

Implementasi Wireless Controller Capsman Pada Virtual Local Area Network Menggunakan Virtual Access Point

**Balada Lintang¹, Ahmad Heryanto^{2,3}, Adi Hermansyah¹, Tri Wanda
Septian¹**

¹Teknik Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya, Palembang, Indonesia

²Sistem Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya, Palembang, Indonesia

³Laboratorium Jaringan Komputer dan Komunikasi Data, Universitas Sriwijaya, Palembang, Indonesia

Penulis Korespondensi: Balada Lintang (baladalintang@gmail.com)

Diterima	:	01 Oktober 2022	URL	:	http://jurnal.netplg.com/index.php/jnca/article/view/36
Disetujui	:	10 Oktober 2022	DOI	:	
Diterbitkan	:	30 Oktober 2022	ISSN	:	234-2341

ABSTRAK

Ketika pandemi covid-19 berlangsung, membuat banyak perubahan dalam kehidupan, salah satunya dengan kebutuhan akan internet dalam kegiatan sehari-hari. Baik itu dari individu, instansi pemerintahan, bisnis hingga pendidikan. Demi kebutuhan tersebut, jaringan yang stabil dan pengelolaan secara terpusat sekarang diperlukan. Saat pengelolaan jaringan wireless masih dilakukan secara manual dan menerapkan satu ssid pada access point yang membuat jaringan menjadi lambat dan tidak stabil. Setelah melakukan penelitian, fitur CAPsMAN pada MikroTik dapat memberikan solusi dalam mengelola jaringan wireless secara terpusat, dan dapat mengontrol semua perangkat dalam satu perangkat. Sistem ini dirancang untuk dapat membuat virtual access point lebih dari satu ssid. dengan virtual local area network sebagai layanan dalam pemberian internet protocol address otomatis di setiap virtual access point. Pada penelitian ini pada keamanan jaringan menggunakan metode WPA2-PSK dan Open System Authentication, dan untuk channel yang diterapkan di setiap virtual access point ialah channel ke-1 yaitu 2412.

Kata Kunci : CAPsMAN, Virtual Access Point, Virtual Local Area Network, CAP.

1. PENDAHULUAN

Ketika pandemi covid-19 berlangsung, membuat banyak perubahan dalam kehidupan, salah satunya dengan kebutuhan akan internet dalam kegiatan sehari-hari. Baik itu dari individu, instansi pemerintahan, bisnis hingga pendidikan. Demi kebutuhan tersebut, jaringan yang stabil dan pengelola secara terpusat sekarang diperlukan.

Menurut penelitian [1], ketika menggunakan model jaringan VLAN, ternyata dapat mengoptimalkan komunikasi data pada rumah sakit mata ramata. Selain menghemat ruang, VLAN dapat menghemat biaya karena tidak perlu melakukan banyak perubahan untuk sistem ini. Namun dibutuhkannya layanan secara otomatis untuk memberikan alamat IP kepada client yang terkoneksi ke jaringan.

Menurut penelitian [2], ketika menggunakan wireless mesh network dengan teknologi control access point dapat memudahkan client mengakses internet secara mobile dalam satu ssid walaupun berpindah-pindah tempat tanpa harus autentikasi ke jaringan hotspot lagi. Namun pada access point hanya memiliki satu ssid yang dapat membuat jaringan menjadi lambat dan tidak stabil. Berdasarkan penelitian [1], [2], dibutuhkan sebuah fitur bernama multiple ssid yang di kontrol dengan CAPsMAN. Multiple ssid adalah fungsi untuk mengelola jaringan nirkabel, membuat jaringan lebih mudah digunakan. Dalam memakai fungsi ini, administrator dapat mengontrol

virtual access point dan mengirimkan beberapa ssid di bawah bandwidth yang sama. Fitur CAPSMAN merupakan pengelola jaringan wireless secara terpusat dan dapat memberikan solusi untuk mengelola virtual access point yang masih banyak dilakukan secara manual. CAPSMAN berfungsi untuk mengelola semua perangkat dalam satu pengontrol perangkat [3].

Berdasarkan uraian latar belakang pada proyek akhir ini akan mengutamakan tentang implementasi wireless controller CAPsMAN pada virtual local area network menggunakan virtual access point. Pada penelitian ini diharapkan dapat membuat jaringan wireless yang di kontrol secara terpusat dengan berbeda segmen namun sama secara logikal.

Dalam proyek akhir ini penulis menggunakan peralatan yang tersedia dan konfigurasi akan berlangsung di laboratorium jaringan komputer dan komunikasi data, fakultas ilmu komputer Universitas Sriwijaya Palembang.

2. TINJAUAN PUSTAKA

A. Virtual Local Area Network

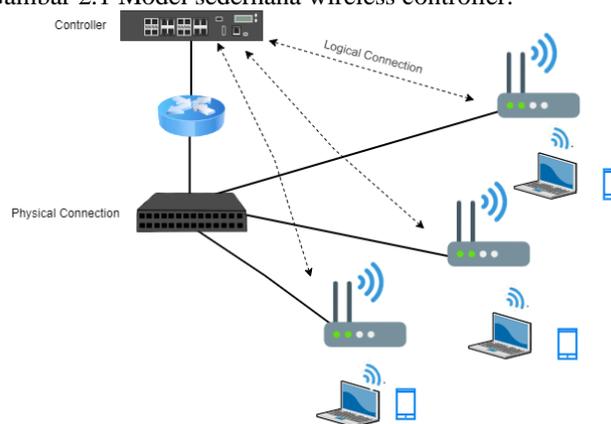
Virtual Local Area Network (VLAN) adalah jaringan area lokal (LAN) yang dapat dirancang untuk berkomunikasi seperti koneksi kabel, menggunakan pengguna seolah-olah mereka berada di satu LAN dan berbagi jaringan tunggal. [4].

VLAN adalah proses pemisahan koneksi fisik pada LAN menjadi beberapa koneksi jaringan. Jaringan itu penting, membuat pengunggahan data lebih cepat dan meningkatkan kinerja jaringan. [5]. Oleh karena itu, pembentukan VLAN tidak didasarkan pada koneksi fisik, tetapi pada koneksi langsung, jauh lebih sederhana.

B. Wireless Controller

Wireless controller merupakan perangkat jaringan yang digunakan sebagai pengontrol jaringan untuk memantau dan dapat mengelola access point secara massal [6]. Memungkinkan perangkat wireless untuk terhubung di mana saja (selama berada dalam jangkauan tertentu).

Oleh karena itu, dapat mengurangi waktu yang dihabiskan untuk mengkonfigurasi, pemantauan, dan pemecahan masalah pada jaringan besar. Wireless Controller dapat memerintahkan perangkat yang dipilih atau sekelompok perangkat untuk menerapkan pengaturan yang telah dikonfigurasi pada pengontrol wireless secara bersamaan. Terlihat pada Gambar 2.1 Model sederhana wireless controller.

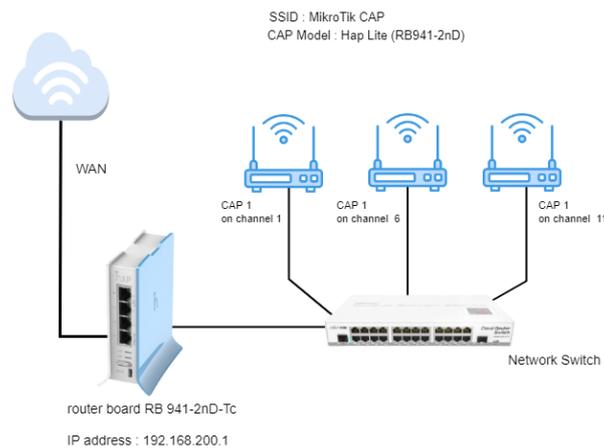


Gambar 1 Model sederhana wireless controller

C. CAPsMAN

Controller Access Point System Management (CAPsMAN) dapat digunakan untuk mengelola berbagai perangkat access point MikroTik dalam satu perangkat. Fungsi CAPSMAN adalah untuk menyediakan koneksi wireless, CAPSMAN hanya dapat beroperasi setelah koneksi antara CAPSMAN dan CAP dibuat. Dengan VLAN juga dapat diimplementasikan pada jaringan wireless.

Ketika dapat menjalankan service VLAN pada jaringan wireless harus digunakan local forwarding untuk membuat jalur data pada CAPSMAN [7]. Terlihat pada Gambar 2.2 Model sederhana dari sistem CAPsMAN.



Gambar 2. Model sederhana dari sistem CAPsMAN

D. Virtual Access Point

Virtual access point adalah antarmuka nirkabel virtual untuk membuat beberapa virtual access point dari satu antarmuka. Jadi hanya perlu menggunakan satu interface wireless fisik, dapat membuat beberapa virtual access point, ssid, network, mac address, setiap virtual access point berbeda-beda.

Namun, ia menggunakan frekuensi dan pita frekuensi yang sama dengan wlan induknya (sebenarnya) [7].

E. SSID

Service set identifier (SSID) adalah identitas yang ditetapkan untuk jaringan wireless. Wireless harus menggunakan ssid dengan huruf besar-kecil yang sama. Berkomunikasi dengan access point (AP). ssid terdiri dari string teks hingga 32 byte. Banyak access point (AP) pada jaringan dapat menggunakan ssid yang sama [7].

SSID digunakan untuk mengatur jaringan yang akan anda gunakan. Oleh karena itu, ketika Anda ingin menggunakan jaringan nirkabel, perangkat yang Anda gunakan harus memilih jaringan LAN nirkabel yang ingin Anda gunakan.

F. Datapath

Datapath adalah kumpulan set register yang terkait dengan register tautan dan register tambahan. Register ini dipergunakan sebagai sumber untuk mengeksekusi instruksi. Jalur data terdiri dari beberapa blok adalah penghitung program, digunakan untuk menyimpan alamat instruksi kemudian akan diambil, dan kemudian register alamat memori menyimpan alamat memori, dan kemudian data akan dikembalikan ke CPU, Seterusnya di teruskan ke register data memori, yang berisi data yang akan digunakan disimpan di RAM. Fungsi datapath pada nirkabel adalah menjadi jalur disebuah jaringan.

G. Band

Kegunaan band dalam jaringan nirkabel adalah menentukan frekuensi channel dan lebar channel yang dapat dilewati [8].

H. Channel

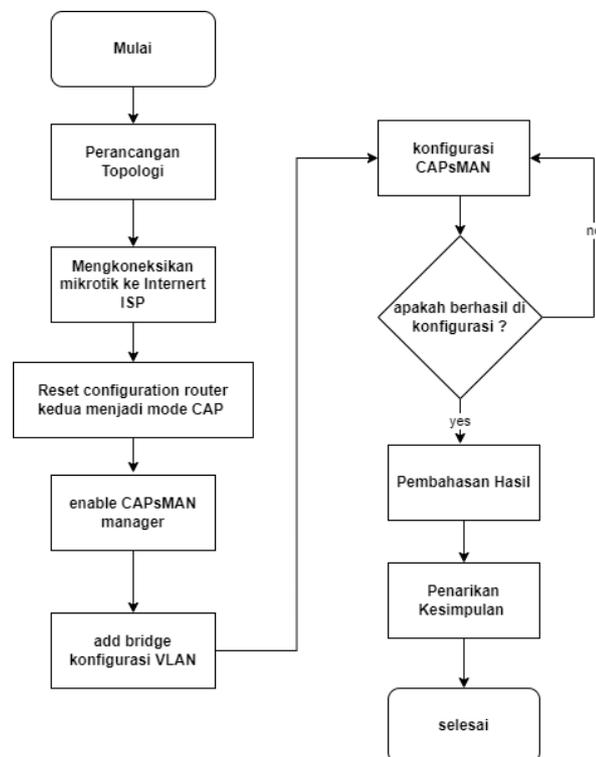
Channel adalah jalur pemisah di Internet [8]. Di saluran Frekuensi operasi 802.11a adalah 5.15 - 5.875 Ghz, 802.11b dan 802.11g Frekuensi bekerja pada 2,4 - 2,497 Ghz. Channel nirkabel terbentuk dari channel frekuensi 2,4 GHz dan channel dengan frekuensi 5 GHz.

I. Frekuensi

Adanya jaringan nirkabel, tentunya dengan berbagai frekuensi dan fungsi frekuensi yang berbeda-beda pada jaringan nirkabel digunakan sebagai jalur komunikasi [8].

3. METODELOGI PENELITIAN

Dalam penelitian ini yang pertama dilakukan adalah melakukan penelitian literatur untuk mencari bahan referensi yang berkaitan dengan penelitian tersebut. Tahap selanjutnya adalah perancangan sistem yang meliputi perancangan topologi, spesifikasi kebutuhan perangkat keras, spesifikasi perangkat lunak. Kemudian, sebelum Implementasi Wireless Controller CAPsMAN Pada Virtual Local Area Network Menggunakan Virtual Access Point dilakukan analisa kebutuhan barang. Selanjutnya instalasi dan konfigurasi. Hasilnya akan dibahas, dan kesimpulan serta saran akan diambil dari penelitian ini. Pada Gambar 3.1 bentuk flowchart dari kerangka kerja penelitian.

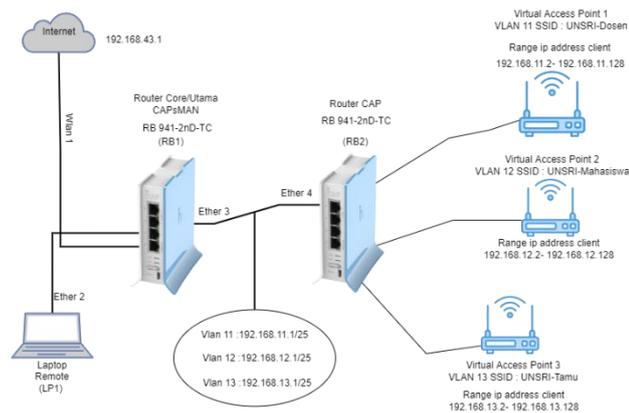


Gambar 3. Flowchart metode penelitian

4. HASIL PENELITIAN

Kegiatan penelitian proyek akhir dilakukan di laboratorium jaringan komputer dan komunikasi data Fakultas Ilmu Komputer Universitas Sriwijaya, dari bulan November 2021 hingga Januari 2022. Beberapa tahapan, termasuk desain topologi, identifikasi kebutuhan perangkat keras dan perangkat lunak, instalasi dan konfigurasi sistem, dan rencana pengujian.

- A. Perancangan Topologi
Pada tahapan desain topologi seperti pada Gambar 4 berikut :



Gambar 4. Desain Topologi

Pada perancangan ini menggunakan 2 router MikroTik, dimana router 1 dijadikan sebagai router CAPsMAN dan router ke-2 menjadi CAP, untuk koneksi internet ISP ke mikrotik melalui router capsman yang menggunakan interface WLAN pada router CAPsMAN, lalu untuk meremote/konfigurasi router menggunakan laptop yang terhubung ke ether2 pada router core, untuk koneksi terhadap router pertama dan kedua digunakan kabel yg terhubung di ether3 CAPsMAN dan ether4 yang terhubung ke router CAP, lalu di buat VLAN 11 dengan IP address 192.168.11.1/25, VLAN 12 dengan IP address 192.168.12.1/25, VLAN 13 dengan IP address 192.168.13.1/25 sebagai service dhcp pada VAP, dan pada router CAP dibuat VAP sebanyak 3 SSID, yang pertama dengan SSID UNSRI-Dosen dengan range IP client 192.168.11.2-192.168.11.128, yang kedua dengan SSID UNSRI-Mahasiswa dengan range IP client 192.168.12.2-192.168.12.128, yang ketiga dengan SSID UNSRI-Tamu dengan range IP client 192.168.13.2-192.168.13.128.

Dalam menerapkan wireless controller secara nyata, diperlukan beberapa perangkat keras yang mendukung jaringan untuk melakukan wireless controller menggunakan fitur CAPsMAN. . Perangkat Keras yang diperlukan pada penelitian ini pada Tabel 1, perangkat lunak yang digunakan dalam penelitian ini pada Tabel 2.

Tabel 1. Kebutuhan Perangkat Keras

No	Perangkat	Jumlah	Keterangan
1.	Router MikroTik RB941-2nD-TC	2	Sebagai penghubung perangkat dalam satu jaringan dan melakukan konfigurasi VLAN, CAPsMAN, VAP.
2.	Laptop Lenovo Ideapad 3	1	Sebagai perangkat yang dapat meremote dan mengkonfigurasi mikrotik.
3.	Laptop-Client	2	Sebagai perangkat client untuk mengakses dan menguji jaringan internet.
4.	HP Redmi 6	1	Sebagai ISP jaringan internet.
5.	HP-Client	2	Sebagai perangkat client untuk mengakses dan menguji jaringan internet.

Tabel 2. Kebutuhan Perangkat Lunak

No	Sistem	Tools	Keterangan
1.	Remote Access Login	WinBox	Versi 3.31
2.	Web Browser	Web client	Ex: Firefox/Chrome/Operas

B. Mengkoneksikan MikroTik Utama ke Internet ISP

Sesuai dengan kerangka penelitian, hal pertama yang dilakukan ialah mengkoneksikan jaringan internet ke MikroTik. Hal yang pertama yang dilakukan ialah mengkonfigurasi WLAN1.

Konfigurasi WLAN ini dilakukan dengan mengkoneksikan MikroTik yang digunakan dengan internet ISP, dalam penelitian ini digunakan hotspot dari smartphone sebagai internet ISP. Yang pertama dilakukan adalah buka menu interfaces pada mikrotik kemudian aktifkan wlan lalu klik dua kali maka akan muncul tampilan seperti diatas. Kemudian, atur modenya menjadi station, pilih band nya menjadi 2 GHz-B/G/N dan channel width nya menjadi 20 MHz. Lalu, scan internet ISP yang akan kita gunakan yaitu "@BL" kemudian sambungkan dan otomatis ssid dan frequency akan terisi. Frequency itu adalah channel dan kali ini menggunakan channel sesuai dengan frequency nya yaitu 2,4 Hz.

C. Men-reset router MikroTik kedua menjadi mode CAP.

Men-setting router MikroTik kedua menjadi mode CAP, agar perangkat wireless access point dapat terkonfigurasi terpusat oleh CAPsMAN. Yang pertama dilakukan ialah login ke MikroTik kedua lalu pilih system pilih menu reset configuration kemudian centang keep user configuration, caps mode dan no default configuration atau juga bisa memanfaatkan menu IP>neighbor karena router utama dan kedua telah tersambung melalui ether3 kemudian melakukan remote melalui MAC Telnet kemudian masukkan login dan password pada mikrotik kedua, lalu untuk reset dapat melakukan melalui terminal dengan perintah system reset-configuration caps-mode=yes kemudian pilih yes.

D. Meng-enable CAPs Manager

Untuk mengaktifkan router utama sebagai CAPsMAN. Pertama, buka menu CAPsMAN lalu klik manager kemudian centang enabled. Sesaat setelah kita mengaktifkan CAPsMAN secara otomatis di menu CAPsMAN pada CAP interfaces akan muncul interfaces wlan yang sebelumnya sudah diaktifkan pada router kedua.

E. Membuat interface bridge

Pada tahap ini membuat interface bridge. Pertama buka menu Bridge lalu buat nama interface "bridge1-AP" kemudian klik OK. Fitur bridge ini berfungsi untuk menggabungkan beberapa interface sehingga gabungan interface tersebut berada dalam satu segment alamat IP.

F. Membuat interface VLAN

Pertama pilih menu interfaces, lalu pilih VLAN, kemudian buat nama "VLAN 11-Dosen", atur VLAN ID menjadi "11" dan pilih interface nya bridge1-AP. Lalu buat nama "VLAN 12-Mahasiswa", atur VLAN ID menjadi "12" dan pilih interface nya bridge1-AP. Kemudian buat nama "VLAN 13-Tamu", atur VLAN ID menjadi "13" dan pilih interface nya bridge1-AP.

G. Memberikan IP address

Pada tahap ini memberikan ip address di setiap interfaces VLAN. Yang pertama dilakukan adalah menambahkan IP address 192.168.11.1/25 pada interfaces pada VLAN 11-Dosen, IP address 192.168.12.1/25 pada interfaces VLAN 12-Mahasiswa dan IP address 192.168.13.1/25 untuk VLAN 13 pada interfaces VLAN 13-Tamu kemudian klik apply dan oke maka IP akan otomatis ditambahkan.

H. Menambahkan service dhcp pada setiap VLAN.

Pada tahap ini DHCP server sangatlah tepat digunakan untuk jaringan yang memiliki user yang bersifat dinamis, dengan jumlah user yang selalu berubah-ubah. Pertama yang dilakukan adalah buka DHCP server pada menu IP dan pilih DHCP set up. Lalu pilih interfaces yang digunakan vlan 11, vlan 12 dan vlan 13. Untuk mengatur gateway dan yang lainnya hanya masukkan IP yang telah terdaftar untuk wireless dan ikuti saja perintahnya dengan klik next.

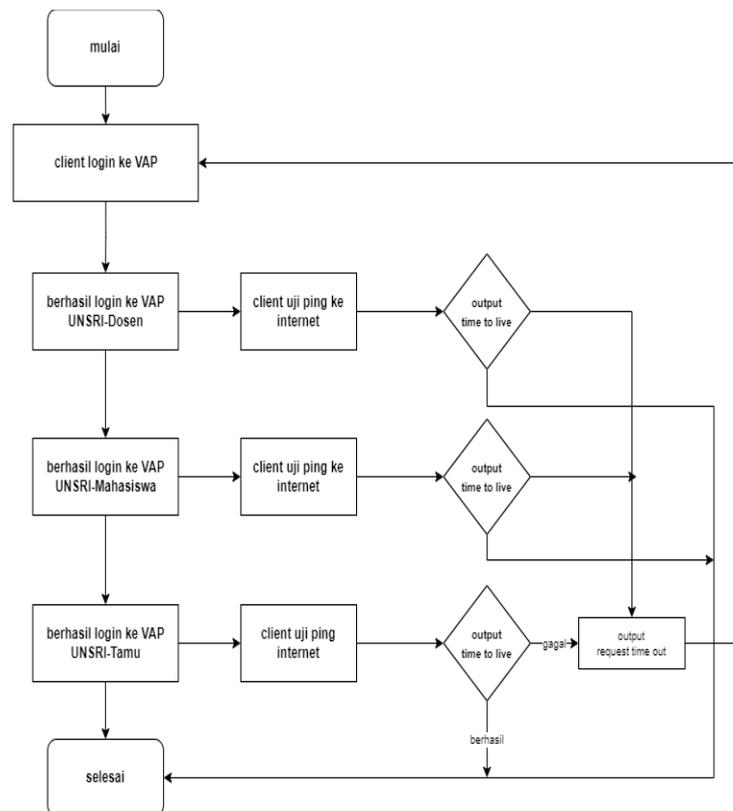
I. Konfigurasi CAPsMAN

Pada tahap ini pada virtual access point 1 dan 2 sama saja konfigurasinya menyesuaikan namun yang membedakan virtual access point pertama menjadi Master pada VAP dan berbeda passphrase dengan VAP 2, untuk VAP 3 yang membedakan hanya metode keamanan bersifat open system authentication. Pada konfigurasi ini memanfaatkan virtual access point yang dapat membuat interface wireless lebih dari satu. Hal pertama yang dilakukan adalah klik CAPsMAN pilih interface wireless CAP, Klik dua kali kemudian atur name wireless menjadi "cfg 1-Dosen" pilih mode ap, buat ssid menjadi "UNSRI-Dosen" lalu pilih country menjadi "indonesia". Jika sudah diatur, kemudian masuk ke menu channel pada frequency ubah menjadi "2412", pada tab control

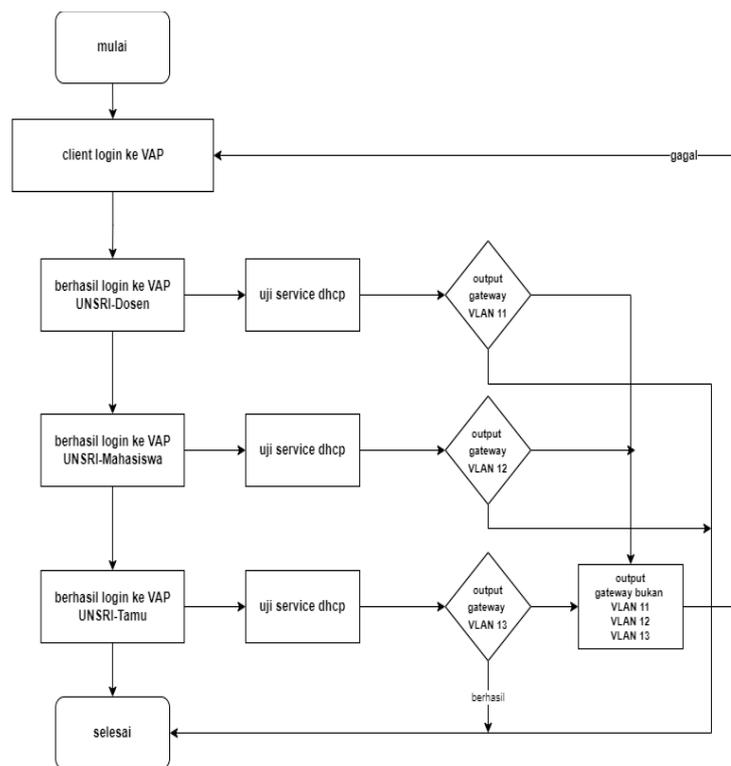
channel width masukkan parameter “20Mhz” dan band “2ghz-b/g/n”. Klik menu datapath ubah tab bridge menjadi “bridge1-AP”, lalu pada tab VLAN mode menjadi “use tag”, kemudian pada tab VLAN ID masukkan “11 untuk VAP 1” dan “12 untuk VAP 2” dan “13 untuk VAP 3”. Pada menu security, pada tab Authentication Type centang “WPA2 PSK, lalu tab Encryption centang “aes ccm dan tkip”, kemudian pada tab passphrase tambahkan sandi yang diinginkan.

J. Skenario Pengujian

Pada tahap percobaan, penelitian ini memiliki dua skenario percobaan, skenario pertama dilakukan dengan pengujian komunikasi dari client untuk mengakses virtual access point. Untuk skenario percobaan kedua dilakukan dengan pengujian apakah setiap virtual access point mendapatkan IP Address sesuai dengan VLAN yang telah dibuat. Terlihat pada gambar 5 skenario pertama dan 6 skenario kedua.



Gambar 5. Skenario Pertama

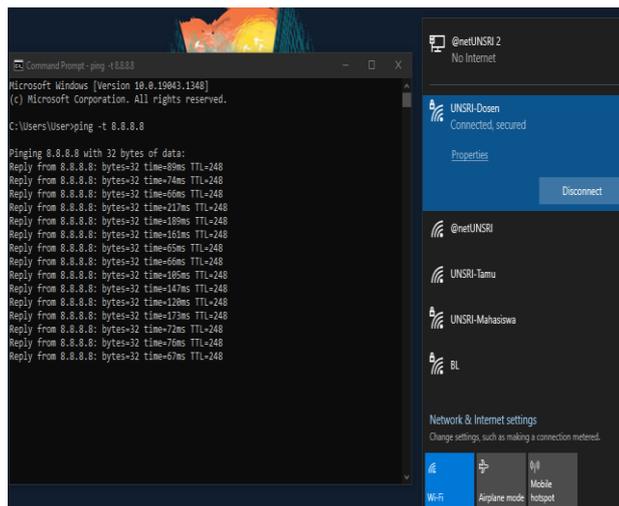


Gambar 6. Skenario Kedua

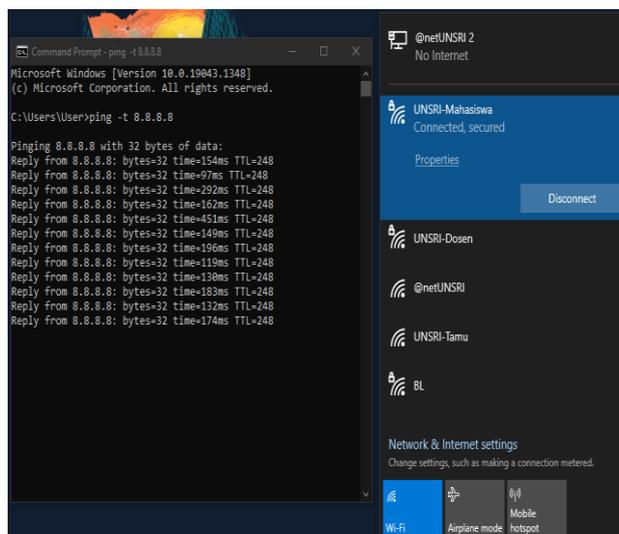
K. Hasil Pengujian Dan Analisa

Pada tahap ini meliputi tahap pengujian dan pembahasan hasil pengujian, yang dibagi menjadi dua tahap. Langkah pertama dilakukan dengan menguji sistem keamanan menggunakan metode WPA2-PSK dan open untuk mengakses jaringan internet, output yang diharapkan pada tahapan ini yaitu time to live (TTL). Tahap kedua dilakukan dengan memverifikasi di setiap virtual access point mendapatkan IP address sesuai dengan konfigurasi VLAN yang telah dibuat.

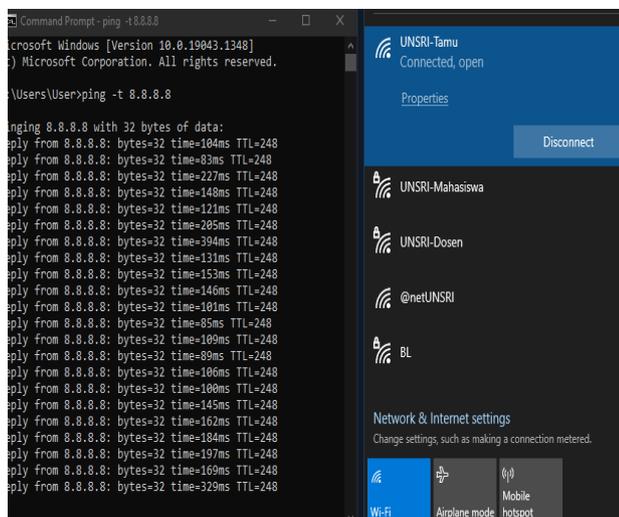
Pengujian Koneksi internet di setiap virtual access point, Pada pengujian ini client 1 masuk ke virtual access point dengan ssid UNSRI-Dosen, masukkan password yang sudah diatur sebelumnya. Untuk password nya yaitu admin123. Kemudian client 2 masuk ke virtual access point dengan ssid UNSRI-Mahasiswa, masukkan password yang sudah diatur sebelumnya. Untuk password nya yaitu User1234. Dan untuk client 3 masuk ke virtual access point dengan ssid UNSRI-Tamu, dengan hanya melakukan autentikasi saja tanpa perlu memasukkan password. Jika berhasil masuk ke virtual access point dan dilakukan pengujian, dengan menggunakan metode Internet Control Message Protocol (ICMP) dengan menggunakan command ping merupakan singkatan dari Packet Internet Network Groper yang merupakan perintah untuk mengecek status dan keberadaan host dalam sebuah jaringan internet. Sedangkan perintah ping -t merupakan melakukan ping secara terus menerus, cara ini berguna untuk memantau kualitas koneksi secara real time. Terlihat pada Gambar 7. berhasil connected ke UNSRI-Dosen, Gambar 8. berhasil connected ke UNSRI-Mahasiswa dan Gambar 9. berhasil connected ke UNSRI-Tamu.



Gambar 7. Berhasil connected ke UNSRI-Dosen



Gambar 8. Berhasil connected ke UNSRI-Mahasiswa



Gambar 9. Berhasil connected ke UNSRI-Tamu

Pengujian verifikasi DHCP di setiap virtual access point, Pada pengujian ini client masuk ke virtual access point dengan ssid UNSRI-Dosen, UNSRI-Mahasiswa dan UNSRI-Tamu lalu memasukkan password yang sudah diatur sebelumnya. Jika berhasil masuk ke virtual access point dan dilakukan pengujian pada client yang menggunakan komputer dan laptop dengan menggunakan command ipconfig merupakan perintah yang digunakan untuk mengetahui ip address di komputer. Pada client yang menggunakan smartphone cukup dengan melihat ip address dengan masuk ke menu Wi-Fi. Terlihat pada gambar 10. client ke-4 berhasil mendapatkan ip address dengan gateway vlan 11, Gambar 11, client ke-5 berhasil mendapatkan ip address dengan gateway vlan 12 dan Gambar 12, client ke-6 berhasil mendapatkan ip address dengan gateway vlan 13.

```
Select C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . . :
    Link-Local IPv6 Address . . . . . : fe80::2902:2e1e:70ba:b36709
    IPv4 Address. . . . . : 192.168.11.128
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 192.168.11.1

C:\Users\user>
```

Gambar 10. Client ke-4 berhasil mendapatkan ip address dengan gateway vlan 11

```
Command Prompt

IPv4 Address. . . . . : 192.168.88.2
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 192.168.200.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.200.1

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Wi-Fi:

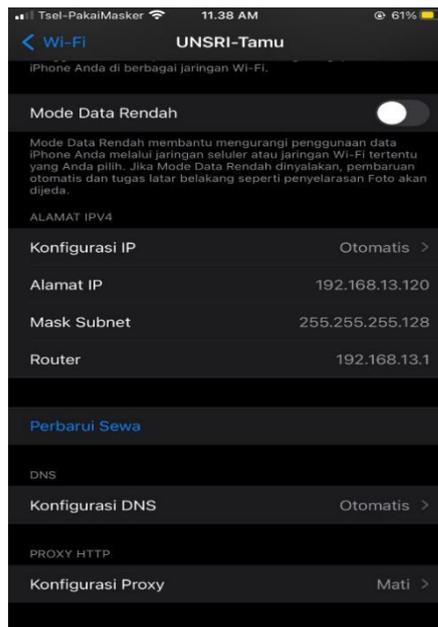
    Connection-specific DNS Suffix . . :
    Link-Local IPv6 Address . . . . . : fe80::3070:3f2a:9626:808821
    IPv4 Address. . . . . : 192.168.12.124
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 192.168.12.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

C:\Users\user>
```

Gambar 11. Client ke-5 berhasil mendapatkan ip address dengan gateway vlan 12



Gambar 12. Client ke-6 berhasil mendapatkan ip address dengan gateway vlan 13

5. KESIMPULAN

Berdasarkan penelitian yang telah di terapkan, maka dapat disimpulkan sebagai berikut bahwa Implementasi controller wireless CAPsMAN dengan virtual local area network telah berhasil dibuat di setiap virtual access point, hasil dari pengujian didapatkan sinyal yang dipancarkan setiap virtual access point berjalan dengan baik. Dalam penggunaan fitur CAPsMAN dapat memudahkan dalam mengontrol 3 (tiga) virtual access point secara terpusat pada 1 (satu) perangkat Mikrotik. Dengan melakukan penerapan virtual access point pada jaringan wireless diperlukannya virtual local area network untuk client yang terkoneksi mendapatkan alamat ip address.

DAFTAR PUSTAKA

- [1] B. B. Yoga and M. A. Raharja, "Implementasi Vlan (Virtual Local Area Network) Pada Rumah Sakit Mata Ramata," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 7, no. 3, p. 177, 2019, doi: 10.24843/jlk.2019.v07.i03.p07.
- [2] J. Al Amien and C. Wibowo, "Implementasi Wireless Mesh Network Menggunakan Controller Access Point System Manager Di Lingkungan Kampus Universitas Muhammadiyah Riau," *J. Fasilkom*, vol. 7, no. 2, pp. 273–283, 2018, doi: 10.37859/jf.v7i2.658.
- [3] F. Febrianti, P. Haryani, and C. Iswahyudi, "PERANCANGAN JARINGAN WIRELESS MULTIPLE SSID MENGGUNAKAN FITUR MIKROTIK CAPSMAN (Studi Kasus di Laboratorium Jaringan Kampus III IST AKPRIND Yogyakarta)," *J. Jarkom*, vol. 8, no. 2, pp. 65–72, 2020.
- [4] S. K. Saad, R. Umar, and A. Fadlil, "Implementasi dan desain vlan," *Semin. Nas. Inform. 2018 (semnasif 2018)*, vol. 2018, no. November, pp. 147–153, 2018.
- [5] A. Hidayat, "Perancangan Virtual Local Area Network (VLAN) Pada Lab Komputer D-III Sistem Informasi Universitas Muhammadiyah Metro (UM Metro)," *Konf. Nas. Sist. Inf. 2018*, pp. 739–745, 2018, [Online]. Available: <http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/442>.
- [6] B. Rifai and A. Sudiby, "Manajemen Wireless Access Point Pada Hotspot Server," *J. PILAR Nusa Mandiri*, vol. 14, no. 1, pp. 111–116, 2018.
- [7] T. A. A. S. E. K. Pratama, I. N. Leksono, and R. S. Anwar, "Implementasi Hotspot Login Menggunakan Capsman Mikrotik Pada Wilayah Yang Berbeda," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019, [Online]. Available: <http://www.akrabjuara.com/index.php/akrabjuara/article/view/460/383>.
- [8] M. R. Arief, "Teknologi Jaringan Tanpa Kabel (Wireless)," *Semin. Nas. Teknol. 2007*, vol. 2007, no. November, pp. 1–8, 2013.