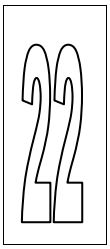
YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 4 Nomor 1 Edisi Februari 2019 (18-26)



IMPLEMENTASI HOTSPOT LOGIN MENGGUNAKAN CAPSMAN MIKROTIK PADA WILAYAH YANG BERBEDA

Tommy Alfian Armawan Sandi , Eka Kusuma Pratama, Ilham Nur Leksono, Rian Septian Anwar
Dosen Universitas Bina Sarana Informatika
(Naskah diterima: 1 Januari 2019, disetujui: 30 Januari 2019)

Abstract

The development of wireless technology is currently so fast, every communication device such as smartphones, tablets, and portable computers supports the wireless technology. It's no stranger when somewhere provides wireless networks especially if the wireless network is connected to the internet network. If the wireless network has been formed then the next problem is how the network can cover all areas or places that exist, then what about the security system, whether the wireless network is already safe than the stylists. Then, whether the administrator can look at controlling the activities of users, and what if there are two or more places with different areas but want to make the administrator centrally. By using CAPsMAN which is synergized with Userman and Radius Server using the Extended Service Set topology and connecting between regions via VPN, this wireless network will be controlled, monitored and configured centrally, bringing Authentication, Authorized and Accounting features in userman to make the network usable using an account By itself, using a VPN for interconnection ensures that account usage can be done using the same account, and applying an extended service set topology can produce a stable network without interrupted interruptions.

Keywords: *CAPsMAN, User Manager, Radius Server, Extended Service Set, VPN*.

Abstrak

Perkembangan teknologi wireless saat ini begitu pesat, disetiap alat komunikasi seperti smartphone, tablet, maupun komputer jinjing mendukung teknologi wireless tersebut. Sudah tidak asing ketika di suatu tempat menyediakan jaringan wireless apalagi jika jaringan wireless tersebut terhubung dengan jaringan internet. Kalau jaringan wireless sudah terbentuk maka persoalan berikutnya adalah bagaimana jaringan tersebut dapat mencakup seluruh area atau tempat yang ada, lalu bagaimana dengan sistem keamanannya, apakah jaringan wireless tersebut sudah aman daripada perentas-perentas. Kemudian, apakah administrator dapat melihat mengontrol aktifitas dari pengguna-pengguna, dan bagaimana jika terdapat dua atau lebih tempat dengan wilayah yang berbeda namun ingin membuat administrator secara terpusat. Dengan menggunakan CAPsMAN yang disingergikan dengan Userman dan Radius Server yang

menggunakan topologi Extended Service Set dan menghubungkan antar wilayah melalui VPN menjadikan jaringan wireless tersebut akan dikendalikan dipantau dan dikonfigurasi secara terpusat, menghadirkan fitur Otentikasi, Otorisasi dan Akuntansi dalam userman menjadikan jaringan tersebut bisa digunakan menggunakan akun tersendiri, dengan menggunakan VPN untuk interkoneksi menjamin penggunaan akun dapat dilakukan menggunakan akun yang sama, dan menerapkan topologi extended service set dapat menghasilkan jaringan yang stabil tanpa adanya gangguan terputus.

Kata Kunci : CAPsMAN, Manager Pengguna, Server Radius, Kumpulan Layanan yang Diperluas, VPN.

I. PENDAHULUAN

CAPsMAN adalah fitur yang dikembangkan oleh Mikrotik yang bertujuan untuk memanajemen jaringan wireless secara terpusat. Karakteristik CAPsMAN terletak pada penggunaan banyak access point dalam suatu tempat atau wilayah, konfigurasi CAPsMAN dilakukan pada router yang akan digunakan sebagai pusat kendali semua (Towidjojo & Farhan, 2015). Kelemahan keamanan dari topologi ini adalah tidak adanya fitur *Authentication, Authorization* dan *Accounting* (AAA) dengan fitur ini bisa mengatur siapa saja yang dapat terkoneksi dengan jaringan tersebut, berapa lama pengguna terhubung, berapa jumlah kuota yang diberikan baik upload maupun download dan kapan saja pengguna bisa terkoneksi dengan jaringan tersebut. (Towidjojo & Farhan, 2015) fitur ini terdapat pada Userman Mikrotik dengan Radius server. Bila tidak ada fitur ini bisa saja *Access Point* asing terhubung untuk memperluas cakupan area *wireless* yang sudah dibuat ISP yang digunakan menggunakan ip public dynamic. Untuk membuat CAPsMAN di dua tempat yang berbeda, antar jaringan mereka harus terhubung. Maka, dibuatlah jalur khusus access point tersebut. Penelitian dilakukan pada CV. Prima Brata yang ingin membuat jaringan wireless terpusat antara kantor pusat dan kantor cabang. Pada setiap kantor CV. Prima Brata memiliki ISP dan topologi WLAN yang berbeda. Beberapa access point yang digunakan menerapkan topologi basic service set yaitu Jaringan *wireless* yang menggunakan 1 (satu) *Access Point* untuk melayani sejumlah *client* dengan VPN untuk menghubungkan kedua kantor tersebut.

II. METODE PENELITIAN

Dalam memperoleh data Penulis melakukan riset secara langsung dalam prosedur yang sistematik dan standar sehingga menda-

patkan data-data yang baik dan benar dengan model pengumpulan data sebagai berikut:

Penulis menggunakan metode ini sebagai sarana pengambilan data-data terkait jaringan yang ada, dimana metode ini merupakan hasil peninjauan langsung dari objek yang diamati, yaitu. CV. Prima Brata. Observasi dilakukan selama 3 hari, untuk melihat bagaimana jaringan itu bekerja dari ISP sampai setiap pengguna yang terdapat di kantor tersebut.

Metode penelitian ini penulis lakukan dengan menanyakan secara langsung baik kepada pembimbing ataupun staf yang sedang bertugas guna mendapatkan informasi dan data serta menambah wawasan keilmuan terkait hal yang belum diketahui.

Analisa penelitian ini dilakukan sebagai salah satu alat proses untuk pengambilan keputusan, analisa penelitian ini berguna untuk mengurangi ketidak pastian dengan menyediakan informasi yang akurat untuk memperbaiki proses pembuatan keputusan itu. Metode penelitian yang penulis gunakan antara lain :

Tahap analisa kebutuhan dalam hal ini, CV. Prima Brata ingin membangun jaringan wireless yang dapat dipantau dan dikendalikan secara terpusat sehingga layanan yang diberikan kepada pengguna menjadi maksimal, maka untuk simulasi dibutuhkan 2 buah router yaitu RB951Ui-2ND dan 2 buah Access Point RBmAPL-2nD.

b. Desain

Desain yang akan digunakan pada impelentasi capsman diambil pada buku “Implementasi Wireless LAN Indoor” dimana konfigurasi standar berada di kantor pusat dan kantor cabang hanya meminta layanan dari kantor pusat.

Pengujian dilakukan dengan membuat simulasi apakah kantor cabang dengan kantor pusat sudah terhubung dengan CAPsMAN dan usermanager, dan access point kantor cabang sudah bisa dipantau aktivitas penggunanya..

Implementasi ini menjalankan semua rules yang telah di buat dan menilai apakah hasilnya lebih baik dan bisa mengurangi kesalahan terhadap manajemen wireless yang telah dilakukan

Dalam proses penelitian dibutuhkan suatu sumber yang relevan guna mendukung setiap gagasan. Berikut penulis cantumkan tiga jurnal ilmiah yang relevan dengan penelitian yang penulis bahas.

1. Manajemen Wireless Access Point Pada Hotspot Server Menggunakan Contoller Access Point System Management.

Pada penelitian yang dilakukan oleh Ba-khtiar Rifai dan Aji Sudibyo tahun 2018 (Rifai & Sudibyo, 2018), menyimpulkan bahwa : Untuk penerapan dan imple-mentasi Controller Access Point System Management (CAPsMAN) dibutuhkan parameter-parameter konfigurasi terle-bih dahulu pada sisi router yang akan di gunakan sebagai Controller access point system management (CAPsMAN) harus memiliki kemampuan wireless control-ler dan dari sisi access point yang akan digunakan untuk mendistribusikan wire-less yang bisa disebut dengan Controller Access Point (CAP).Penerapan Contro-ller access point system management (CAPsMAN) ialah dengan membuat konfigurasi Bridge interface, configura-tions, Channels, Data paths, Security Configurations pada system manag-ement Controller Access Point (CAP). (Rifai & Sudibyo, 2018).

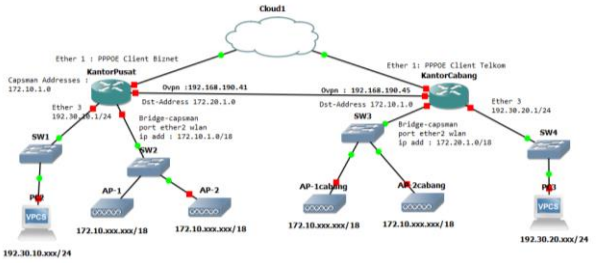
2. Implementasi Controller Access Point System Manager (CAPSMAN) Dan Wireless Distribution System (WDS) Jaringan Wireless Di SMK Terpadu Al Ishlahiyah Singosari Malang.

Pada penelitian yang dilakukan oleh Santi Dwi Ratnasari, Eni Farida, Nasrul Firdaus tahun 2017 menyimpulkan bah-wa : Banyaknya SSID yang tersedia akan mengganggu kinerja user, dikare-nakan saat berpindah tempat harus login kembali. Selain itu, kemananan jaringan di SMK Al Ishlahiyah sangatlah kurang sehingga dengan mudah dapat diterobos oleh user yang mengakses jaringan secara ilegal. Dengan menggunakan sist-em keamanan jaringan WPA2-PSK, dapat membantu mengatasi masalah keamanan jaringan wireless pada SMK Al Islahiyah agar tidak mudah diterobos oleh user yang tidak bertanggung jawab. Selanjutnya untuk menangani banyak-nya SSID yang tersedia diterapkan fitur CAPsMAN dan WDS, dapat memper-mudah user yang mendapatkan ijin akses secara legal tidak sering login kembali jika berpindah tempat. Selain itu dilakukan bandwidth management dengan menggunakan metode Queue Tree dan Per Connection Queue (PCQ) yang disertai penambahan mangle, agar bandwidth yang tersedia tidak terbuang begitu saja. (Ratnasari, Farida, & Fir-daus, 2017).

3. Analisa Perbandingan Kinerja Fitur Mikrotik Capsman Dengan Konfigurasi Tunnel Dan Tanpa Menggunakan Tun-nel Pada Router Mikrotik Rb951-2n.

Dalam Analisa perbandingan kinerja fitur mikrotik Capsman dengan konfi-gurasi tunnel dan tanpa menggunakan tunnel, terhadap

kecepatan download data dan rata-rata bandwidth yang dibutuhkan disaat mendownload. Pengu-jian dilakukan dengan menggunakan dua sampel data yang berformat ISO dan RAR dengan ukutan data 100MB sampai 900MB. Pengujian kecepatan download data iso tanpa tunnel didapat-kan hasil dengan file ISO dengan ukuran 100MB dibutuhkan waktu 4 (empat) menit atau 240 (dua ratus empat puluh) detik untuk mendownload sedangkan pengujian dengan menggunakan tunnel didapatkan hasil 280 (dua ratus delapan puluh) detik untuk mendownload. Selan-jutnya, pengujian kecepatan download data RAR tanpa menggunakan tunnel dengan ukuran file 100MB didapatkan hasil 243 (dua ratus empat puluh tiga) detik waktu yang dibutuhkan untuk mendownload, sedangkan pengujian kecepatan download data RAR dengan tunnel dibutuhkan waktu 298 (dua ratus Sembilan puluh delapan) detik. Penguj-ian rata-rata bandwidth tanpa tunnel file ISO dengan ukuran 100MB dibutuhkan waktu 240 (dua ratus empat puluh) detik dengan rata - rata bandwidth 426.67 Kbps. Sedangkan, pengujian rata-rata bandwidth dengan tunnel file ISO dengan ukuran 100MB dibutuhkan wak-tu 280 (dua ratus delapan puluh) detik dengan rata-rata bandwidth 365.72 Kbps. Selanjutnya, pengujian rata-rata bandwidth dengan data RAR tanpa menggunakan tunnel dengan ukuran file 100MB dibutuhkan waktu 243 (dua ratus empat puluh tiga) detik dengan rata-rata bandwidth 421.40 Kbps. Sedangkan, pengujian rata-rata band-width dengan data RAR menggunakan tunnel lama waktu download yang dibutuhkan 298 (dua ratus sembilan puluh delapan) detik dengan rata-

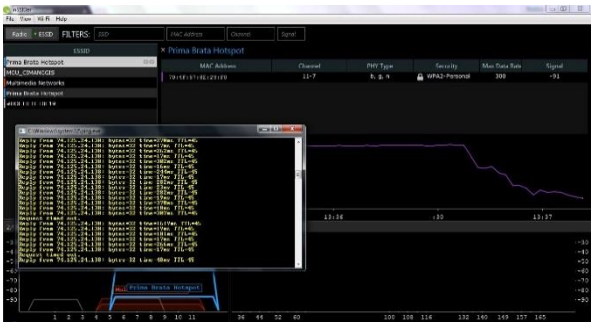


rata bandwidth 343.63 Kbps. Berdasarkan penelitian yang telah dilakukan terhadap Perbandingan Kinerja Fitur Mikrotik CAPsMAN dengan Konfigurasi Tunnel dan Tanpa Menggunakan Tunnel Pada Router Mikrotik, maka dapat disimpul-kan bahwa paket data yang dilewatkan pada jaringan wireless tanpa mengguna-kan tunnel lebih cepat dari pada meng-gunakan tunnel, karena paket data yang dilewatkan pada jalur ini tidak terjadi pemerikasaan dan penambahan paket data header terhadap data yang dikirim. Sementara pada saat melakukan pengiri-man paket pada jalur tunnel terjadi pemeriksaan

dan penambahan paket data header disetiap protokol yang dilewa-tinya. Dalam melakukan pengujian download data di ambil dua jenis sampel data, yaitu data ISO dan RAR dengan rata-rata selisih waktu 3 menit 6 detik dengan rata-rata bandwidth 61,66 Kb-ps.(Warman & Nofrizal, 2016)

III. HASIL DAN PEMBAHASAN

VPN dibuat untuk menghubungkan kan-



tor pusat dan cabang dan ditambah dengan konfigurasi static route pada setiap router. Pastikan antar kedua router sudah terhubung.

Sumber : Hasil Penelitian, 2018

Gambar 1. Topologi Jaringan

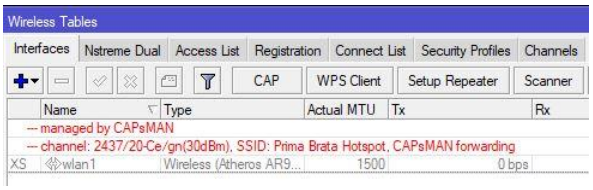
Router Pusat : Interface ether 2 dan wlan di-buat *bridge* dengan ip 170.10.1.0/18 dan di konfigurasi DHCP, selanjutnya konfigurasi pada router CAPsMAN, konfigurasi CAPs-MAN seperti konfigurasi *channel*, konfigurasi profil dan konfigurasi *provisioning*.

Untuk konfigurasi channel terdapat pada tab Channel → Add, Channel yang akan digunakan adalah Channel 6 yang berada di frekuensi 2437 dengan Width 20Mhz dan Ban 2Ghz-b/g/n. Selanjutnya konfigurasi profil, berfungsi sebagai parameter wireless yang nantinya akan digunakan oleh Access Point. Configuration → Add, maka muncul jendela CAPs Configuration, yang diubah hanya mode =ap dan SSID =”Prima Brata Hotspot”, masih pada CAPs Configuration, pada tab Channel, pilih Channel 6 yang sudah dibuat sebelum-nya.

Pada tab Datapath. Bridge yang diguna-kan adalah Brigdecapsman yang artinya menujukkan bahwa traffic dari client wireless akan mengalir pada interface bridge-capsman. Langkah terakhir dalam konfigurasi CAPsMAN adalah Provisioning yang bertuju-an untuk mendaftarkan MAC Address setiap Access Point supaya dapat menjalankan fungsi CAPsMAN yang sudah dibuat.

Konfigurasi selanjutnya terletak pada Access Point yang menjadi CAP, untuk router CAPsMAN yang terdapat interface wireless, tidak perlu konfigurasi dhcp-client, tetapi hanya perlu mengaktifkan mode CAP pada Wireless dan memasukan IP CAPsMAN, namun, jika memakai interface ether 2 maka harus menggunakan dhcp-client untuk inter-face wireless pada Access Point. Sampai disini

konfigurasi pusat dan cabang sudah terkoneksi dengan baik.



Sumber : Hasil Penelitian, 2018

Gambar 2. Interface wlan pusat

Sumber : HasilPenelitian, 2018

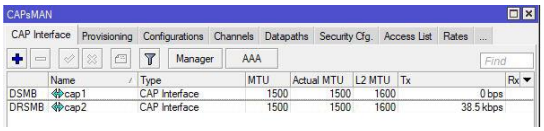
Gambar 3. Interface wlan cabang

Konfigurasi *Hotspot server* dengan *Radius Server* yang terhubung dengan *User manager* pada Mikrotik. Pada AP-1 dan AP-2 di konfigurasikan Dhcp-Client dan mengaktifkan CAP dengan CAPsMAN *Address* 172.10.1.0.

Pada *router gateway* (Cabang) *interface* yang digunakan hampir sama dengan *router gateway* (Pusat). *interface bridge* terdiri dari ether 2 dan wlan1 yang terhubung pada *switch* dan *Access Point*. Tidak ada konfigurasi tentang CAPsMAN pada *router gateway* (Cabang) hanya penambahan radius untuk menghubungkan *router* pada *User Manager router gateway* (Pusat). Konfigurasi CAP dilakukan oleh *Access Point* dengan memasukan IP CAPsMAN atau IP bridge-capsman pada *router gateway* (Pusat). Secara otomatis *Access Point* Cabang akan mengikuti konfigurasi CAPsMAN yang ada di *router gateway* (Pusat).

Pengujian Jaringan Awal

Pengujian dilakukan dengan menggunakan aplikasi inSSIDer4, menganalisa jaringan wireless dengan metode Scanning.



Gambar 4. Scanning Wireless

Terdapat 2 SSID yang teridentifikasi, untuk membedakan antara *root access point* dan *repeater access point* dengan melihat simbol yang diberikan pada SSID, jika ada simbol kunci/lock berarti SSID tersebut adalah *repeater* dari *root access point. Channel* yang digunakan memakai *channel* 7 – 11 yang berjalan pada frekuensi 2,442 Ghz sampai 2,462 Ghz. menggunakan sistem keamanan WPA2-Personal, *Signal strange range* -29 artinya *client wireless* sebagai objek pengujian berada dekat dengan access point

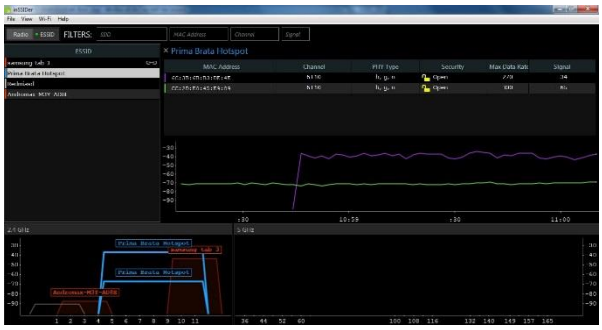
Selama perpindahan berlangsung *signal wire-less* akan menjadi lemah seiring dengan berge-raknya objek menjauhi access point dan

ping akan menjadi tinggi atau terputus-putus, kare-na objek yang berada diluar jangkauan access point sebelumnya dan dibuktikan dari nilai signal -91.

Pengujian Jaringan Akhir

Langkah pengujian akhir dengan melibatkan *router* kantor pusat maupun *router* kantor cabang yang terhubung melalui internet dengan jalur VPN dan menggunakan *hotspot login* untuk *client* pada masing-masing kantor. *Router* pusat yang sudah di konfigurasikan sebagai CAPsMAN akan memberikan layanan kepada *router* cabang, saat *router* cabang sudah meminta layanan dari CAPsMAN, maka status *CAP interface* CAPsMAN pada *router* pusat akan seperti gambar berikut :

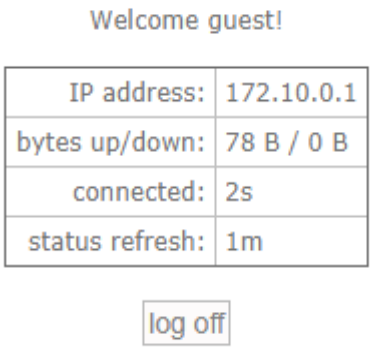
Gambar 6. Status interface CAPsMAN pada router pusat



Gambar 7. Pengujian Extended Service Set (ESS)

Dapat disimpulkan hanya terdapat 1 SSID pada jaringan *wireless* yang ada namun, tidak mengurangi kualitas signal yang diberi-kan. Pada konsep ESS setiap *access point* bekerjasama untuk membuat *roaming* sehing-ga *client* akan terus terhubung walaupun berbeda access point, selain itu penggunaan *hotspot login* pada CAPsMAN menjadikan manajemen *user* manjadi lebih efisien.

Pengujian selanjutnya adalah mengim-plementasian *user* yang sudah dibuat pada *user manager*, pengujian pertama dilakukan pada kantor cabang dengan user “guest”.



Gambar 8. tampilan sesudah *login* dengan *user guest*

V. KESIMPULAN

Penerapan CAPsMAN dengan topologi *extended service set* dalam jaringan *wireless*

pada suatu lokasi atau tempat telah menjawab permasalahan dimana admistrator sulit untuk mengatur beberapa *access point* atau menghubungkan *access point* yang ada pada satu jaringan wireless yang sama, oleh karena itu dapat disimpulkan bahwa, dengan konsep CAPsMAN yang memanajemen secara terpusat memberi efisiensi waktu konfigurasi yang selama ini harus dilakukan pada setiap perangkat *access point*, hanya dengan mengubah mode pada *access point* menjadi CAP dan memanggil IP *router* CAPsMAN secara otomatis *access point* akan terkonfigurasi. Dalam memanajemen user dengan fitur usermanager pada mikrotik yang disinergikan oleh CAPsMAN dapat membantu administrator untuk memberikan, memantau dan mengatur *username* maupun *password* secara terpusat. Sehingga *client wireless* dapat menggunakan *user* dan *password* yang sama pada jaringan *wireless* yang menggunakan CAPsMAN. Adapun penggunaan topologi *extended service set* pada jaringan wireless membuat antar *access point* saling berkoordinasi untuk melayani *client wireless* sehingga meminimalisir *client wireless* terputus dengan koneksi wireless yang ada. Penggunaan Radius Server pada *router* cabang menggunakan ip bridge capsman yang berada di *router* cabang, sehingga autentifikasi dapat dijangkau oleh usermanager yang berada pada *router* pusat.

DAFTAR PUSTAKA

Towidjojo, Rendra dan Mohammad Eno Farhan. 2015. Router Mikrotik : Implementasi Wireless LAN Indoor, Jakarta: Jasakom.

Rifai, B., & Sudibyo, A. 2018. *Manajemen Wireless Access Point Pada Hotspot Server Menggunakan Controller Access Point System Management*, *14*(1), 111–116.

Ratnasari, S. D., Farida, E., & Firdaus, N. 2017. *Implementasi Controller Access Point System Manager (Capsman) Dan Wireless Distribution System (Wds) Jaringan Wireless Di Smk Terpadu Al Ishlahiyah Singosari Malang*, (September), 624–635.

Warman, I., & Nofrizal. 2016. *Analisa Perbandingan Kinerja Fitur Mikrotik Capsman Dengan Konfigurasi Tunnel dan Tanpa Menggunakan Tunnel pada Router Mikrotik RB951-2N*. *Vol. 4 No. 2 Oktober 2016*, *4*(2), 96–105

Pengenalan User manager | Mikrotik Indonesia. (n.d). Retrieved May 8. 2018. from Mikrotik.co.id. http://www.mikrotik.co.id/artikel_lihat.php?id=46