MANAJEMEN WIRELESS ACCESS POINT PADA HOTSPOT SERVER MENGGUNAKAN CONTROLLER ACCESS POINT SYSTEM MANAGEMENT

Bakhtiar Rifai[1]; Aji Sudibyo[2]

Teknik Informatika
STMIK Nusa Mandiri Jakarta
www.nusamandiri.ac.id
bakhtiar.bri@nusamandiri.ac.id[1], ngabloe.aji@gmail.com[2]

Abstract— *Wireless is a good medium for internet access and has a limited reach so that all methods are required to distribute wireless with both broad and wide and signal coverage, able to manage with good access point and needed good security for access to wireless available problems happens is the more wireless and access point and the number of connected users that are not managed properly and optimally it will result in the performance of the access point will be less than optimal and effective. Controller Access Point System Management (CAPsMAN) is a good method of managing access points to make it easy and manageable and effective and hotspot server is needed to manage multiple users connected to the access point and can handle hundreds of users simultaneously.*

Keywords: Controller Access Point, Hotspot Server.

Intisari— Wireless merupakan media yang baik untuk akses internet dan mempunyai jangkuan yang terbatas sehingga diperlukan semua metode untuk dapat mendistibusikan wireless dengan baik merata dan luas serta jangkauan signal, mampu mengelola dengan baik access point serta dibutuhkan keamanan yang baik untuk akses ke dalam wireless yang tersedia permasalahan yang terjadi ialah semakin banyak wireless dan access point serta banyaknya user yang terkoneksi yang tidak dikelola dengan baik dan secara optimal maka akan mengakibatkan kinerja dari access point tersebut akan kurang optimal dan efektif. Controller Access Point System Management (CAPsMAN) merupakan metode yang baik dalam memanajemen access point agar mudah dan dapat di kelol adengan baik dan effesien dan hotspot server diperlukan untuk mengelola banyak user yang terhubung kedalam access point serta dapat menangani ratusan user dalam bersamaan.

Kata Kunci*: Controller Acces Point, Hotspot Server.*

PENDAHULUAN

Teknologi nirkabel atau wireless berkembang dengan pesat dan seiring dengan penggunaan perangkat berbasis teknologi baik laptop, tablet PC dan gadget tidak lepas dari perangkat wireless di era teknologi informasi ini, dengan mengunakan wireless mempermudah dan meringkas transfer data dan akses internet.

Untuk menerapkan jaringan wireless dengan lingkupan luas di perlukan banyak perangkat *Access Point,* ketika banyaknya *Access Point* yang dikonfigurasi oleh administrator, baik dari sisi *service set identifier* (SSID) frekuensi dan channel yang harus dimaintenance terus menerus (Towidjojo & Farhan, 2015) permasalahan akan timbul jika tidak adanya sebuah manajemen wireless dan access point yang baik ketika dibuat seperti kesalahan pembuatan *service set identifier* (SSID) sehingga fitur roaming pada *Access Point* tidak dapat bekerja dan banyaknya *access point* dan *service set identifier* (SSID) dalam suatu tempat serta tanpa manajemen yang baik dalam mengelolanya sehingga akan menimbulkan permasalahan dalam memonitoring jaringan internet yang disebarkan oleh access point tersebut (Ratnasari, Farida, & Firdaus, 2017).. Karena paket data yang dikirmkan oleh wireless dibagi tiga macam yaitu *management*, *control* dan data (S'to, 2014). Pengelolaan *user* yang ingin mengakses internet bukan pekerjaan mudah (Putra, 2013), karena sulit untuk mengkontrol *user* dengan jumlah yang banyak dan memiliki karakteristik yang berbeda-beda (Kurniawan, 2016) terlebih *user* meggunakan media jaringan wireless berubah-ubah tempat dalam mengaksesnya. Terlebih perangkat wireless yang banyak dan security key wireless yang hanya menggunakan *wireless protected access* (WPA) masih menghasilkan setumpuk masalah. (Towidjojo, 2017)

Untuk dapat mengendalikan masalah yang terjadi dari penggunaan wireless untuk user dan persediaan perangkat *Access Point* untuk user diperlukan pengelolaaan yang baik untuk masalah tersebut ialah dengan menggunakan Hotspot Server dan penerapan *Controller Access Point System Management* (CAPsMAN) untuk meningkatkan efesiensi dan pengelolaan yang lebih baik pada jaringan wireless.

Hotspot server merupakan konsep akses internet dengan menggunakan *authentication* pada halaman web untuk sisi keamanan, setiap user akan diberikan akses sesuai dengan aturan yang berlaku berupa *username* dan *password* sehingga setiap user hanya bisa menggunakan *username* sesuai ketentuan dan jika username dan password yang digunakan tidak sesuai atau valid makan user tersebut tidak dapat menggunakan akes internet yang diberikan

Controller Access Point System Management (CAPsMAN) merupakan sebuah fitur yang digunakan untuk mengontrol jaringan access point secara terpusat (Warman & Nofrizal, 2016). Penggunaan wireless LAN memiliki fleksibelitas, mendukung mobilitas, memiliki teknik *frequency reuse, selular* dan *handover*, menawarkan efisiensi dalam waktu (penginstalan) dan biaya (pemeliharaan dan penginstalan ulang di tempat lain), mengurangi pemakaian kabel dan penambahan jumlah pengguna dapat dilakukan dengan mudah dan cepat. (Arianto, 2009).

BAHAN DAN METODE

Wireless yang dikenal dengan standard IEEE 802.11x, merupakan teknologi transmisi jarak pendek dengan standart 802.11a/b/g/n/ac, dengan data rate sebesar 300Mbps, *transmission distance* maksimum 300 Meter, bekerja pada *frequency* 2.4 Ghz dan 5 GHz, menggunakan *channel bandwidth* 20 – 25 MHz (Song & Issac, 2014).

Studi literatur dan jurnal terdahulu tentang wireless telah ada serta bervariasi dan pengembangan wireless management yang diterapkan dibeberapa situasi tertentu yang menjadi acuan sebagai referensi antara lain:

1. Analisa Perbandingan Kinerja Fitur Mikrotik Capsman Dengan Konfigurasi Tunnel Dan Tanpa Menggunakan Tunnel Pada Router Mikrotik Rb951-2n. Pada penelitian yang dilakukan oleh Indra Warman dan Nofrizal tahun 2016 (Warman & Nofrizal, 2016) melakukan pengujian terhadap kofigurasi tunnel dan tanpa menggunakan tunnel terhadap kecepatan download data dan rata-rata bandwidth yang dibutuhkan saaat mendownload dengan menggunakan sample pengujian 2 sempel berformat iso dan RAR dengan ukuran data 100 MB sampai 900 MB. Maka didapat hasil dari penelitian ini ialah konfigurasi *Controller Access Point System Management* (CAPsMAN) menggunakan tunnel dan tanpa menggunakan tunnel didapat tanpa tunnel lebih cepat dalam mentranfer data dibandingkan dengan menggunakan tunnel karena paket data yang lewat tidak diperiksa dan penambahan paket header terhadap paket data yang dikirmkan dengan hasil rata-rata selisih dari paket yang dikirmkan yaitu data ISO dan RAR 3 menit 6 detik dengan rata-rata bandwidth yang digunakaan 61,66 Kbps.
2. Implementasi Wireless Local Area Network dalam RT/RW Net (Arianto, 2009), melakukan penelitian impelementasi Wireless LocalArea Network pada RT/RW Net. Usaha RT/RW Net yang digunakan untuk Wireless Local Area Network cukup di kerjakan di rumah dengna mendirikan BTS (*Base Transceiver Station*) berupa tower sekitar 4 sampai 5 stak dengan jarak 1 stak sekitar 5 meter dan menggunakan antena Omni JB 10dB serta wireless access point unutk memancarkan signal wireless kerumah rumah sekitarnya sehingga warga sekitar bisa menggunakan dan memperoleh internet tersebut karena jaringan wireless LAN mempunyai keunggulan dari sisi mobilitas fleksibilitas, keamanan, skalabilitas yang baikdari pada jaringan menggunakan kabel.
3. Implementasi *Controller Access Point System Manager* (CAPsMAN) Dan *Wireless Distribution System* (WDS) Jaringan Wireless Di Smk Terpadu Al Ishlahiyah Singosari Malang (Ratnasari, Farida, & Firdaus, 2017) Penelitian tentang penerapan *Controller Access Point System Manager* (CAPsMAN) dan *Wireless Distribution System* (WDS) yang dilakukan Santi Dwi Ratnasari, Eni Farida, Nasrul Firdaus pada tahun 2017. Menjelaskan tentang penerapan *Controller Access Point System Manager* (CAPsMAN) dan WDS untuk mengurangi banyaknya SSID yang ada pada SMK Al Ishlahiyah sehingga banyak user di sekolah tersebut harus login terus ketika berpindah tempat dan tidak adanya keamanan yang digunakan pada sekolah tersebut minimal WPA2-PSK. Dengan penerapan *Controller Access Point System Management* (CAPsMAN) dan *Wireless Distribution System* (WDS) dapat membantu guru, staff, serta siswa di SMK Terpadu Al Ishlahiyah melaksanakan aktifitas perkantoran dan belajar mengajar tanpa memikirkan terputus jaringan internet serta tidak perlu login kembali saat berpindah tempat dari gedung satu ke gedung yang lainnya. Dengan terbangunnya sistem keamanan jaringan wireless menggunakan fitur WPA2-PSK di SMK Terpadu Al Ishlahiyah Singosari Malang, dapat meminimalisir terjadinya pembobolan jaringan wireless.

Controller Access Point System Management (CAPsMAN)

Koneksi *Controller Access Point* (CAP) ke *Controller Access Point System Management* (CAPsMAN) menggunakan 2 protokol transport yaitu melalui layer 2 dan layer 3 (Mikrotik.com, 2017). Pada koneksil lapisan 2 yaitu MAC address tidak perlu ada konfigurasi IP karena pada *Controller Access Point* (CAP) dan *Controller Access Point System Management* (CAPsMAN) berada pada segmen yang sama yaitu layer 2. sedangkan pada layer IP atau layer 3 *Controller Access Point* (CAP) perlu melintasi NAT untuk menuju capsman karena ip *Controller Access Point System Management* (CAPsMAN) berbasis multicast IP.

Untuk penerapan dan implementasi *Controller Access Point System Management* (CAPsMAN) dibutuhkan parameter-parameter konfigurasi terlebih dahulu pada sisi router yang akan di gunakan sebagai Controller access point system management (CAPsMAN) harus memiliki kemampuan wireless controller dan dari sisi access point yang akan digunakan untuk mendistribusikan wireless yang bisa disebut dengan *Controller Access Point* (CAP). Penerapan *Controller access point system management* (CAPsMAN) ialah dengan membuat konfigurasi Bridge interface, configurations, Channels, Data paths, Security Configurations pada system management *Controller Access Point* (CAP).

Hotspot Server

Untuk membangun Hotspot Server ada beberapa parameter dan service yang harus digunakan seperti DHCP Server berfungsi untuk memberikan ip address kepada user ketika terhubung ke Server Hotspot, NAT Firewall untuk melakukan masquerade. Web Proxy berfungsi menampilkan halaman login saat user melakukan *authenticaton* pada hotspot server, firewall filter digunakan untuk memblokir user yang tidak sesuai dengan authentication. Firewall mangle digunakan untuk melakukan marking packet yang masuk dan keluar pada user, simple queue digunakan untuk alokasi bandwidth yang aka diberikan pada user baik upload dan download.

Parameter awal sebelum menerapakan hotspot server meliputi konfigurasi IP address, default Rout DNS Server, Masquerade dan DHCP server. Setelah parameter dan konfigurasi tersebut terpenuhi baru melakukan konfigurasi Hotspot server yang akan digunakan yaitu interface yang digunakan, gateway yang dituju masquerade network harus ada agar dapat memberikan internet pada user setelah itu address pool pada hotspot server diperuntukan untuk alokasi atau range ip address yang akan diberikan keuser melalui DHCP server. Setelah parameter tersebut dilakukan konfigurasi DNS Server yang digunakan dan DNS name yang dipakai untuk domain Hotspot Server yang digunakan,

Jenis Penelitian

Penelitian ini menggunakan metode *experiment* yaitu penelitian yang menggabungkan konfigurasi dan implementasi antara Hotspot Server dengan implementasi *Controller Access Point System Management* (CAPsMAN) yang bertujuan untuk optimal dalam penerapan dan security yang diterapkan pada *wireless access point* dan mempermudah dalam proses maintenance dan troubleshooting wireless. Metode yang digunakan untuk mendapatkan data sebagai objek penulisan adalah sebagai berikut:

1. Analisa Kebutuhan
   Untuk bisa membuat simulasi perancangan system ini maka dibutuhkan 4buah wireless access point yaitu 951ui-2HnD, 951-2n dan 2 buah 941 Hap Lite dengan *Controller Access Point System Management* (CAPsMAN) yang diterapkan pada RB2011Ls-IN.
2. Desain
   Untuk desain yang akan digunakan pada simulasi capsman dan hotspot server menggunakan perangkat real yang telah di konfigurasi sedemikian rupa agar dapat menangani.
3. Testing
   Pada tahap ini melakukan perbandingan terhadap implementasi yang telah dibuat dan membuat report tentang hasil penelitian ini.
4. Implementasi
   Implementasi ini menjalankan semua rules yang telah di buat dan menilai apakah hasilnya lebih baik atau bisa mengurangi kesalahan terhadap manajemen wireless yang telah dilakukan.

HASIL DAN PEMBAHASAN

Konfigurasi *Controller Access Point System Management* (CAPsMAN) yang digunakan ialah menggunakan mode= AP atau *Access Point* dengan nama *Service Set Indentification* (SSID)= BKTR-Cap pemilihan country Indonesia dengan menggunakan security authentication type= WPA-PSK dan WPA2-PSK karena menggunakan Hotspot server dan auntefikasinya menggunakan hotspot Server, untuk metode ekripsi yang digunakan AES serta group encryption AES CCM dengan menggunakan password yang terdiri dari 8 karakter. Pada datapath menggunakan client-to-client-forwarding dan local-forwading dengan name bridge wifi-cap. Pada channel yang digunakan menggunakan channel dengan frequency 2412 Ghz channel width pada 20mhz serta band 2ghz-b/g/n.

Sumber: Rifai & Sudibyo (2018)

Gambar 1. Konfigurasi CAPsMAN

Pada tahapan ini konfigurasi channel dan frekunsi bandnya di perlukan Tahapan untuk membuat system management *Controller Access Point* (CAP) ialah membuat channel frequency untuk menentukan chanel berapa yang digunakan. Selanjutnya Bridge interface agar antar *Controller Access Point* (CAP) dan system management *Controller Access Point* (CAP) dapat berkomunikasi.

Selanjutnya di lakukan konfigurasi pada sisi *Controller Access Point* (CAP) yang akan di remote dengan melakukan konfigurasi pada parameter wireless cap. Maka akan didapat hasil

Konfigurasi *Controller Access Point* (CAP)

Pada tahapan selanjutnya sesudah seting *Controller Access Point System Management* (CAPsMAN) ialah melakukan konfigurasi di sisi *Controller Access Point* (CAP) meliputi setting bridge dengan protocol RSTP actual mtu=1500 l2mtu=1600 dengan port yang dibuatkan bridge pada interface pada ether1 dengan wlan1.Setelah melakukan konfigurasi cap diperlukan setting wireless dengan mode *Controller Access Point* (CAP) dengan enable=yes interfaces wlan1 certificate none discovery=ether1 dan *Controller Access Point System Management* (CAPsMAN) Addresses= 10.11.11.1 konfigurasi ini dilakukan pada setiap access point yang diperuntukan untuk *Controller Access Point* (CAP)

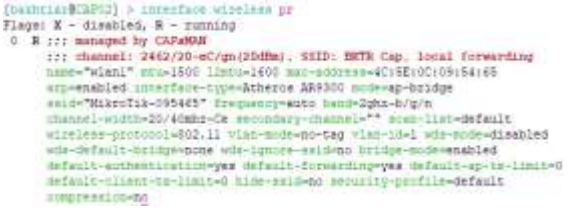
Controller Access Point (CAP) pada CAP01

Sumber: Rifai & Sudibyo (2018)

Gambar 2. Interface Wireless CAP01

Pada CAP01 dengan MAC Address: 4C:5E:0C:59:D7:CF yang didapat bahwa sudah termanaged oleh CAPsMan dengan channel: 11 frekuensi 2462 dengan SSID BKTR CAP

Controller Access Point (CAP) Pada CAP02



Sumber: Rifai & Sudibyo (2018)

Gambar 3. Interface Wireless CAP02

Sama hanya dengan CAP01 untuk CAP02 juga termanaged oleh CAPsMAN yang sudah di konfigurasikan dengan MAC Address: 4C:5E:0C:09:54:65 dengan channel 11 2462 Mhz dengan SSID BKTR Cap.

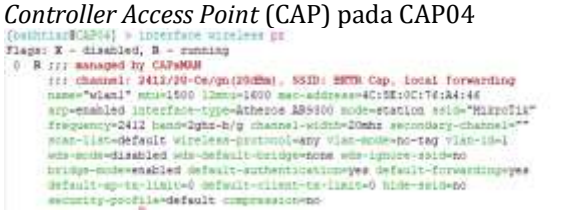
Controller Access Point (CAP) pada CAP03

Sumber: Rifai & Sudibyo (2018)

Gambar 4. Interface Wireless CAP03

Begitu juga dengan CAP03 dimanaged oleh CAPsMAN yang sudah di konfigurasikan dengan MAC Address: D4:CA:6D:B3:3A:69 dengan channel 11 2462Mhz dengan SSID BKTR Cap.

Controller Access Point (CAP) pada CAP04



Sumber: Rifai & Sudibyo (2018)

Gambar 5. Interface Wireless CAP04

Dan untuk *Controller Access Point* (CAP) yang terakhir yaitu CAP04 gambar diatas ialah hasil dari konfigurasi dan sinkronisasi dari *Controller access point system management* (CAPsMAN) yang sama hanya seperti CAP01, CAP02 dan CAP03 yang di managed dengan SSID BKTR Cap dengan MAC Address 4C:5E:0C:A4:46.

Maka akan didapat *Controller Access Point* (CAP) interface sebanyak 4 access point yang sudah terhubung dengan *Controller access point system management* (CAPsMAN) bisa dilihat dengan perintah caps-man remote-cap print detail.

Sumber: Rifai & Sudibyo (2018)

Gambar 6. CAPsMAN remote CAP

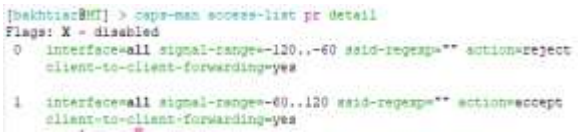
Gambar diatas menjelaskan status cap yang terhubung pada *Controller access point system management* (CAPsMAN) dan mengindetifikasinya cap serta serial CAP, IP address yang digunakan, MAC Address yang terhubung serta Serie dari Router Mikrotik yang digunakan

Sumber: Rifai & Sudibyo (2018)

Gambar 7. Radio CAPsMAN

Jika sudah menerapkan *Controller access point system management* (CAPsMAN) maka semua konfigurasi yang ada pada sisi accesspoint dapat langsung dilakukan pada controller *Controller access point system management* (CAPsMAN)

Selanjutnya membuat parameter akses yang bertujuan untuk menjaga kualitas layanan wireless pada client dan mengontrol koneksi pada setiap access point.



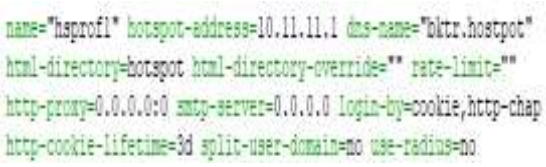
Sumber: Rifai & Sudibyo (2018)

Gambar 8. Access List CAPsMAN

Parameter access list yang dibuat ialah jika sinyal range yang didapat pada client antara -60 dB sampai 120 dB maka client tersebut diijinkan menggunakan access point tersebut tapi jika signal range yang didapat antara -120 dB sampai -60 dB maka client tidak dapat mengakses wireless yang tersedia sehingga client akan mencari access poin terdekatnya dan terbaik signalnya.

Konfigurasi Hotspot Server

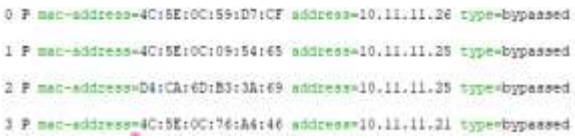
Untuk dapat Hotspot Server dapat bekerja baik makan di butuhkan beberapa parameter konfigurasi antara lain membuatkan nama hotspot yang digunakan, alamat IP address yang digunakan untuk Server Hotspot, DNS name untuk dapat dipanggil melalui browser. Selain itu perlu ada konfigurasi di sisi dhcp server dan lease time yang digunakan serta IP Pool yang digunakan.



Sumber: Rifai & Sudibyo (2018)

Gambar 9. Konfigurasi Hotspot

Karena pengujian ini menggunakan 4 access point maka agar dapat user yang akses menggunakan layanan hotspot dan capsman makan untuk device access point ini dibuatkan bypassed sehingga tidak membutuhkan auntetication di hotspot server bypass dilihat dari mac address dan ip address yang didapat dari 4 access point tersebut.



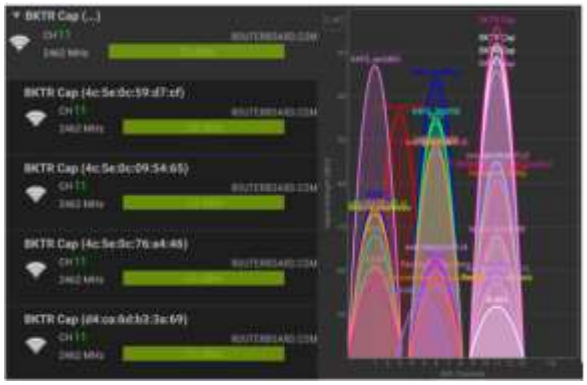
Sumber: Rifai & Sudibyo (2018)

Gambar 10. ByPass Access Point CAP

Fungsi dari bypass pada CAP yang terhubung dengan capsman ialah agar perangkat tersebut tidak memerlukan authentication agardapat terhubung dengan *Controller access point system management* (CAPsMAN), hotspot server dan internet. Sehingga yang memerlukan autenfikasi ialah hanya user yang ingin terhubung ke internet melalui hotspot server yang tersedia.

Pengujian

Penting dalam penerapan channel wireless yang baik agar tidak overlapping memilih channel 1 pada frekuensi 2412 GHz, channel 6 pada frekuensi 2437 GHz dan channel 11 dengan frekuensi 2462GHz (Mikrotik.com, 2013). Pada tahap pengujian ini dilakukan scanning sinyal CAP didapat dari hasil konfigurasi *Controller access point system management* (CAPsMAN) menggunakan channel 11 dengan frekuensi 2462 dan sebanyak 4 Access Point di implementasikan pada channel 11.



Sumber: Rifai & Sudibyo (2018)

Gambar 11. Hasil Pengujian Signal CAP

Dari hasil scan wireless signal didapat bahwa dari 4 CAP yang dikonfigurasikan semua CAP telah terregisrasi di channel 11 yaitu 2462 Mhz tujuannya agar signal yang yang didapat tidak overlapping dan dapat membuat roaming antar access point.

Untuk melihat berapa banyak client yang terkoneksi pada jaringan wireless yang menggunakan *Controller access point system management* (CAPsMAN) dapat menggunakan *registration table* dan IP Hotspot Active untuk dapat melihat berapa banyak user yang terkoneksi Hotspot server yang dibuat.

KESIMPULAN

Dengan penerapan dan impelementasi Hotspot Server dan *Controller access point system management* (CAPsMAN) dapat disimpulkan bahwa sangat efektif dan effesien jika kedua konfigurasi ini dikembangkan, karena dari sisi keamanan hotspot server dapat memberi kemananan dari sisi user dan password yang diberikan. Sedangkan dari sisi *Controller access point system management* (CAPsMAN) bisa memberikan pelayanan baik dalam sisi wireless access point dan dapat memudahkan dalam proses distribusi dan maintenance dan ketika beberapa access point di konfigurasi bersama akan menciptakan roaming dan jangkauan area distribusi wireless yang baik.

REFERENSI

Arianto, T. (2009). Implementasi Wireless Local Area Network dalam RT / RW Net. *Jurnal Teknologi Informasi DINAMIK*, *XIV*(2), 152–157.

Kurniawan, E. (2016). Internet Network Topology with Method Optimal for the Needs of Client. *Techno*, *17*(1), 13–18. Retrieved from http://jurnalnasional.ump.ac.id/index.php/Techno/article/view/74

Mikrotik.com. (2013). MikroTik Wireless Networks. Retrieved March 20, 2018, from https://wiki.mikrotik.com/wiki/Testwiki/MikroTik_Wireless_Networks#Channels_and_frequencies

Mikrotik.com. (2017). CAPsMAN. Retrieved March 22, 2018, from https://wiki.mikrotik.com/wiki/Manual:CAPsMAN#CAPsMAN_Configuration_Concepts

Putra, I. E. (2013). Perancangan Jaringan Hotspot Berbasis Mikrotik Router OS 3.3.0. *Jurnal TEKNOIF*, *1*(1), 36–40.

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. In *Seminar Nasional Sistem Informasi 2017 Fakultas Teknologi Informasi – UNMER Malang* (pp. 624–635). Malang.

S'to. (2014). *Wireless Kung Fu : Networking & Hacking*. (Jasakom, Ed.) (2015th ed.). Jakarta: Jasakom. Retrieved from www.jasakom.com

Song, S., & Issac, B. (2014). Analysis of Wifi and Wimax and Wireless Network Coexistence. *International Journal of Computer Networks & Communications*, *6*(6), 63–77. https://doi.org/10.5121/ijcnc.2014.6605

Towidjojo, R. (2017). *Mikrotik Hotspot Server*. (B. Hilika, Ed.) (I). Palu, Indonesia: Ilmu Jaringan Infotama. Retrieved from www.ilmujaringan.com

Towidjojo, R., & Farhan, M. E. (2015). *Router Mikrotik : Implementasi Wireless LAN Indoor*. (Jasakom, Ed.). Jakarta: Jasakom. Retrieved from www.jasakom.com

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.