

## Peningkatan Keamanan Wireless Pada Jaringan Komputer di Universitas Amikom Menggunakan Protokol IEEE802.1X

Ichsan Wiratama\*<sup>1</sup>, Putu Sugiartawan<sup>2</sup>

<sup>1</sup>Fakultas Ilmu Komputer, Universitas AMIKOM, Yogyakarta, Indonesia, <sup>2</sup>Teknik Informatika, STMIK STIKOM Indonesia, Bali, Indonesia

e-mail: \*<sup>1</sup>[x-sun@amikom.ac.id](mailto:x-sun@amikom.ac.id), <sup>2</sup>[putu.sugiartawan85@gmail.com](mailto:putu.sugiartawan85@gmail.com)

### Abstrak

*Konfigurasi access point yang digunakan untuk koneksi wireless di amikom di konfigurasi secara manual satu persatu. Setiap access point dikonfigurasi dengan menggunakan beberapa SSID berdasarkan departemen yang akan terkoneksi ke access point tersebut. Penggunaan beberapa SSID dalam satu access point ternyata mempunyai akibat buruk dalam performansi jaringan, dari hasil pengujian, untuk access point yang dikonfigurasi dengan lebih dari empat SSID terasa koneksi yang sangat lambat. Standar keamanan yang digunakan untuk koneksi dari user ke access point adalah WPA Personal, dimana WPA Personal ini bisa dikatakan sangat lemah karena untuk setiap SSID akan menggunakan user dan password yang sama untuk semua pengguna, hal ini sering menjadi penyebab kebocoran akses.*

*Untuk memperbaiki keamanan jaringan dan memudahkan penulis melakukan maintenance terhadap jaringan maka penulis mencoba untuk menggunakan protokol IEEE 802.1X yang dihubungkan dengan RADIUS dan kontroller access point sehingga diharapkan konfigurasi dan maintenance wireless network dapat dilakukan secara centralized, administrasi user dan password juga dapat dilakukan secara terpusat menggunakan radius server dan juga tingkat keamanan yang lebih baik dengan menggunakan pengamanan WPA Enterprise yang ada di protokol IEEE 802.1X*

**Kata kunci**— *Wireless, IEEE 802.1X, Network, Internet, Amikom*

### Abstract

*The access point configuration used for wireless connections in Amikom is manually configured one by one. Each access point is configured using several SSIDs based on the department that will connect to the access point. The use of multiple SSIDs in one access point turned out to have a bad effect on network performance, from the test results, for access points configured with more than four SSIDs, the connection was very slow. The security standard used for connection from the user to the access point is WPA Personal, where WPA Personal can be said to be very weak because for each SSID it will use the same user and password for all users, this is often the cause of access leaks.*

*To improve network security and make it easier for the author to do maintenance on the network, the author tries to use the IEEE 802.1X protocol that is connected with RADIUS and access point controllers so that the configuration and maintenance of wireless networks can be centralized, user administration and passwords can also be centralized server radius and also a better level of security using WPA Enterprise security in the IEEE 802.1X protocol.*

**Keywords**— *Wireless, IEEE 802.1X, Network, Internet, Amikom*

## 1. PENDAHULUAN

Untuk dapat terkoneksi ke dalam jaringan internet yang disediakan di Universitas Amikom Yogyakarta, media penghubung yang digunakan adalah menggunakan kabel dan juga tanpa kabel (wireless). Masing-masing media penghubung memiliki kelebihan dan kekurangan masing-masing. Media kabel mempunyai kelebihan antara lain koneksi yang stabil, kecepatan koneksi yang lebih baik dibandingkan wireless karena media kabel mendukung bandwidth sampai dengan 1 gbps sesuai dengan kategori dari kabel dan perangkat yang digunakan. Kekurangan dari media kabel adalah fleksibilitas dan kepraktisannya yang kurang baik hal ini disebabkan pemasangan kabel yang harus secara permanen, tidak dapat dipindah-pindah dengan mudah. Pada media wireless, kelebihan yang didapat adalah kepraktisan dan kemudahan penggunaan. Sedangkan kelemahan media wireless adalah koneksi yang tidak sebaik kabel dalam hal kestabilan koneksi, bandwidth yang jauh lebih kecil, dengan semakin banyaknya pengguna dalam 1 access point menyebabkan kualitas koneksi yang semakin jelek.

Sebelum penelitian ini dilakukan, konfigurasi access point dilakukan secara manual pada setiap access point yang ada, konfigurasi yang dilakukan adalah mengatur user dan password yang digunakan untuk koneksi ke access point, mendaftarkan mac address dari setiap perangkat yang akan digunakan, mengatur SSID yang akan digunakan pada setiap network yang akan dilayani oleh access point. Kendala yang dihadapi dengan konfigurasi secara manual ini adalah repotnya proses konfigurasi yang harus dilakukan pada setiap titik access point, setiap pengguna mengeluhkan proses login yang berulang kali harus dilakukan ketika berpindah tempat sehingga harus berpindah access point yang digunakan.

Dengan penelitian ini, penulis mencoba untuk menyelesaikan permasalahan yang dihadapi dalam manajemen layanan wireless dan hotspot dengan menggunakan fitur-fitur layanan yang ada di protocol IEEE 802.1X seperti tingkat keamanan wireless yang menggunakan standar WPA tingkat enterprise dimana dilihat dari jumlah pengguna wireless yang sudah termasuk dalam kelas enterprise. Fitur manajemen user yang dilakukan secara terpusat (centralized) yang memudahkan seorang administrator menambahkan data user dan password hanya di satu titik tetapi dapat digunakan di seluruh jaringan yang ada di Amikom.

## 2. METODE PENELITIAN

Universitas Amikom Yogyakarta mempunyai peranan yang besar dalam dunia pendidikan sebagai pusat pengembangan ekonomi kreatif untuk meningkatkan daya saing bangsa, telah membuktikan mampu mengatasi berbagai kesulitan dan hambatan dalam pengelolannya. Saat ini kepercayaan masyarakat cukup baik, dibuktikan diantaranya dengan meningkatnya jumlah mahasiswa dari tahun ke tahun pada 2014 mempunyai 12.882 mahasiswa untuk program studi. Mulai dari program Studi Diploma III Manajemen Informatika, Program Studi Diploma III Teknik Informatika, Program Studi S1 Sistem Informasi, Program Studi S1 Teknik Informatika dan Program Studi S2 Magister teknik Informatika. Bahkan Program Magister Teknik Informatika dipercaya oleh Direktorat Jendral pendidikan Tinggi dikala itu bersama 5 Perguruan Tinggi lain seperti (Universitas Indonesia, Universitas Gadjah Mada, Institut Teknologi Bandung, Institut sepuluh November Surabaya dan Universitas Bina Nusantara) yang diberikan hibah sebagai proyek percontohan Pendidikan Jarak Jauh (PJJ).

Pada masa mendatang, Universitas Amikom berkeinginan untuk tetap lebih maju sesuai dengan jaman dan tantangannya yang terus berubah. Oleh karenanya dengan semakin berkembang dan dewasanya Universitas Amikom Yogyakarta serta kebutuhan untuk memenuhi kepercayaan masyarakat dan tuntutan perubahan jaman yang sulit diprediksi, diperlukan strategi dan sasaran pengembangan yang terencana, sistematis dan terukur. Dengan memanfaatkan berbagai keunggulan strategis yang dimiliki secara optimal, evaluasi kondisi saat ini serta berpijak pada visi dan misi Universitas Amikom Yogyakarta, maka perlu disusun sebuah

rencana strategis yang akan memberikan arah serta menjadi acuan bagi Universitas Amikom Yogyakarta dalam perjalanan kedepan.

### 2.1 Wireless Local Area Network

Jaringan Wireless LAN hampir sama dengan jaringan LAN Kabel, akan tetapi setiap node pada WLAN menggunakan piranti Wireless agar dapat berhubungan dengan jaringan, node pada WLAN menggunakan kanal frekuensi yang sama dan SSID yang menunjukkan identitas dari piranti Wireless. Yang membedakan jaringan kabel LAN, jaringan Wireless memiliki dua model yang dapat digunakan : infrastruktur dan Ad-Hoc. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah Access point pada WLAN atau LAN. Jaringan ad hoc adalah jaringan bersifat sementara tanpa bergantung pada infrastruktur yang ada dan bersifat independen. Ad-Hoc Network adalah jaringan Wireless yang terdiri dari kumpulan mobile node (mobile station) yang bersifat dinamik dan spontan, dapat diaplikasikan di mana pun tanpa menggunakan jaringan infrastruktur (seluler ataupun PSTN) yang telah ada.

Wireless Local Area Network (WLAN) merupakan teknologi LAN yang menggunakan frekuensi dan transmisi radio sebagai media penghantarnya pada area tertentu menggantikan fungsi kabel [1]. Konfigurasi WLAN terdiri dari akses point yang dihubungkan ke pengguna melalui media udara (frekuensi dan transmisi radio) seperti pada Gambar 1.



Gambar 1 Wireless Local Area Network

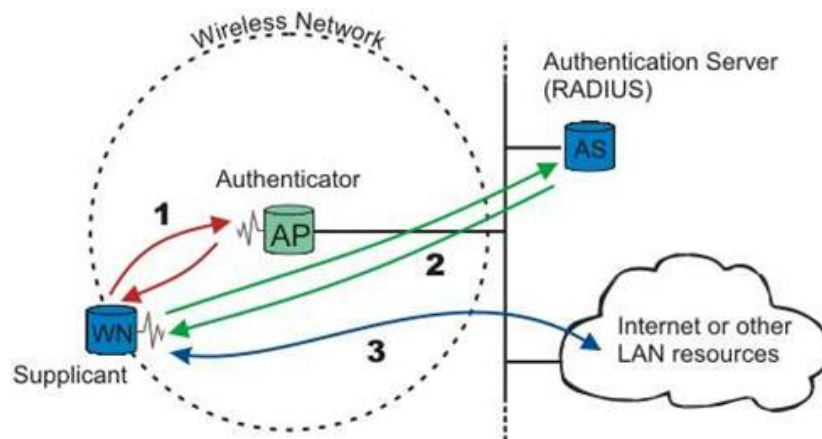
Remote Authentication Dial-In User Service (RADIUS) adalah sistem otentikasi dan manajemen akun yang digunakan oleh banyak penyedia layanan Internet untuk mengotentikasi pengguna mereka. Radius juga cocok untuk otentikasi nirkabel. RADIUS hanya mengotentikasi pengguna. Bagian yang sangat penting dari RADIUS adalah interoperabilitasnya, yang memungkinkan server untuk berkomunikasi dengan server lain yang didasarkan pada protokol yang sama [2]. RADIUS merupakan suatu protokol yang berbasis client/server dan software yang memungkinkan server akses jarak jauh untuk berkomunikasi dengan central server untuk melakukan otentikasi dan otorisasi pengguna dial-in yang akan mengakses ke sistem dan layanan yang dibutuhkan. RADIUS memungkinkan suatu perusahaan atau lembaga untuk memelihara profil pengguna pada suatu basisdata yang terpusat yang dapat diakses oleh server lain secara remote. Protokol ini menyediakan dukungan keamanan yang lebih baik, memungkinkan suatu lembaga atau perusahaan untuk membuat suatu aturan yang dapat diimplementasikan pada pengelolaan satu titik yang terpusat. Dengan adanya layanan yang terpusat juga berarti dapat mempermudah dokumentasi pada billing dan statistik network. RADIUS yang dibuat oleh Livingston, secara de facto merupakan standar yang digunakan oleh banyak perusahaan yang juga diusulkan sebagai standar IETF. Ketika server RADIUS dikonfigurasi untuk digunakan pada otentikasi, hanya kebijakan di server RADIUS yang

digunakan. Jika perubahan diperlukan dalam kebijakan akses jaringan apa pun, modifikasi kebijakan hanya dapat dilakukan di server RADIUS [3].

## 2.2 Protokol IEEE 802.1X

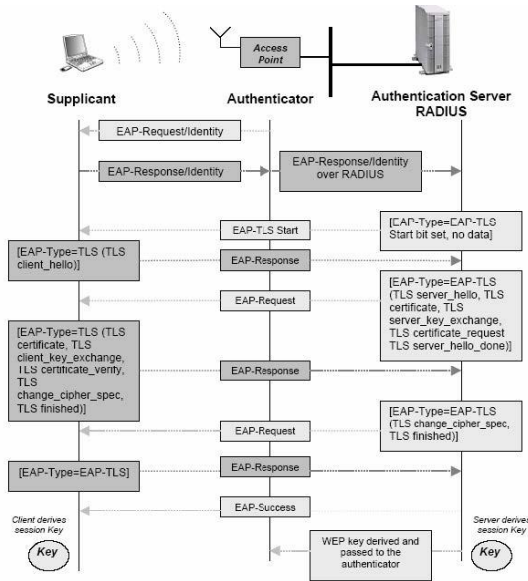
Keamanan merupakan hal yang sangat penting dalam jaringan wireless. Pada network wireless, IEEE mendukung standar 802.1X untuk meningkatkan keamanan transmisi data. Port-based network access control memungkinkan seorang administrator network untuk membatasi penggunaan IEEE 802 Lan service access points (ports) untuk mengamankan komunikasi antara peralatan yang sudah di otentikasi dan di otorisasi IEEE Std 802.1X menentukan suatu arsitektur, elemen fungsional dan protokol yang mendukung mutual authentication antar client yang menggunakan port yang terpasang pada LAN yang sama dan mengamankan komunikasi antar ports.

Keunggulan protokol IEEE 802.1X adalah antara lain, mengembangkan standar yang sudah ada seperti EAP (RFC 228), RADIUS (RFC 2138, 2139), dapat dioperasikan untuk identifikasi user, otentikasi secara terpusat, identifikasi berdasarkan Network Access identifier (RFC 2486) yang mengaktifkan dukungan untuk roaming access di ruang publik (RFC 2607). Skema arsitektur IEEE 802.1X ditunjukkan pada Gambar 1.



Gambar 1 Skema arsitektur IEEE 802.1X

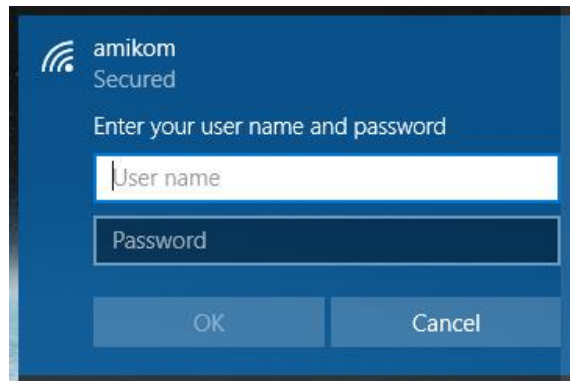
Supplicant merupakan perangkat yang digunakan oleh pengguna, bisa berupa laptop, handphone, PDA dan juga gadget lainnya akan menyambungkan diri ke perangkat authenticator berupa access point. Dari koneksi antara supplicant dan authenticator tersebut maka di sisi supplicant akan muncul menu yang meminta memasukkan data berupa data user dan password untuk koneksi ke jaringan, kemudian authenticator akan meneruskan data dari user itu ke authentication server yang berupa RADIUS server. Reply dari radius server yang akan menentukan apakah pengguna itu bisa terkoneksi dengan network dan tergabung di vlan apa user tersebut. Proses autentikasi ditunjukkan pada Gambar 2.



Gambar 2 Proses autentikasi

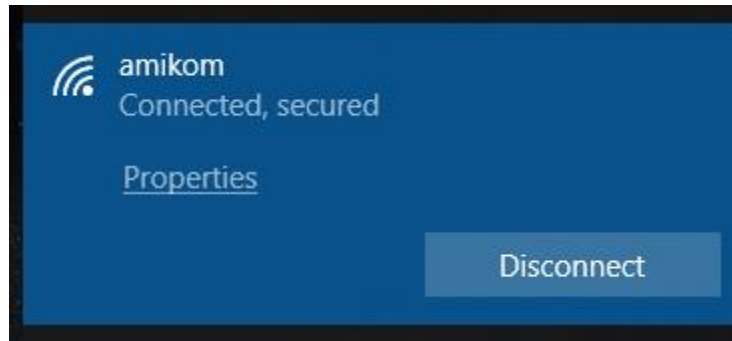
### 3. HASIL DAN PEMBAHASAN

Pengguna melakukan pengaturan pada device yang digunakan untuk terkoneksi ke jaringan wireless dengan SSID amikom, setelah terhubung dengan access point yang memancarkan sinyal dengan SSID amikom maka pada device yang digunakan akan muncul menu untuk login untuk memasukkan user dan password milik pengguna. Menu login di sistem operasi Microsoft Windows 10 bisa dilihat pada Gambar 3.



Gambar 3 Menu login

Masukkan dari user kemudian akan di kirimkan ke server RADIUS untuk pengecekan kecocokan data nama user dan password, jika nama user dan password sesuai dengan data yang ada di database di server RADIUS maka server radius akan mengirimkan data kembalikan ke authenticator bahwa user tersebut merupakan user yang valid beserta data vlan yang akan di assign ke koneksi user tersebut. Setelah berhasil login maka status dari koneksi wireless di komputer / laptop pengguna akan berubah menjadi seperti yang ditunjukkan oleh Gambar 4.

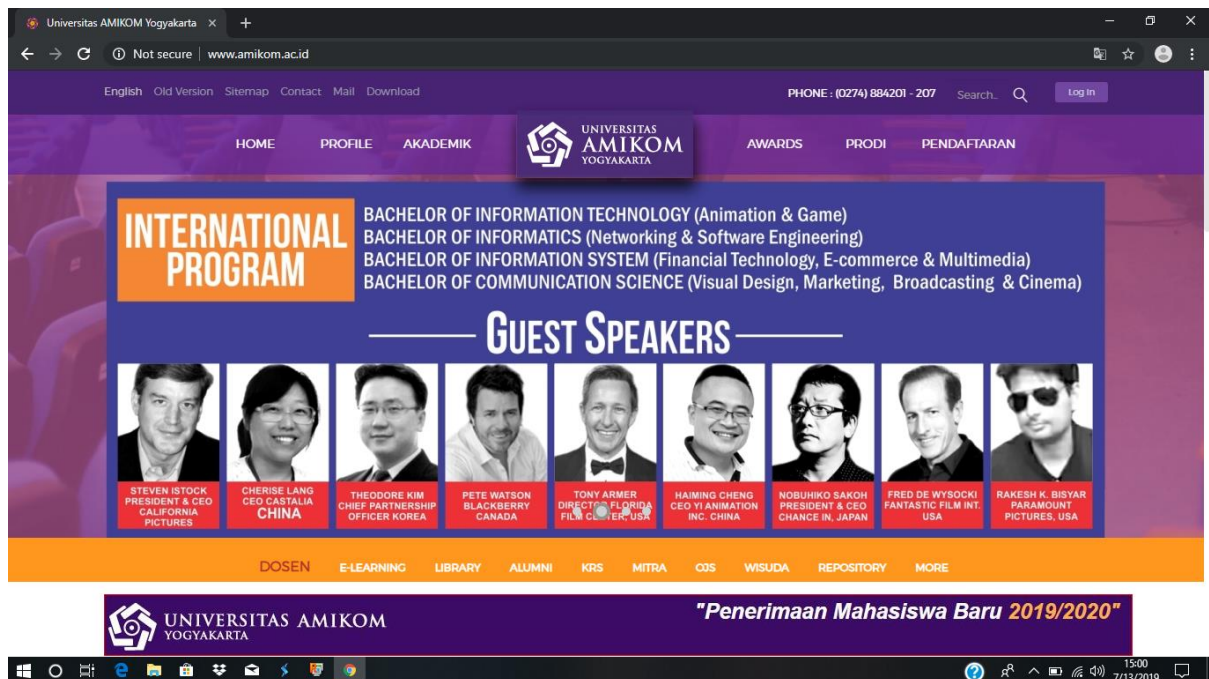


Gambar 4 Status koneksi wireless

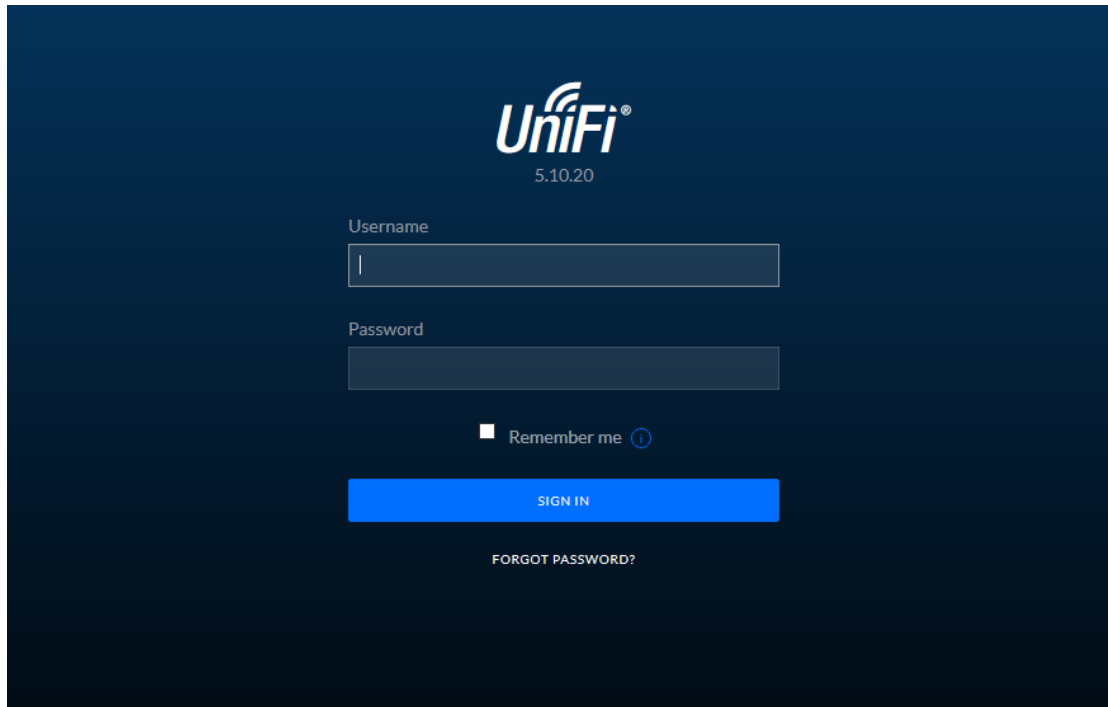
Komputer milik pengguna yang sudah berhasil melakukan login tersebut kemudian dicoba digunakan untuk mengakses halaman situs web <http://www.amikom.ac.id>, seperti ditunjukkan pada Gambar 5.

Hasilnya menunjukkan bahwa konfigurasi yang dilakukan sudah berhasil dengan munculnya halaman web yang dituju di browser yang digunakan.

Untuk manajemen access point secara terpusat (centralized), penulis menggunakan aplikasi yang disediakan oleh vendor yang sama dengan vendor yang digunakan untuk access point yaitu unifi controller dengan access point dengan merk dagang ubiquity. Tampilan dari aplikasi unifi ditunjukkan oleh Gambar 6.

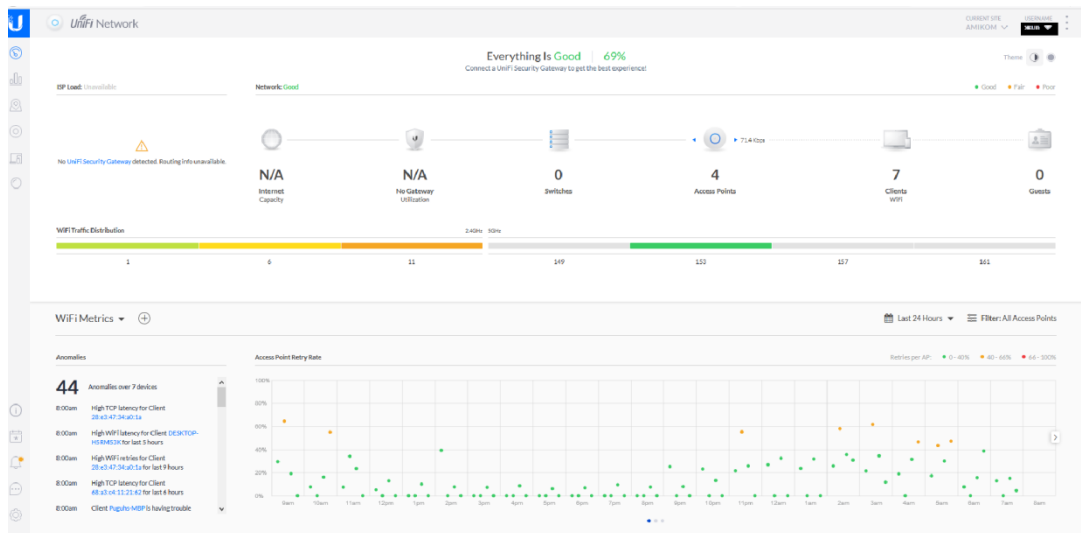


Gambar 5 Halaman situs web AMIKOM



Gambar 6 Tampilan aplikasi unifi

Untuk melakukan konfigurasi access point menggunakan kontroler unifi ini, langkah pertama yang harus dilakukan adalah login ke dalam aplikasi menggunakan user dan password yang dibuat ketika proses instalasi aplikasinya. Tampilan setelah berhasil melakukan login ditunjukkan oleh Gambar 7.



Gambar 7 Tampilan setelah berhasil melakukan login

Dengan menggunakan aplikasi kontroler ini, penulis dapat melakukan konfigurasi pada access point tanpa harus mendatangi langsung ke setiap access point yang terpasang dan juga aplikasi ini digunakan untuk mengarahkan setiap data user ke server RADIUS di alamat ip tertentu.

Data username dan password serta bagian / departemen di amikom disimpan di server radius yang menggunakan aplikasi freeradius yang dijalankan di sistem operasi berbasis ubuntu server dengan menggunakan database mysql. Dengan menggunakan freeradius dan mysql ini sangat memudahkan penulis untuk melakukan manajemen user seperti menambah dan mengurangi user, mengganti password user hanya di satu titik, dan itu akan langsung berlaku di semua daerah yang terjangkau sinyal dari access point yang terpasang di amikom.

#### 4. KESIMPULAN

Sesuai dengan latar belakang dan tujuan penelitian peningkatan keamanan wireless pada jaringan komputer di Universitas Amikom Yogyakarta dengan menggunakan protokol IEEE 802.1X maka di dapat kesimpulan yaitu penelitian ini berhasil meningkatkan keamanan wireless di jaringan komputer di Amikom, dengan menggunakan protokol IEEE 802.1X ini pengguna hanya bisa melakukan komunikasi data setelah berhasil login ke dalam sistem dimana jika menggunakan sistem yang lama, pengguna bisa melakukan berbagai aktifitas di jaringan walaupun belum berhasil login. Penulis berhasil melakukan manajemen perangkat hanya dari 1 kontroler untuk mengatur semua access point yang ada. Penulis berhasil melakukan manajemen user dan password pengguna hanya dari 1 server radius.

#### 5. SARAN

Bagian ini adalah opsional. Apabila ada maka saran-saran berisi saran penelitian lebih lanjut untuk menutup kekurangan penelitian saat ini atau pengembangan dari penelitian yang sudah dilakukan.

#### DAFTAR PUSTAKA

- [1] H. Mukhtar, "Teknik Open Source," Sleman: DEEPUBLISH, 2019.
- [2] A. Genco and S.Sorce, "Pervasive Systems and Ubiquitous Computing," Southampton: WIT Press, 2010.
- [3] D. Gibson, "MCITP Guide to Microsoft Windows Server 2008 Enterprise Administration," Boston: Cengage Learning, 2011.