transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari clients remote. AP 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.

Dengan *Access Point* (AP) klien *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 klien dapat saling terhubung melalui jaringan (Network). *Access Point* (AP) dalam hal ini AP Cisco yang akan digunakan oleh penulis menggunakan sebuah protokol *Lightweight Access Point protocol* (LWAPP). LWAPP adalah protokol yang dapat mengontrol banyak *wireless access points* secara sekaligus. Hal ini

dapat mengurangi waktu yang digunakan untuk melakukan konfigurasi, *monitoring*, atau *troubleshooting* pada pada jaringan dengan skala yang besar. Protokol ini juga memungkinkan administrator jaringan untuk menganalisa jaringan secara seksama.

Pada AP dikenal juga istilah *Control And Provisioning of Wireless Access Points* (CAPWAP). CAPWAP adalah protokol standar, protokol jaringan yang memungkinkan pusat LAN nirkabel (dalam hal ini adalah WLC) untuk mengelola *wireless access point* atau dikenal juga dengan AP. Protokol ini didefinisikan pada RFC 5415. CAPWAP ini juga berdasarkan pada LWAPP, namun dengan penambahan *Datagram Transport Layer Security* (DTLS).

DTLS adalah protokol komunikasi yang menyediakan keamanan untuk aplikasi berbasis datagram dengan memungkinkan mereka berkomunikasi dengan cara yang sudah dirancang untuk mencegah penyadapan, perusakan, atau pemalsuan pesan. Dengan penambahan DTLS ini, maka komunikasi antara AP dengan WLC lebih aman dari gangguan yang meungkin dilakukan oleh pihak pihak yang tidak bertanggung jawab.

AP yang digunakan oleh penulis adalah AP Cisco yang juga sudah mendukung protokol tersebut. Trap dari AP akan dikirimkan kepada kontroller, kemudian kontroller akan mengirimkan pesan trap tersebut kepada host untuk kemudian dilakukan *parsing.*

2.1.4 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. Trap yang dikirimkan nanti berupa trap otentikasi dari setiap user yang terhubung. Untuk mendapatkan trap otentikasi terlebih dahulu harus disiapkan sebuah protokol yang menangani otentikasi. Protokol yang nanti digunakan adalah RADIUS.

2.1.5 Protokol 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 (Rigney et. al., 1997). *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 (Rigney et.al., 1997) pada bulan januari 1997, RFC ini berisi standar yang diajukan. Pada januari 1997 juga diperkenalkan RADIUS *Accounting* yang didefinisikan pada RFC 2059 (Rigney, 1997) yang statusnya adalah sebatas informasional. Kemudian pada bulan april 1997 RFC tersebut dianggap sudah usang oleh RFC 2138 (Rigney et.al., 1997)

dan RFC 2139 (Rigney et.al., 1997). Kemudian pada bulan juni 2000 di RFC 2865 (Rigney et.al., 2000) 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 atau 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.

2.2 Review Penelitian Sebelumnya

Penulis melakukan *review* terhadap penelitian yang dilakukan sebelumnya yang saling berkaitan , kemudian penulis menemukan sebuah paper dengan judul "*Experience Report: System Log Analysis for Anomaly Detection".* Penulis menemukan sebuah hubungan antara penelitian yang penulis lakukan dengan penelitian pada *paper* tersebut.

Penulis pada *paper* tersebut melakukan penelitian dengan cara *parsing* pada log dataset yang telah di sebarkan ke publik yang terdiri dari 15,923,592 message log dan 365.298 contoh anomali dalam sebua sistem, kemudian melakukan analisis terhadap log tersebut salah satunya dengan metode *log parsing* dan menampilkan visualisai dari data dengan menggunakan grafik.

Penulis juga melakukan *review* paper pada penelitian dengan judul *"Rancang Bangun Aplikasi Monitoring Jaringan dengan Menggunakan Simple Network Management Protocok"*. Penulis menemukan point point penting pada

definisi – definisi SNMP. Paper ini memberikan informasi yang menarik terhadap SNMP dan juga mudah dipahami karena penggunaan bahasanya yang jelas dalam menjelaskan.

Penulis pada paper ini memaparkan bahwa semakin meningkatnya jumlah ukuran dan jumlah pernagkat jaringan akan semakin kompleks masalah pada jaringan sehingga penulis tersebut memanfaatkan protokol SNMP untuk melakukan *monitoring* dengan cara membuat sebuah aplikasi yang dilengkapi dengan *database* untuk menyimpan dan mengolah nilai SNMP. Hal ini mirip dengan yang penulis lakukan, bedanya penulis melakukan parsing terhadap trap yang masuk untuk dilakukan penyortiran terlebih dahulu terhadap trap otentikasi, kemudian nilainya disimpan di dalam *database* untuk kemudian bisa ditampilkan di sistem web yang penulis buat.

Hasil dari penelitian yang di-*review* oleh penulis diatas telah dilakukan pengujian untuk mengetahui keakuratan apkikasi yang dibuat. Hasil pengujian sistem menunjukan bahwa aplikasi yang dibuat cukup akurat jika dibandingkan dengan *software* Wireshark dan Netstat dengan selisih nilai 0.278%. Hal ini cukup membuat penulis kagum karena aplikasi yang dibuat lebih baik dari Wireshark dan Netstat dimana kedua aplikasi tersebut merupakan aplikasi yang sangat terkenal dan jumlah penggunanya banyak.

BAB III
METODOLOGI PENELITIAN

3.1 Langkah Peneltian

Langkah Penelitian akan dilakukan menjadi beberapa tahapan, yaitu:

a. Studi pustaka terhadap protocol SNMP dan penerapannya secara langsung pada Cisco WLC
b. Analisis kebutuhan sistem
c. Perancangan alur sistem secara keseluruhan
d. Menerapkan metode parsing menggunakan Python terhadap *Trap* yang didapat
e. Implementasi sistem.
f. Pengujian sistem.

3.2 Studi Pustaka dan Penerapan SNMP

Studi pustaka dilakukan dengan melihat literatur dan paper yang ada di internet tentang SNMP dan penerapannya di berbagai macam alat jaringan, terutama dari vendor Cisco. Penerapan protokol SNMP dilakukan dengan menjalankan layanan SNMP Agent pada alat Cisco WLC, kemudian mem-*forward Trap* dari SNMP Agent ke sebuah *Host* linux. Hal ini dilakukan untuk mengetahui informasi-informasi *Trap* yang dikirimkan oleh Cisco WLC.

3.3 Metode Pengembangan Sistem

Tahapan pengembangan sistem yang dilakukan pada penelitian ini adalah analisis kebutuhan sistem, perancangan, implementasi dan pengujian. Tahapan analisis kebutuhan sistem dilakukan untuk memperoleh rancangan sistem yang akan dibangun. Tahap implementasi dan pengujian sistem akan dibahas pada bab selanjutnya. Tahapan perancangan sistem yang dilakukan pada penelitian ini adalah analisis kebutuhan sistem, perancangan, implementasi dan pengujian.

3.3.1 Analisis Kebutuhan Sistem

Pengembangan sistem menggunakan komputer virtual yang berjalan pada aplikasi VMware Workstation Pro dengan spesifikasi: Sistem Operasi Ubuntu 14.04 LTS, Memory sebesar 1 GB dengan sebuah Prosesor sebesar dari 1 core dari Prosesor *Host* Komputer yang menjalankan VMware, serta *Storage* sebesar 20 GB. Pembuatan aplikasi menggunakan Terminal Linux dan menggunakan bahasa pemrograman Python 2.7 serta HTML sebagai bahasa untuk membuat *interface* dari program yang dibangun dengan basis *web*. Sistem menggunakan Basis Data *platform* MySql sebagai *container* data dari sistem yang dibuat. Sedangkan komputer *host* yang menjalankan aplikasi Vmware Workstation Pro memiliki spesifikasi: Prosessor Intel(R) Core(TM) i5-5200U 2.2GHz, Memory sebesar 4GB RAM dengan Sistem Operasi Windows 10 Education 64-bit (10.0, Build 15063). Analisis kebutuhan lainnya pada pengembangan sistem meliputi kebutuhan masukan, proses dan keluaran adalah sebagai berikut:

a. Analisis Kebutuhan Masukan (*Input*)

Kebutuhan masukan pada sistem berupa *Trap* yang berasal dari SNMP Agen (Cisco WLC) yang merupakan bagian dari proses otentikasi *user* terhadap *Access Point (AP)* Cisco, dengan format berupa (*[oid] [info])*, kemudian *trap* tersebut di uraikan sehingga akan diambil nilai *[info]* saja yang kemudian akan di kumpulkan dalam satu buah file sebelum kemudian di analisis lebih lanjut untuk kemudian di masukkan kedalam basis data sistem

b. Analisis Kebutuhan Proses

Proses yang dibutuhkan sistem berupa penguraian atau *parsing* terhadap info *Trap* sehingga akan memisahkan data mana saja yang akan diambil sebagai input dari sistem yang dibuat. Dalam analisis kebutuhan proses ini di butuhkan sebuah proses *daemon* yang akan berjalan terus menerus selama sistem aktif dimana proses *daemon* tersebut akan selalu *stand by* ketika ada sebuah *Trap* yang masuk ke dalam sistem dan proses akan menyimpan *Trap* tersebut untuk kemudian di *parsing.*

c. Analisis Kebutuhan Keluaran (*Output*)

Keluaran akhir yang dihasilkan oleh sistem berupa informasi tentang *Access Point(AP)* mana yang memiliki jumlah pengguna paling sedikit dan informasi-informasi yang berguna bagi perspektif manajemen.

d. Analisis Kebutuhan *Interface*

Interface pada sistem hanya pada keluaran *output*, sehingga pengguna akan berhubungan hanya dengan antarmuka *output*. Pada analisis interface ini terdapat beberapa tampilan yang diinginkan.

3.4 Perancangan Alur Sistem

Perancangan Alur sistem ini dilakukan dengan menggunakan bagan *Flowchart* dimana bagan ini akan lebih mudah dipahami secara detail tentang proses apa saja yang terjadi. Dalam *flowchart* bagan dibuat dengan menggunakan simbol – simbol yang telah disepakati.

Alur sistem yang akan dibangun adalah kontroller dalam hal ini Cisco WLC akan mengirimkan semua *Trap* ke *host* Linux yang menjalankan proses *daemon snmptrap*. *Trap* yang ada di kontroller pada dasarnya adalah segala aktifitas yang terjadi pada *Access Point (AP)*. Prosesnya detailnya yaitu semua *Access Point (AP)* yang terasosiasi dengan kontroller akan mengirimkan *Trap* dari dirinya ke kontroller tersebut, kemudian dari kontroller akan meneruskannya ke *host* yang menjalankan *daemon snmptrap*.

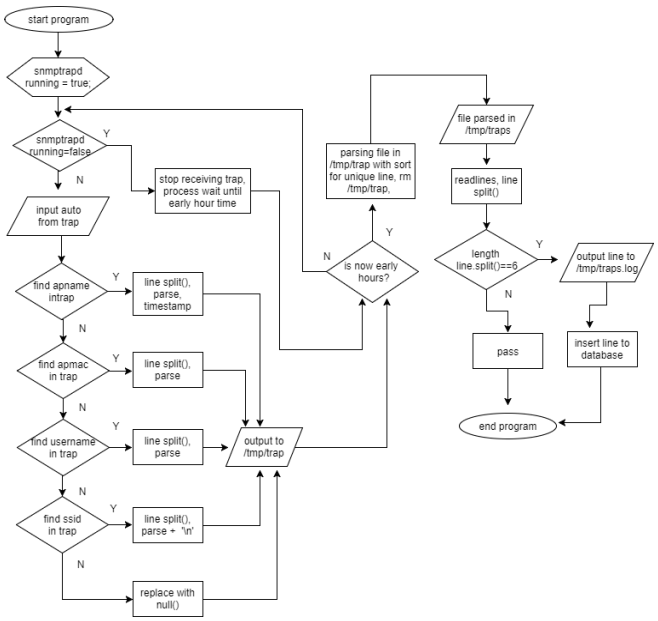
Dari sisi *host* kemudian proses akan berlanjut dengan mekanisme *host* menjalankan sebuah kode dalam bahasa pemrograman Python untuk menyortir *Trap* yang akan digunakan untuk ke proses berikutnya. Dalam hal ini proses hanya menyortir *trap* yang memiliki OID tertentu yang berhubungan dengan otentikasi *user* sehingga *trap* akan lebih rapi lagi setelah sebelumnya disortir pada proses internal di kontroller. Hal ini dilakukan untuk memastikan apabila sistem sortir pada kontroller kurang tepat maka kode program akan menangani input *Trap* tersebut supaya data yang di sortir lebih akurat.

Proses selanjutnya sistem akan melakukan penyortiran lagi dari proses yang dilakukan sebelumnya, hal ini dilakukan karena pada implementasinya setiap *Trap*

yang di kirimkan oleh kontroller kepada *host* pasti di jumpai *Trap* yang redundan sehingga harus di optimalisasi sebelum data *Trap* ini di proses kedalam basis data sistem. Proses sortir data ini dilakukan dengan menggunakan perintah internal yang adal di Linux tanpa melibatkan bahasa pemrograman Python, yaitu perintah *sort* diikuti opsi untuk mendeteksi setiap *trap* harus bersifat ***unique,*** dengan alasan bahwa menggunakan perintah internal di dalam linux akan lebih mempercepat proses sortir dan perintah yang dijalankan lebih mudah daripada perintah dengan menggunakan bahasa pemrograman Python untuk kasus sortir pada proses ini. Pada proses ini menjamin kelak *Trap* yang dimasukan ke basis data tidak ada yang redundan. Sebenarnya *Trap* redundan ini tidak menjadi masalah apabila jaringan yang digunakan berskala kecil dengan pengguna yang sedikit karena yang dibutuhkan adalah informasi berapa banyak sebuah *Access Point* di otentikasi oleh *user*, tetapi apabila jaringan yang di gunakan berskala besar seperti jaringan sebuah Universitas maka akan menjadi masalah karena data yang ditampung pada basis data akan sangat besar dan ini tidak optimal dilihat dari sisi penggunaan *resource.*

Kemudian proses selanjutnya adalah melakukan auto input kedalam basis data terhadap data *Trap* yang telah terkempul selama rentang waktu 1 jam. Secara otomatis sistem akan melakukan *auto input trap* yang di dapatkan dan dikumpulkan dari proses sebelumnya.

Proses terakhir adalah menampilkan *output* data yang tersimpan di dalam basis data yang diperoleh dari hasil proses sebelumnya dalam sebuah web. Pengguna akan melihat informasi yang dapat diperoleh dari analisis data yang sudah dilakukan.



Gambar 3.1 Flowchart Sistem

3.5 Implementasi Sistem

Implementasi sistem dilakukan dengan menggunakan bahasa pemrograman Python, beberapa *Command* dalam linux untuk melakukan *parsing* serta HTML untuk melakukan visualisasi via web. Keluaran yang diperoleh adalah informasi tentang *Access Point* (AP) mana yang memiliki jumlah pengguna paling kecil dan beberapa informasi yang berguna dari perspektif manajemen

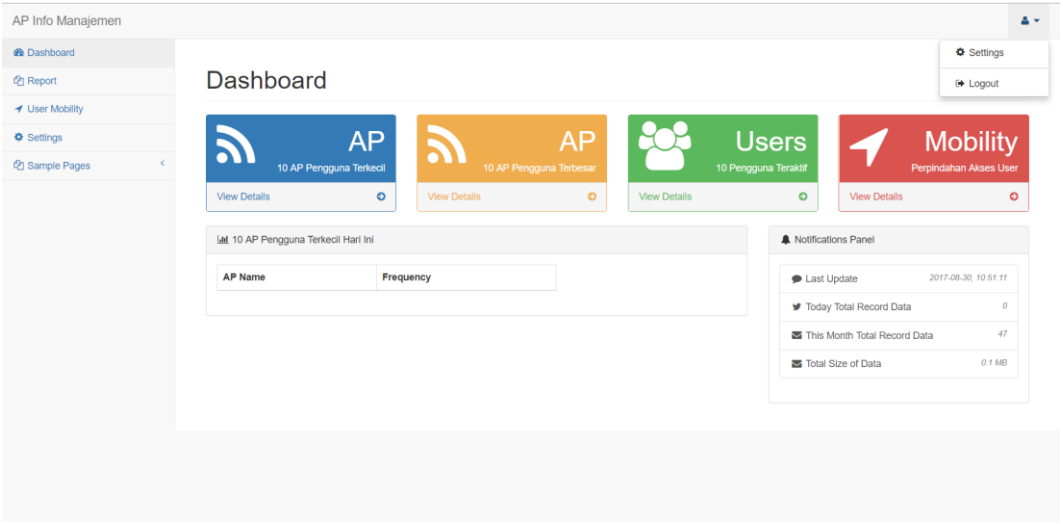
3.6 Pengujian

Sesuai dengan judul penelitian diatas, pengujian akan dilakukan dengan menjalankan sistem yang telah dibuat dengan mengotentikasi banyak *user* ke AP yang terhubung dengan kontroller kemudian pengujian juga dilakukan pada jaringan BSI UII. Pengujian ini akan mengirimkan data yang berasal dari WLC milik BSI UII, sehingga sistem nanti akan berjalan. Setelah sistem berjalan, Pengelola jaringan bisa mengambil keputusan berdasarkan perspektif manajemen.

BAB IV
DESAIN PERANCANGAN SISTEM

4.1 Desain *Interface*

Desain *interface* terbagi menjadi 4 *interface* penting yang merupakan menu dari halaman web yaitu *interface* pada halaman dashboard, *interface* report, *interface* mobility dan *interface* settings.

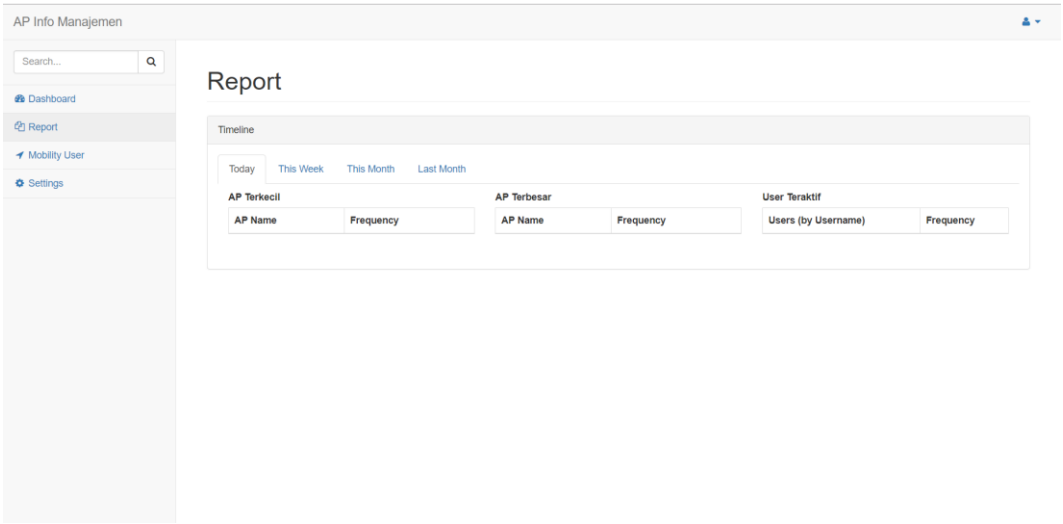


Gambar 4.1 Desain *Interface* Menu *Dashboard*

Desain *interface* dashboard pada Gambar 4.1 diatas berisi menu - menu umum yang terletak pada sebelah kiri halaman web yang berfungsi sebagai halaman navigasi untuk berpindah ke halaman yang lain. Menu navigasi yang terletak pada sebelah kiri halaman akan selalu ada dan dapat diakses di halaman manapun *user* pergi. Kemudian isi dari halaman dashboard disamping menu umum adalah menu - menu spesifik yang terdiri dari menu untuk melihat 10 AP dengan pengguna terkecil, 10 AP dengan pengguna terbersar, 10 pengguna teraktif yang menggunakan AP dan mobility. Pada saat berada di halaman dashboard secara *default* akan muncul tabel 10 pengguna terkecil. Hal ini dilakukan untuk membuat tampilan halaman dashboard lebih menarik dilihat disamping sudah ada menu untuk menampilkan 10 pengguna AP terkecil di bagian atas.

Pada halaman dasboard juga berisi panel notifikasi yang terdiri dari informasi berupa *last update, today total record data, this month total record data,* dan *total size of data. Last update* menampilkan informasi berupa kapan data terakhir yang di proses untuk ditampilkan di halaman, *today total record data* menampilkan informasi tentang banyaknya jumlah baris data yang ditampung pada basis data sistem hari ini, *this month total record data* menampilkan informasi tentang banyaknya jumlah baris data yang ditampung dalam basis data sistem pada bulan ini, dan *total size of data* menampilkan jumlah total ukuran dari data yang ditampung secara keseluruhan pada basis data dalam hitungan *Mega Bytes*(MB).

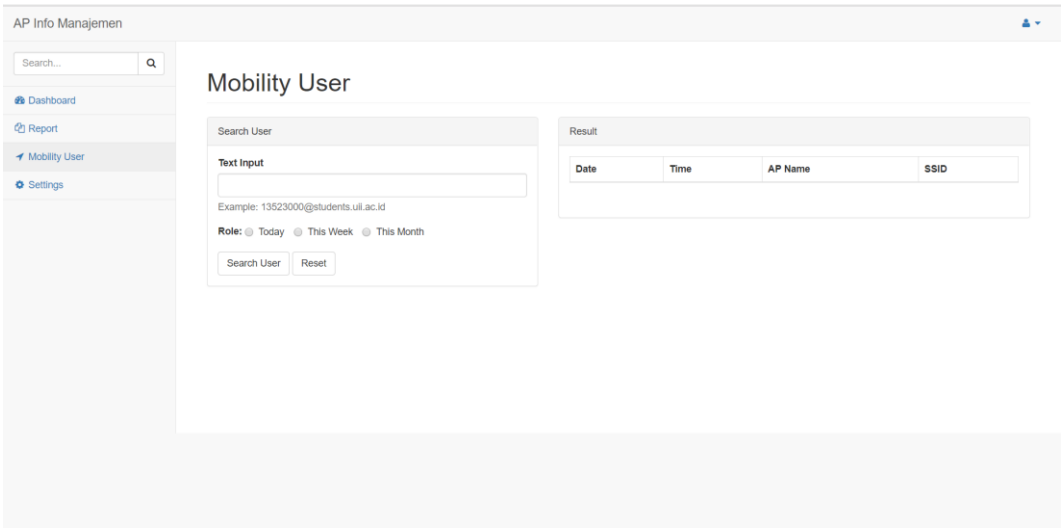
Pada bagian kanan atas halaman terdapat tanda *user* yang terdiri dari dua menu yang jika di klik akan menampilkan pilihan *setting* dan *logout.* Jika menu setting dipilih maka akan *redirect* ke menu setting yang sama yang terdapat pada halaman menu di sebelah kiri, dan menu *logout* akan mengeluarkan kita dari sistem. Menu ini ada di semua halaman dimanapun *user* pergi.



Gambar 4.2 Desain *Interface* Menu *Report*

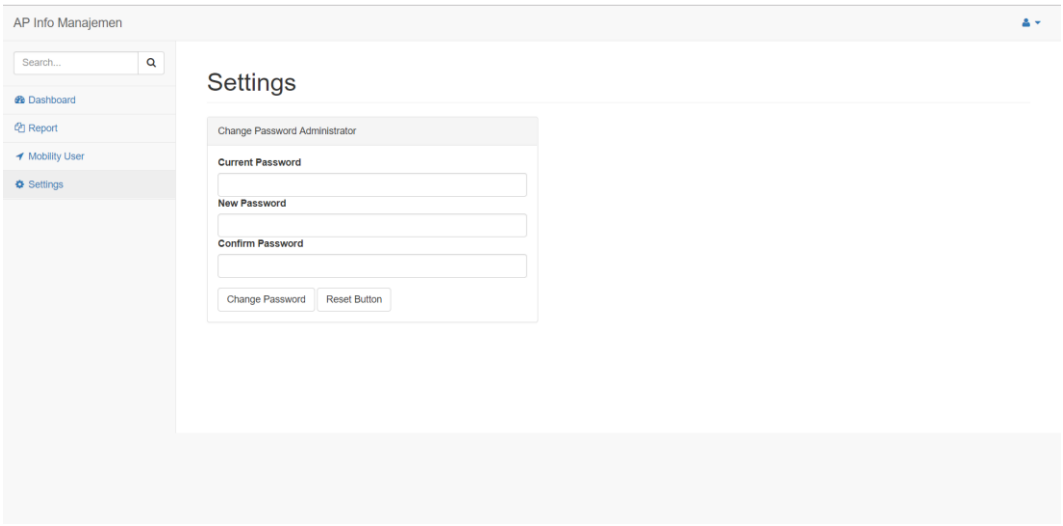
Desain *interface* menu report pada Gambar 4.2 berisi menu umum seperti pada Gambar 4.1, dan juga menu khusus pada halaman *report*. Menu *report* ini menampilkan informasi berupa laporan dari 10 AP dengan pengguna terkecil, 10 AP dengan pengguna terbesar, dan 10 *user* teraktif yang terbagi dalam menu today

(hari ini), *this week* (minggu ini), *this month* (bulan ini), dan *last month* (bulan kemarin).



Gambar 4.3 Desain *Interface* Menu *Mobility*

Desain *interface* menu *mobility* pada Gambar 4.3 digunakan untuk mencari mobilitas atau perpindahan *user* dalam mengakses jaringan nirkabel. Pada menu ini dapat diketahui kemana saja *user* berpindah tempat dengan cara memasukkan nama *user* yang dicari pada kolom *text input*, kemudian memilih *role* berupa *today*, *this week, atau This month. Role today* digunakan untuk mencari perindahan akses *user* untuk hari ini saja, *this week* digunkana untuk mencari perpindahan akses *user* untuk minggu ini, dan *this month* digunakan untuk mencari perpindahan akses *user* untuk satu bulan. Kemudian terdapat tombol *submit button* dan *reset button. Search user* berfungsi untuk mencari berdasarkan nilai-nilai yang ditelah di tentukan di atas, dan *reset* berfungsi untuk menghapus nilai yang telah dimasukkan. Pada sebelah kanan halaman mobility terdapat tabel yang berfungsi untuk menampilkan informasi hasil dari pencarian *user* yang dilakukan.

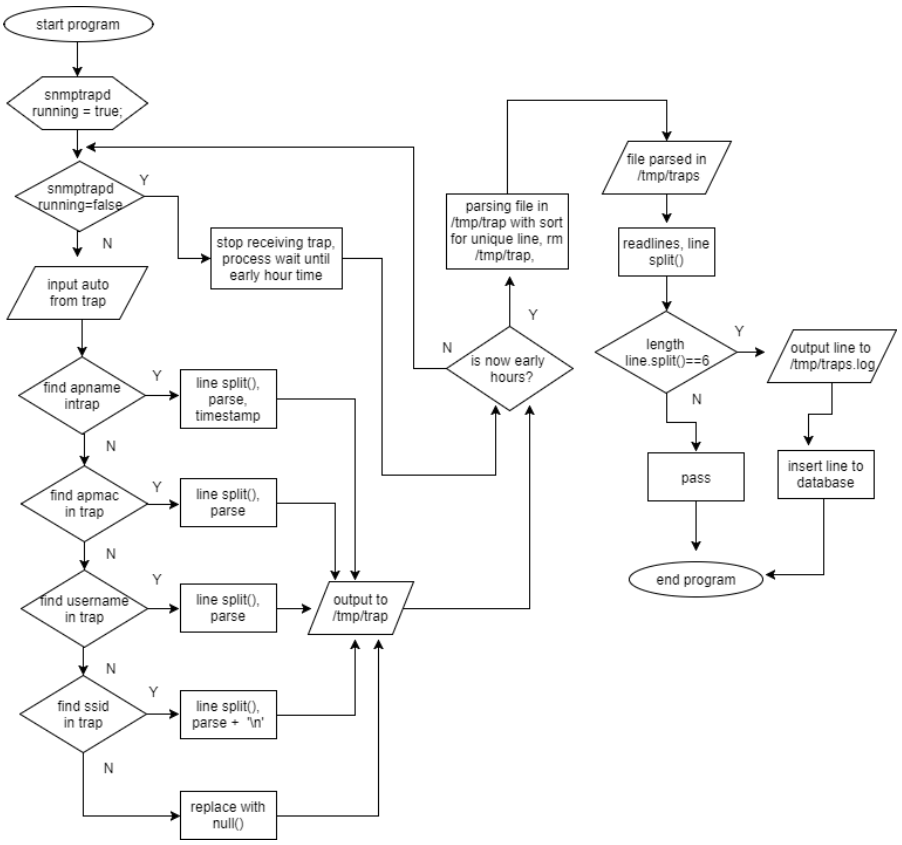


Gambar 4.4 Desain *Interface* Menu *Settings*

Desain *interface* menu *settings* pada Gambar 4.4 terdapat satu menu yaitu menu untuk merubah password administrator sistem web. Merubah password dapat dilakukan dengan memasukkan *password* sekarang pada kolom *Current password*, memasukkan *password* baru pada kolom *New Password*, dan memasukkan kembali *password* baru pada kolom *Confirm Password* yang berfungsi untuk memastikan bahwa password yang dimasukkan pada kolom *New Password* sama dengan yang dimasukkan pada kolom *Confirm Password*, dengan tujuan untuk menghindari kesalahan dalam memasukkan *password* sehingga nantinya administrator tidak kehilangan akses ke sistem karena *password* yang dirubah tidak sesuai.

4.2 Alur Sistem

Alur sistem yang akan dibuat dirancang dengan menggunakan *flowchart* yang menampilkan berbagai macam proses yang ada pada program secara keseluruhan sehingga bisa dilihat proses – proses apa saja yang ada di dalam program. Proses dimulai dari kondisi *start* dilanjutkan dengan proses *parsing* dan menyimpan hasil *parsing* kedalam basis data hingga akhir proses sistem. Alur sistem atau *flowchart* yang akan dibangun sebagai berikut (Gambar 4.5):



Gambar 4.5 Alur Sistem

Sistem yang dibuat akan mendapat input berupa *trap* dari proses snmptrapd yang berjalan dalam komputer *host* secara background. Pengguna hanya perlu mengatur input dari WLC agar otomatis mengirimkan *trap* nya ke komputer *host*, kemudian semua proses akan berjalan secara otomatis. Ketika sistem sedang berjalan dan menerima *trap*, terdapat proses pengecekan terhadap *trap* yang masuk ke komputer *host*. Karena data yang dibutuhkan untuk program hanya 4 variabel, maka terjadi proses percabangan untuk mendeteksi setiap *trap* yang masuk kedalam sistem. Jika *trap* yang masuk diketahui merupakan *trap* yang dicari oleh sistem, maka *trap* akan diambil kemudian di proses untuk mendapatkan informasi yang dibawa oleh *trap* tersebut. Informasi yang didapat kemudian disimpan kedalam file /tmp/trap.

Proses pengecekan *trap* ini terus menerus terjadi selama proses snmptrapd masih berjalan pada komputer *host*, dan proses akan terhenti ketika nilai *running* snmptrapd bernilai *false*. Sistem secara otomatis akan memproses *trap* yang sudah didapatkan setiap pergantian awal, jika waktu belum menunjukan keadaan tersebut maka *trap* yang diterima akan disimpan terlebih dahulu

Proses selanjutnya adalah *parsing. Parsing* kali ini dilakukan untuk mengeliminasi duplikasi baris data yang sama, karena pada proses menerima *trap* seringkali terjadi pengiriman suatu nilai variabel-variabel yang sama persis dari WLC. Setelah selesai, hasil dari data yang telah di-*parsing* akan dimasukkan ke dalam /tmp/*trap*s.

Proses selanjutnya yaitu membaca setiap baris data yang ada di dalam file /tmp/*trap*s.log kemudian memasukkan setiap baris data ke dalam basis data. Dalam file /tmp/*trap*s.log sudah di desain sedemikian rupa berdasarkan proses sebelumnya sehingga akan terdapat sebanyak 6 variabel data per barisnya, yang terdiri dari variabel *date, time, apname, macAP, username, SSID.* Karena dalam basis data juga terdapat 6 kolom tempat untuk menyimpan data, maka di cek terlebih dahulu untuk memastikan bahwa setiap baris data terdiri dari 6 variabel data. Jika lebih brati ditemukan masalah terdapat data yang telah dikumpulkan dan proses akan melewati data yang bermasalah tersebut sehingga proses hanya akan memasukkan data yang benar kedalam basis data.

Basis data yang digunakan terdiri dari 2 tabel, yaitu tabel authentikasi dan tabel admin. Tabel authentikasi digunakan untulk menyimpan data yang sudah di *parsing* oleh sistem. Pada tabel authentikasi terdiri dari 7 kolom untuk menyimpan data, yaitu kolom *id, date, time, apname, macap, user,* dan *ssid*. Kolom *id* digunakan untuk menyimpan id yang secara otomatis diisi oleh sistem dan bersifat *auto increment* dengan tipe data *integer,* kolom *date* dan *time* digunakan untuk menyimpan tanggal dan waktu dari data, kolom *apname* digunakan untuk menyimpan data yang berupa nama *access point*, kolom *macap* digunakan untuk menyimpan data yang berupa nilai MAC *Address* dari setiap *access point,* kolom user digunakan untuk menyimpan data yang berupa nama user, dan kolom *ssid* digunakan untuk menyimpan data yang berupa nama dari *wifi* yang digunakan.

Tabel admin berisi kolom *id, name, username,* dan *password*. Kolom *id* berfungsi untuk menyimpan data id yang di-*generate* oleh sistem basis data, kolom *name* berisi nama orang atau administrator, kolom *username* dan *password* digunakan untuk menyimpan data yang akan digunakan sebagai kombinasi untuk masuk ke dalam sistem. Kedua tabel tidak memiliki relasi satu sama lain dan bersifat independen.

Gambar 4.6 Basis data sistem

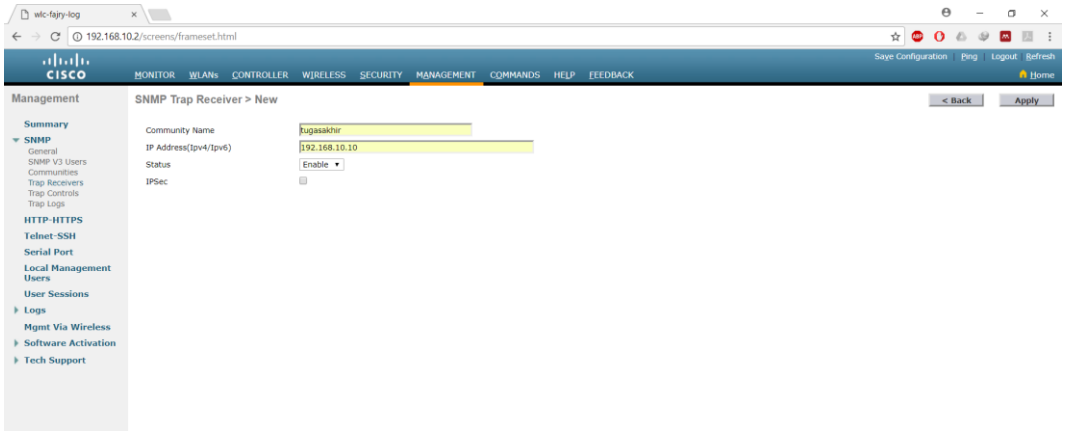
BAB V
IMPLEMENTASI DAN PENGUJIAN SISTEM

5.1 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:

A. 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*.



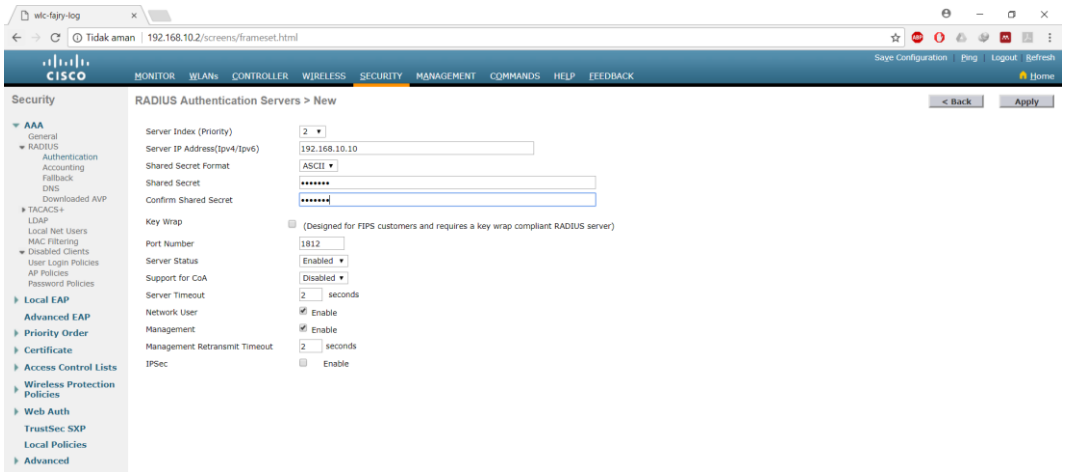
Gambar 5.1 Setting *Trap Receiver* WLC

B. 2 unit Cisco 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.

C. FreeRADIUS

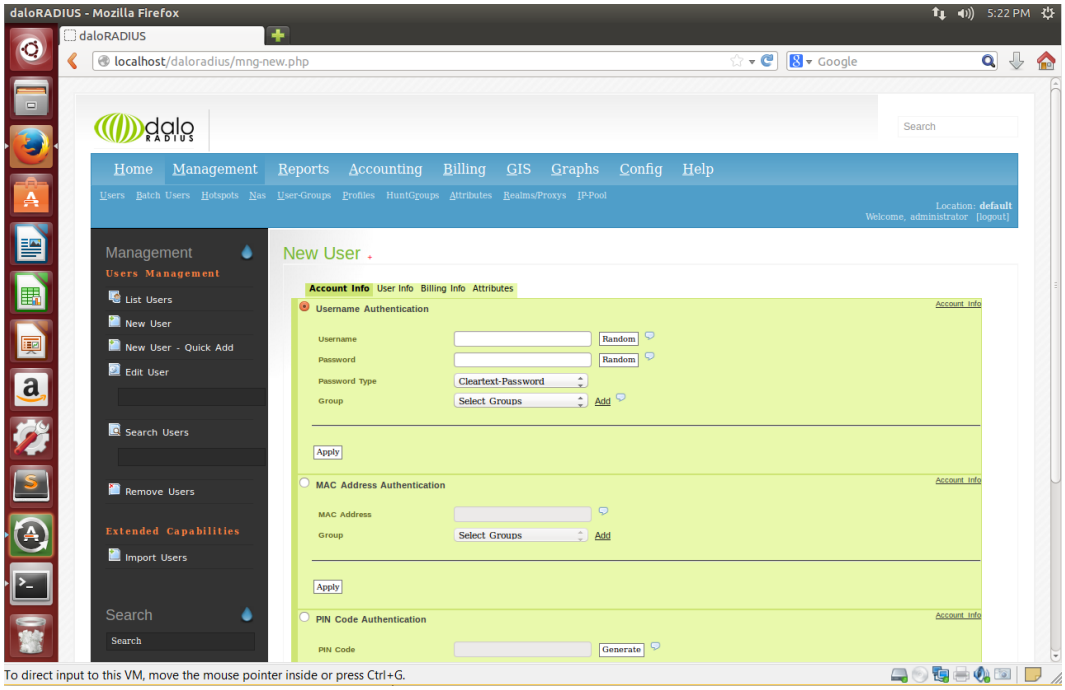
FreeRADIUS digunakan sebagai server RADIUS yang menangani proses otentikasi dari *user* untuk terhubung ke AP. Alurnya adalah setiap *user* yang akan terhubung ke AP untuk mengakses jaringan akan mengirimkan *request* ke FreeRADIUS, kemudian FreeRADIUS akan melakukan pengecekan terhadap *user*name dan 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. Setelah FreeRADIUS di atur sedemikian rupa, lakukan agar WLC mengetahui alamat IP dari *host* yang menjalankan layanan ini.



Gambar 5.2 Setting Radius di WLC

D. 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 atau perusahaan. Namun peneliti hanya menggunakan fungsi dasar saja yaitu menambah *user* untuk otentikasi agar *user* dapat terhubung ke dalam jaringan melalui AP.



Gambar 5.3 Tambah *User* Dalo Radius

E. SNMP Trap

Saat penulis melalukan implementasi terhadap sistem yang dibuat, data atau trap yang didapatkan dari WLC yang digunakan mengirimkan trap yang masih belum rapi yang berbentuk seperti pada Gambar 5.4 dibawah ini:

```
UDP: [192.168.10.2]:32768->[192.168.10.10]:162
iso.3.6.1.2.1.1.3.0 0:1:18:10.00
iso.3.6.1.6.3.1.1.4.1.0 iso.3.6.1.4.1.9.9.599.0.4
iso.3.6.1.4.1.9.9.599.1.3.1.1.1.0 "F4 37 B7 9D D7 7E "
iso.3.6.1.4.1.9.9.513.1.1.1.1.5.0 "AP.LOG.NO2"
iso.3.6.1.4.1.9.9.599.1.3.1.1.8.0 "00 B0 E1 9F D8 A0 "
iso.3.6.1.4.1.9.9.513.1.2.1.1.1.0 1
iso.3.6.1.4.1.9.9.599.1.3.1.1.10.0 192.168.10.22
iso.3.6.1.4.1.9.9.599.1.3.1.1.27.0 "trial"
iso.3.6.1.4.1.9.9.599.1.3.1.1.28.0 "cisco-log"
```

Gambar 5.4 Trap yang dikirim oleh WLC

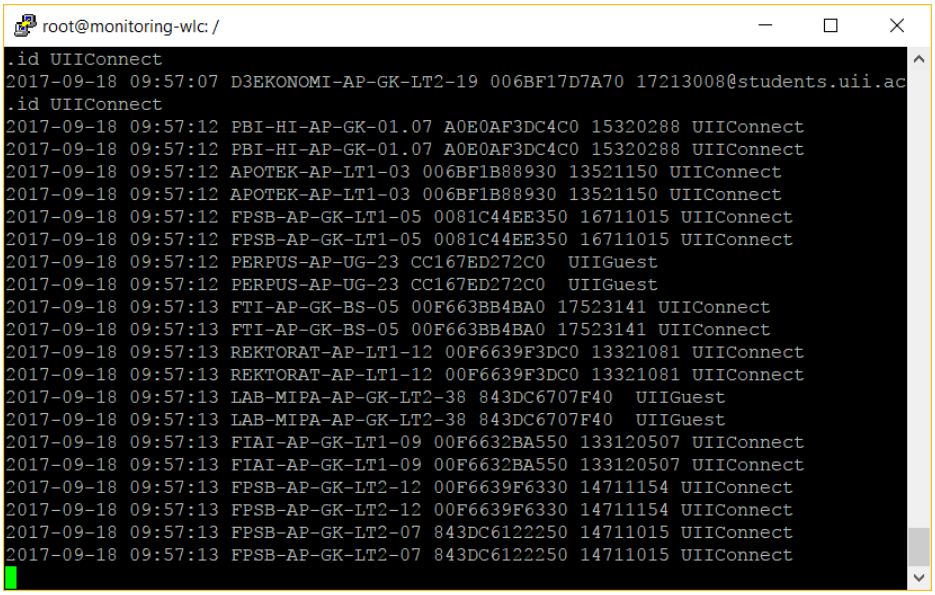
Dengan menggunakan teknik *parsing* yang ditulis dengan bahasa pemrograman Python, penulis dapat mengambil data yang dibutuhkan berdasarkan *oid* yang sesuai dan merapikan setiap data yang masuk seperti pada Gambar 5.5 berikut:

```
fajry@ubuntu:~/tugasakhir$ tail -f /tmp/traps
2017-09-04 15:42:59 AP.LOG.NO1 00B0E19FD060 usertest cisco-log
2017-09-04 15:42:59 AP.LOG.NO1 00B0E19FD060 usertest cisco-log
2017-09-04 15:42:59 AP.LOG.NO1 00B0E19FD060 usertest cisco-log
2017-09-04 15:42:59 AP.LOG.NO1 00B0E19FD060 usertest cisco-log
2017-09-04 15:43:10 AP.LOG.NO1 00B0E19FD060 trial cisco-log
2017-09-04 15:43:10 AP.LOG.NO1 00B0E19FD060 trial cisco-log
```

Gambar 5.5 Trap yang telah di parsing

5.2 Pengujian Sistem

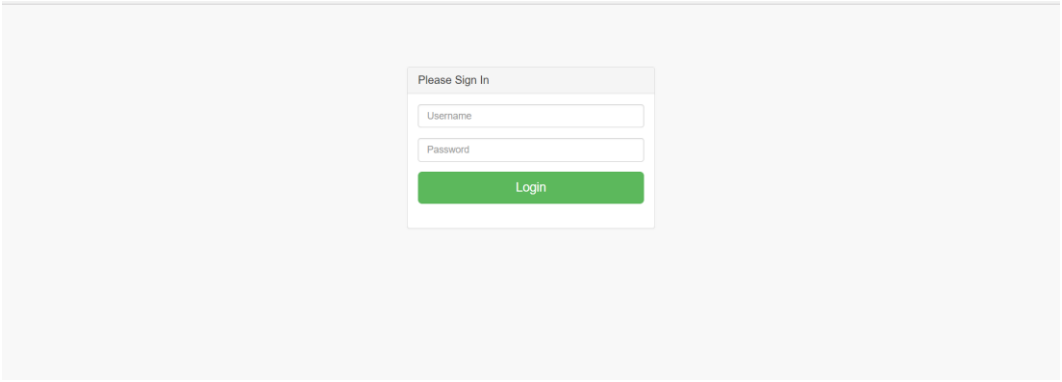
Pengujian sisem dilakukan dengan menggunakan server *Virtual Private Server* (VPS) yang dibangun oleh BSI untuk menjalankan sistem yang sudah penulis buat. Hal yang berbeda pada pengujian ini dengan implementasi yang dilakukan oleh penulis terletak pada WLC yang digunakan. Jadi penulis hanya mengkopi 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.



Gambar 5.6 Trap yang diterima

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 beberapa hasil pengujian yang penulis lakukan pada sistem yang dijalankan di VPS:

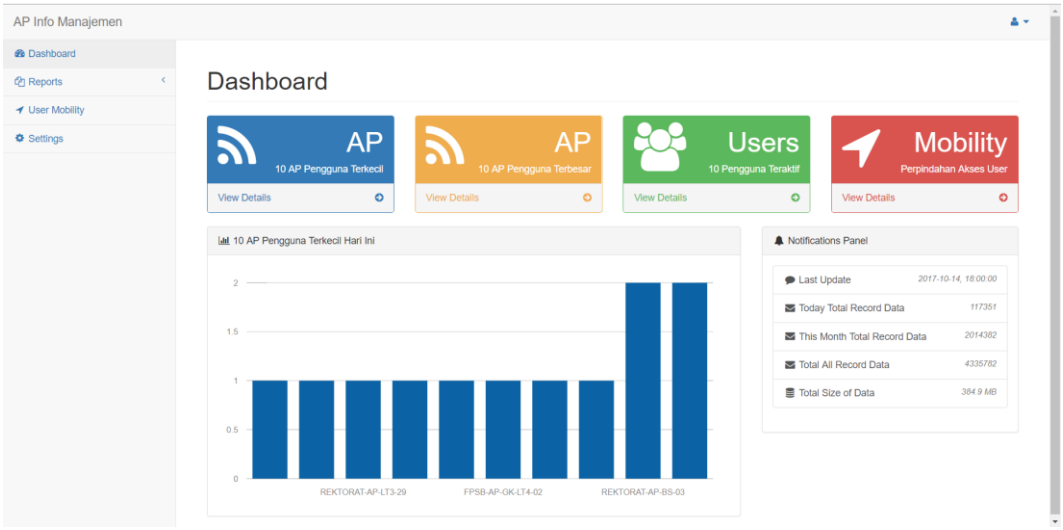
A. Tampilan Login



Gambar 5.7 Tampilan Login

Pengujian pertama dilakukan pada halaman *login* untuk menguji keberhasilan otentikasi untuk masuk ke sistem. Pengujian berhasil dilakukan dan hasilnya sistem bisa mengenali dengan tepat apabila kombinasi antara *username* dan *password* sudah atau belum tepat. Ketika kombinasi sudah tepat, sistem akan melakukan *redirect* ke halaman dashboard, dan ketika kombinasi tidak tepat, user akan mendapat pemberitahuan jika *login* yang dilakukan gagal dan user akan diarahkan kembali ke halaman *login* untuk melakukan *login* ulang.

B. Tampilan Menu Dashboard

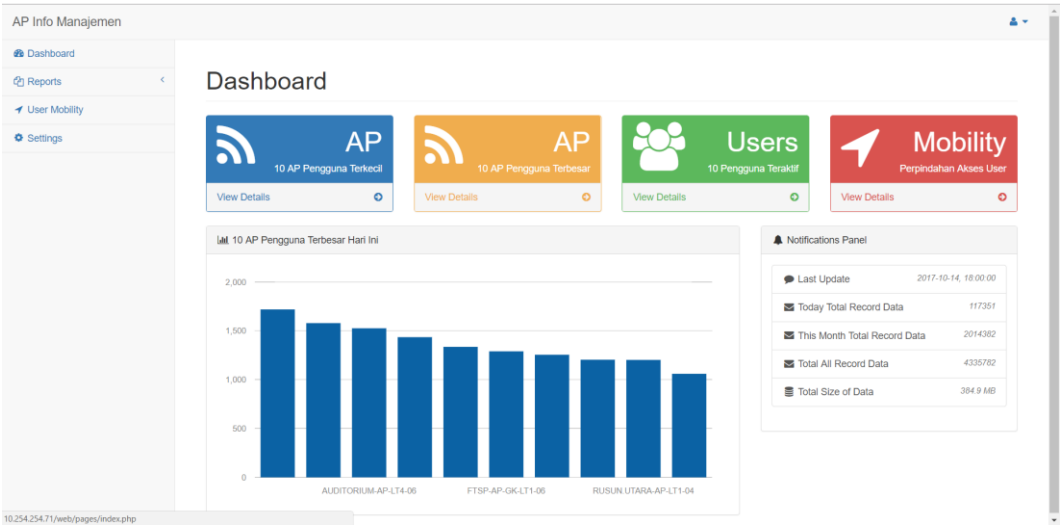


Gambar 5.8 Tampilan Pengujian Menu Dashboard

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 dengan menggunakan *chart* berbentuk batang yang telah diurutkan dimulai dari yang terkecil dari sebelah kiri.

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), *total all record data* (jumlah total trap yang diterima dan disimpan dalam *database),* dan *total size of data* (jumlah total ukuran data yang tersimpan di dalam basis data sistem) dalam hitungan *Mega Bytes* (MB)

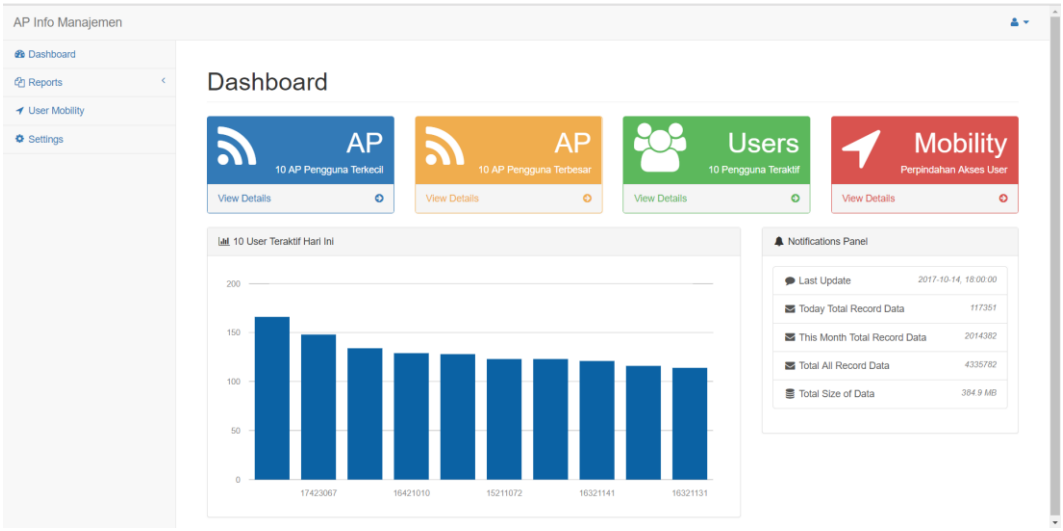
C. Tampilan Menu AP Terbesar



Gambar 5.9 Tampilan Pengujian Menu AP Terbesar

Pengujian terhadap menu 10 AP Pengguna terbesar pada halaman dashboard berjalan sukses. Halaman ini menampilkan 10 AP dengan total pengguna terbesar dalam waktu hari ini, waktu dimana pengelola yang berwewenang sedang mengakses halaman ini. Data yang tampil berupa data AP dengan pengguna yang paling besar di lingkungan UII dalam bentuk grafik batang yang telah diurutkan berdasarkan jumlah AP yang paling besar dimulai dari sebelah kiri. Pada halaman ini tampil juga tab *notification panel* sama seperti pada halaman dashboard.

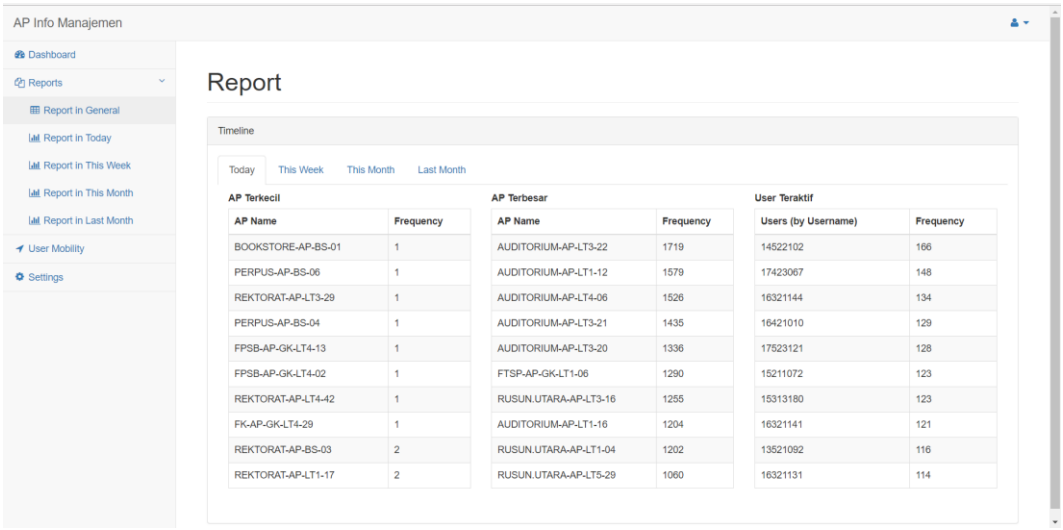
D. Tampilan menu *User* Teraktif



Gambar 5.10 Tampilan Pengujian Menu User Teraktif

Pengujian pada menu ini juga sukses. Pada halaman ini ditampilkan sebuah grafik yang berisi 10 *user* yang paling aktif dalam menggunakan jaringan nirkabel. Aktif berarti bahwa frekuensi *user* dalam terhubung ke sebuah AP tinggi, namun bisa jadi karena user berpindah – pindah tempat sehingga sistem mendeteksinya.

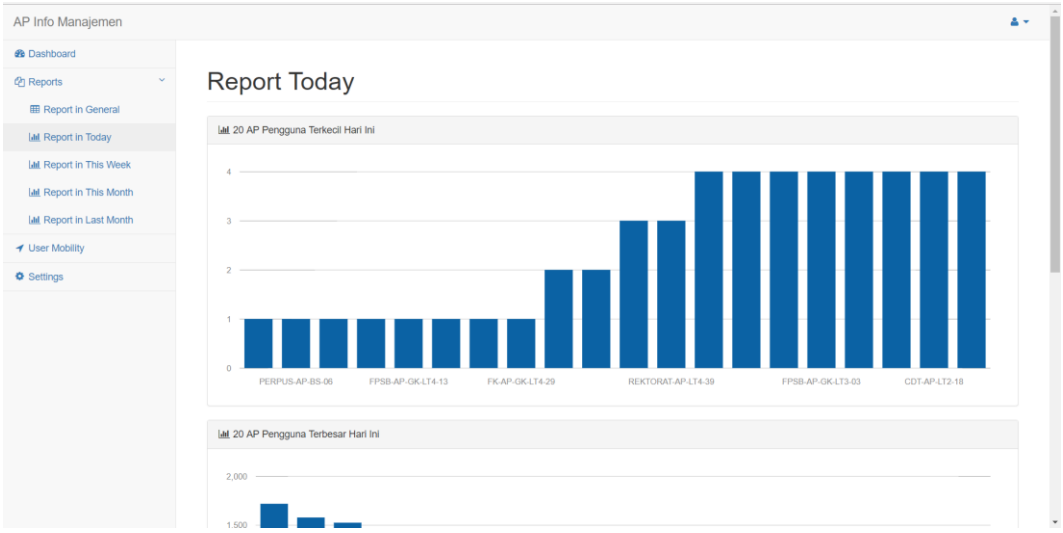
E. Tampilan Menu Reports - Report in General



Gambar 5.11 Tampilan Pengujian Menu Report in General

Pengujian pada halaman *report in general* menunjukan gambaran secara umum yang ditampilkan dengan menggunakan tabel dengan data yang ditampilkan berupa AP Terkecil, AP Terbesar, dan User Teraktif yang menggunakan jaringan dengan jumlah 10 data. Pada halaman ini tampilan dibentuk dengan menggunakan tab yang menampilkan gambaran data secara umum dalam hitungan *today* (hari ini), *this week* (minggu ini), *this month* (bulan ini), dan *last month* (bulan kemarin).

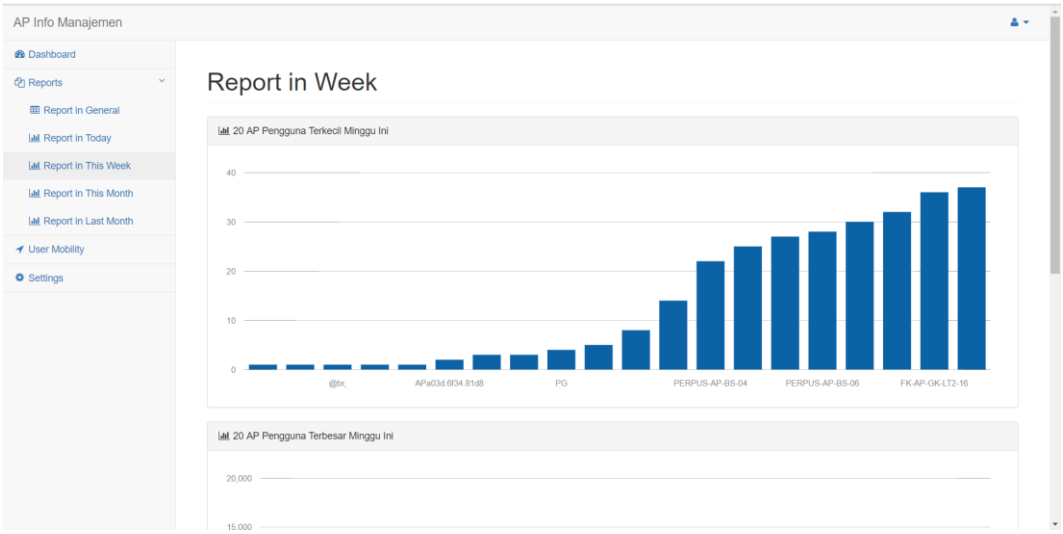
F. Tampilan Menu Reports – Report in Today



Gambar 5.12 Tampilan Pengujian Menu Report in Today

Pengujian pada menu Report in Today telah sukses dilakukan. Pada halaman Report in Today ini menampilkan report data dalam bentuk grafik berupa 20 AP dengan pengguna terkecil hari ini yang telah diurutkan dimulai dari yang paling kecil di sebelah kiri kemudian nilai terkecil kedua diletakan persis di samping kanannya, 20 AP dengan pengguna terbesar hari ini yang telah diurutkan dimulai dari AP yang paling besar di sebelah kiri kemudian nilai terbesar urutan kedua di sebelah kanannya, dan 20 User teraktif hari ini yang telah di urutkan dimulai dari nilai yang paling besar dan kemudian nilai terbesar kedua di sebelah kanannya dan seterusnya.

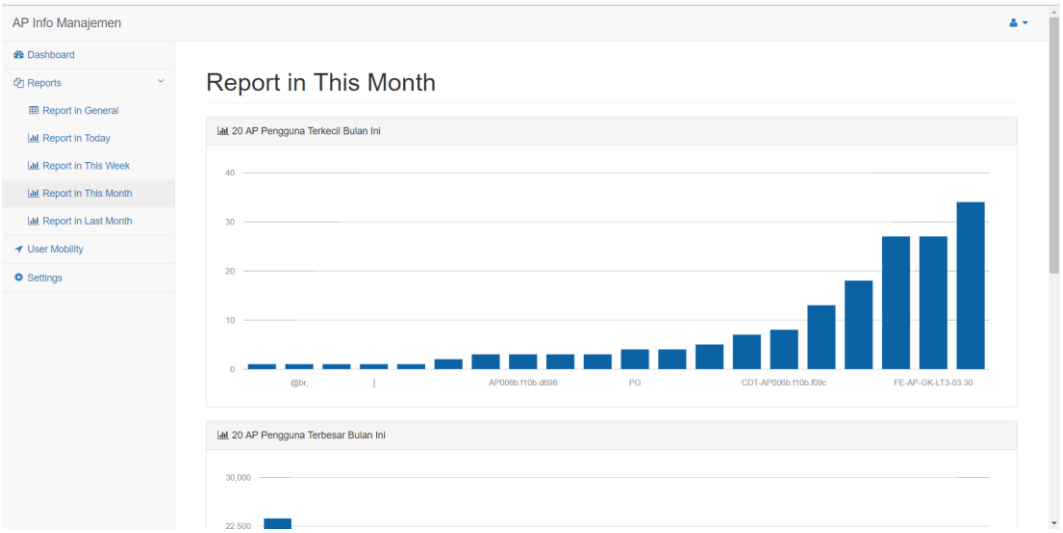
G. Tampilan Menu Reports – Report in Week



Gambar 5.13 Tampilan Pengujian Menu Report in Week

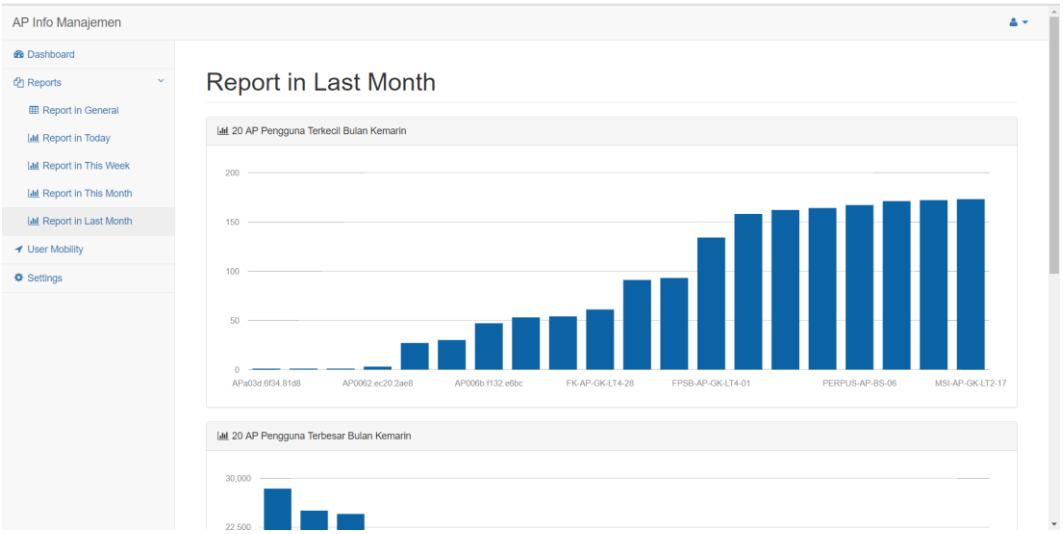
Pengujian pada halaman Report in Week berjalan sukses. Tampilan pada halaman ini sama persis seperti pada halaman Report in Roday, yang membedakan adalah data yang ditampilkan yaitu berupa 20 AP dengan pengguna terkecil dalam minggu ini, 20 AP dengan pengguna terbesar dalam minggu ini, dan 20 User teraktif hari ini.

H. Tampilan Menu Reports – Report in This Month



Gambar 5.14 Tampilan Pengujian Menu Report in This Month

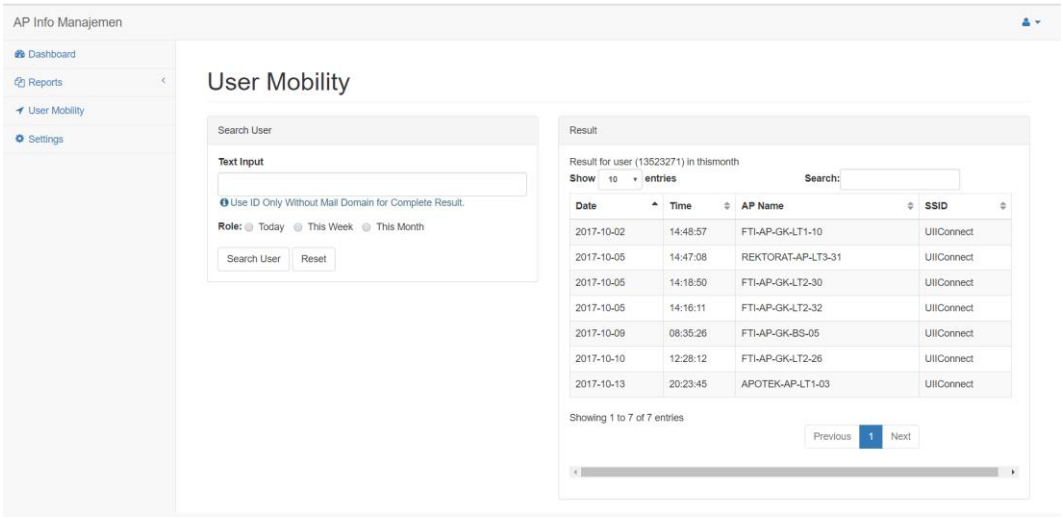
I. Tampilan Menu Reports – Report in Last Month



Gambar 5.15 Tampilan Pengujian Menu Report in Last Month

Pengujian pada halaman Report in Last Month berjalan sukses. Sama seperti tampilan pada halaman report sebelumnya, halaman Report in Last Month ini menampilkan 20 AP dengan pengguna terkecil bulan kemarin, 20 AP dengan pengguna terbesar bulan kemarin, dan 20 User teraktif bulan kemarin dalam bentuk grafik batang.

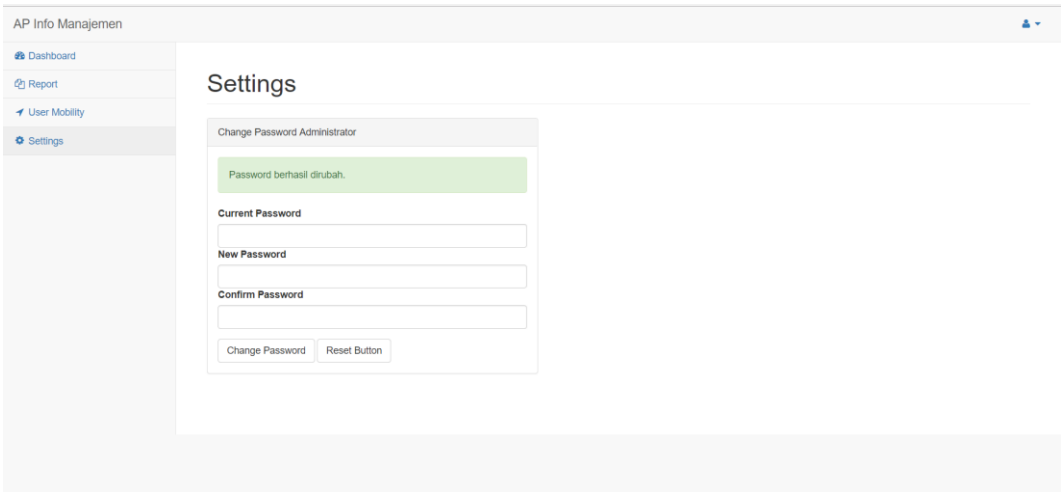
J. Tampilan Menu Mobility



Gambar 5.16 Tampilan Pengujian Menu Mobility

Pengujian pada menu mobility berjalan sukses. Pengujian dilakukan dengan memasukkan ID user disertai dengan memilih *role* untuk menentukan hasil pencarian. Terdapat 3 pilihan yang tersedia dalam *role*, yaitu *today* (perpindahan hari ini), *this week* (perpindahan selama minggu ini), dan *this month* (perpindahan selama satu bulan terakhir). Penulis mencoba memasukan ID kedalam kolom *search user*, kemudian sistem bisa menampilkan perpindahan akses penulis pada kolom *result.* Hasil yang ditampilkan kedalam tabel bisa diurutkan berdasarkan tanggal, waktu, nama AP, ataupun berdasarkan SSID.

K. Tampilan Menu Setting



Gambar 5.17 Tampilan Pengujian 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.

5.3 Hasil Pengujian

Hasil pengujian akan memperlihatkan rangkuman pengujian sistem sesuai dengan sub-bab diatas dalam bentuk tabel. Hasil Pengujian dilihat pada Tabel 5.1 berikut:

Tabel 5.1 Tabel Hasil Pengujian

No.	Nama	Fungsi	Hasil Pengujian
1	Login	Otentikasi untuk mengakses sistem	Sukses
2	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
3	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
4	Menu Mobility	Mencari informasi terkait perindahan tempat akses *user* dalam jaringan	Sukses
5	Menu Setting	Merubah *password* akses ke sistem untuk Administrator	Sukses

BAB VI
KESIMPULAN DAN SARAN

6.1 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.

6.2 Saran

Dari sistem yang dibuat ini masih terdapat kekurangan dan kelemahan yang sebenarnya dapat dikembangkan lebih lanjut. Melalui hasil diskusi bersama 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

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.

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

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

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.

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.

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

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

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

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

Pradikta, Reza., Affandi, Achmad., dan Setijadi, Eko. 2013. *Rancang Bangun Aplikasi Monitoring Jaringan dengan Menggunakan Simple Network Management Protocol.* Surabaya: JURNAL TEKNIK POMITS Vol. 2, No.1, (2013) ISSN: 2337-3539 (2301-9271 Print).

LAMPIRAN