ELIT JOURNAL
Electrotechnics And Information Technology
P-ISSN: 2721-5636 | E-ISSN: 2721-5644 Vol. 5 No. 1, April 2024

Implementasi *Repeater* Berdasarkan Pemetaan Jangkauan Dan Pemakaian *Channel* Sinyal *Access point* Hotspot Pada Jurusan Elektro Politeknik Negeri Pontianak

Muhammad Diponegoro[1], Rusman[2], Suharto[3]
Jurusan Teknik Elektro, Politeknik Negeri Pontianak, Pontianak – Kalimantan Barat
e-mail: muhammaddiponegoro@gmail.ac.id, rusman.dn@gmail.com, suharto@gmail.com

Abstrak

Perkembangan infrastruktur jaringan dan internet saat ini telah merambah pada berbagai bidang. Politeknik Negeri Pontianak (POLNEP) adalah salah satu lembaga pendidikan tinggi vokasi yang ada di Pontianak yang menggunakan internet sebagai media pembelajaran termasuk pada Jurusan Teknik Elektro. Namun pada saat ini jaringan internet di Jurusan Elektro Politeknik Negeri Pontianak seiring bertambahnya jumlah dosen dan mahasiswa menjadi tidak stabil dan lambat serta tidak dapat menjangkau suluruh tempat dan mempengaruhi aktivitas kemahasiswaan yang di lakukan. Salah satu penyebabnya yaitu ketebatasan pada sinyal access point atau hotspot pemancar internet wireless. Tujuan dari penelitian ini adalah mengimplementasikan Repeater pada jurusan Teknik Elektro Polnep berdasarkan pemetaan jangkauan dan pemakaian Channel Sinyal Access point Hotspot. Adapun metode penelitian yang dilakukan yaitu studi Literatur, pengamatan performa jaringan Jurusan Teknik Elektro Polnep, pengamatan topologi jaringan Jurusan Elektro Polnep, pengamatan topologi infrastruktur jaringan, pengamatan topologi jaringan. Konfigurasi perangkat Repeater, implementasi perangkat Repeater, persiapan perangkat pengukuran, perangkat QoS setelah implementasi Repeater, membandingkan hasil pengukuran setelah implementasi, selesai sedangkan luaran tambahan dicapai yaitu berupa teknologi tepat guna yang dapat diterapkan pada Jurusan Teknik Elektro Polnep.

***Kata kunci**: Basis Data, Sistem Informasi, Elektronika*

Abstract

The development of network and internet infrastructure has now spread to various fields. Pontianak State Polytechnic (POLNEP) is one of the vocational higher education institutions in Pontianak that uses the internet as a learning medium, including in the Electrical Engineering Department. However, currently the internet network in the Electrical Department of Pontianak State Polytechnic, along with the increasing number of lecturers and students, has become unstable and slow and cannot reach all places and affects the student activities carried out. One of the causes is the limitation of the access point signal or wireless internet transmitter hotspot. The aim of this research is to implement a Repeater in the Polnep Electrical Engineering department based on mapping the reach and use of Hotspot Access Point Signal Channels. The research methods used were literature studies, observing the network performance of the Polnep Electrical Engineering Department, observing the network topology of the Polnep Electrical Engineering Department, observing the network infrastructure topology, observing network topology. Configuration of Repeater devices, implementation of Repeater devices, preparation of measurement devices, QoS devices after Repeater implementation, comparing measurement results after implementation, are completed while additional output is achieved, namely in the

form of appropriate technology that can be applied to the Polnep Electrical Engineering Department.

Keywords : *Database, Information System, Electronics*

1. PENDAHULUAN

Politeknik Negeri Pontianak (POLNEP) sebagai Politeknik yang mengalami pertumbuhan jumlah mahasiswa yang sangat signifikan. Dari jumlah jurusan, prodi, gedung dan jumlah mahasiswa. Perkembangan teknologi yang pesat juga tidak luput mempengaruhi teknologi yang dipakai POLNEP untuk mendukung aktivitas akademik maupun operasional, seperti jaringan komputer dan internet.

Selain menggunakan jaringan kabel, komunikasi antar gedung terhubung melalui jaringan *wireless*. Fasilitas akses internet publik juga banyak yang menggunakan *wireless*, selain dapat menjangkau banyak area juga memudahkan pengguna jika memiliki laptop atau Handphone.
Lokasi-lokasi hotspot yang ada di gedung teori Elektro Polnep dengan jangkauan dan pemakaian *Channel* sinyal dari masing-masing *access point* dengan *me-scanning received of signal strength*. Dari hasil *scanning* akan menghasilkan pemetaan jaringan *wireless* secara riil beserta detail jangkauan area *horizontal* dan *Channel* yang digunakan serta informasi status *enkripsi*. Penelitian ini akan dikembangkan perencanaan atau penataan *access point* secara optimal di POLNEP berbasis GIS yang digunakan sebagai acuan bagi pengelola jaringan komputer di POLNEP.

2. METODE

2.1 Bahan Penelitian

- Data *access point* masing-masing unit di Gedung Teori POLNEP.
- Foto udara dan data spasial POLNEP.
- Hasil *wardriving* jaringan *wireless* di unit-unit POLNEP.

2.2 Alat Penelitian

- Perangkat Wardriving meliputi:
- Bluetooth GPS Holux (GPS receiver).
- Perangkat lunak NetStumbler.
- Laptop IBM R50e dengan network adapter internal Intel(R) PRO/ *Wireless* 2200BG.
- PCMCIA card (veritech VAC2511-D 802.11b). Link Quality=0/92, Signal level=-68 dBm, Noise level=-122 dBm.
- 2,4 GHz 7 dbi Antena *wireless* LAN bermagnet jenis omnidirectional.
- Aplikasi pemetaan GIS (Global Mapper v8.3, ArcView dan aplikasi konversi data NetStumbler di http://www.gpsvisualizer.com/map?output_wifi.
- VisiWave *Site survey* SO (Software Only) dan VisiWave *Site survey* Report.

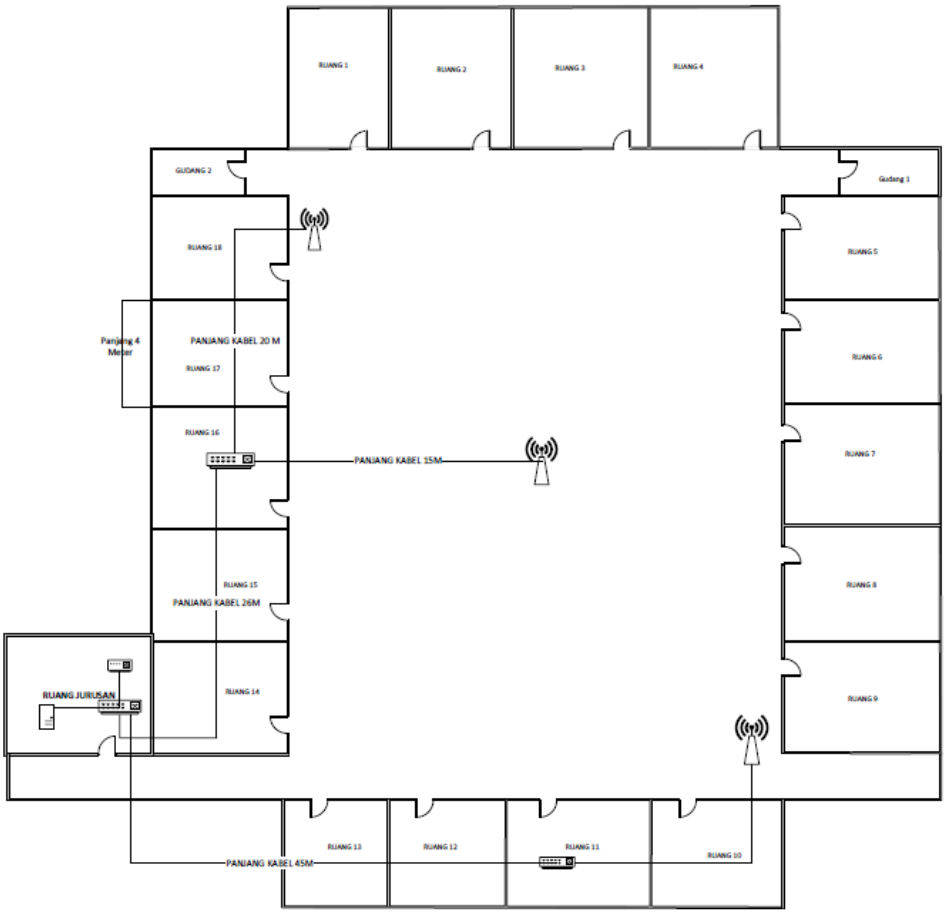
2.3 Jalan Penelitian

Penelitian dilakukan dengan cara:

- Pengambilan data *access point* di gedung Elektro Polnep Lt. 2 dengan cara Wardriving. Cara ini dilakukan untuk mendata *access point* dengan software NetStumbler dengan posisinya jika terdeteksi oleh GPS.
- Data Wardriving dalam format file ns1 di-upload ke http://www.gpsvisualizer.com/map?output_wifi. Sehingga diperoleh pemetaan data *access point* beserta signal strength yang terdeteksi GPS.

- Data *access point* yang diperoleh sebelumnya di data kembali dengan survei lapangan. Cara ini ditempuh untuk memverifikasi lokasi *access point* di masing-masing gedung
- Hasil survei lapangan akan di tuangkan dalam data spasial dengan lokasi yang riil.
- Pemetaan riil tersebut akan dianalisa dengan teori pemakaian *Channel* dan jangkauannya berdasarkan lokasi *access point* pada software aplikasi GIS.
- Hasil analisa akan menghasilkan perbaikan atau penataan instalasi *access point* dengan pemakaian *Channel* dan jangkauan.

Penelitian dilakukan pada gedung elektro lantai 2 dengan pemantauan sekali waktu pada jam sibuk, pemantauan dilakukan menggunakan peralatan yang sudah direncanakan sebelumnya. Berikut ini adalah gambaran denah ruang pada gedung elektro lantai 2:



Gambar 1 denah lokasi

Ruang terdiri dari 18 kelas dan 1 ruang jurusan, berikut ini foto lokasi kelas dari sebelah kanan,

Gambar 2 foto tampak samping

Gambar 3 foto tampak depan kelas

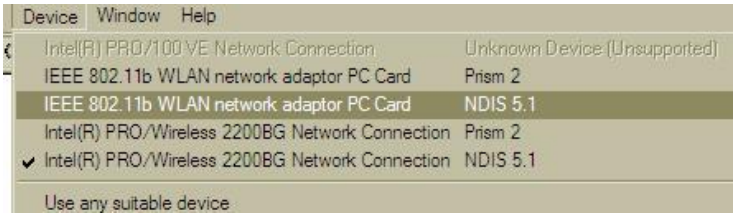
Gambar 4 foto tampak dalam kelas

3. HASIL DAN PEMBAHASAN

Pengambilan data dilakukan dengan 2 cara yaitu *WarDriving*: cara ini ditempuh untuk mengetahui jaringan *wireless* di lokasi survey baik yang dimiliki internal maupun eksternal. Wawancara dengan Admin jaringan: cara ini ditempuh untuk mendata *access point* yang dimiliki yaitu 18 kelas dan 1 ruangan jurusan dan wawancara kepada pengguna layanan internet, *WarDriving* dilakukan pada tanggal 24 September 2023 dengan hasil seperti yang ditunjukkan pada table 1 hasil *WarDriving*. Peralatan yang akan digunakan untuk *wardriving* di persiapkan sebagai berikut: PCMCIA card dihubungkan dengan antena luar melalui pigtail. Antena ini untuk memperkuat daya tangkap signal strength *access point* dari PCMCIA. PCMCIA card yang terhubung dengan antena luar dimasukkan ke slot PCMCIA laptop. Koneksi antara antena luar, pigtail dan PCMCIA dapat dilihar di gambar 5 Koneksi antara Antena Luar, Pigtail dan PCMCIA Card pada Laptop.

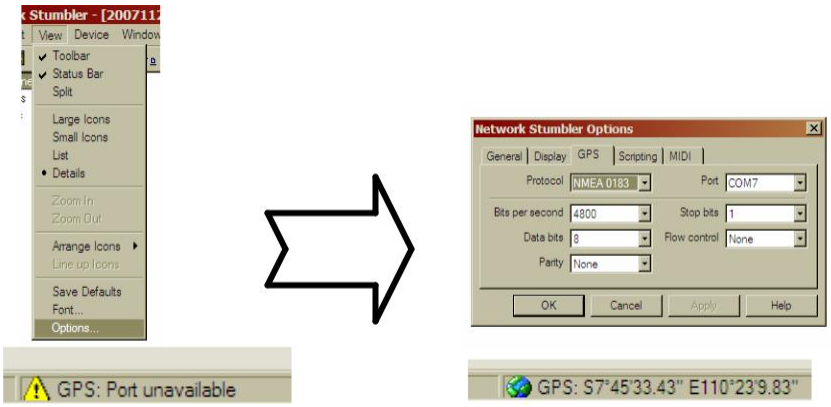
Gambar 5 Koneksi antara Antena Luar, Pigtail dan PCMCIA Card pada Laptop

Software untuk men-scanning sinyal *access point*, NetStumbler akan mendeteksi device dari PCMCIA. Di menu device, masing-masing device memiliki dua versi NDIS 5.1 dan Prism 2. Seperti terlihat pada gambar 6.



Gambar 6 Seting Device pada NetStumbler

Pemilihan versi ini dilakukan dengan men-scanning sinyal *access point* dengan salah satu versi device tersebut. Hal ini mempengaruhi compatible tidaknya versi device dengan NetStumbler, yang hasilnya dapat diketahui dengan dapat tidaknya NetStumbler mendeteksi sinyal *access point* pada awal scanning. (Sundar, April 2006). Setelah proses pengujian, PCMCIA yang digunakan compatible jika menggunakan chipset NDIS 5.1. Pendeteksi lokasi *access point* saat wardriving digunakan Bluetooth GPS yang terintegrasi dengan *NetStumbler*. Sehingga saat *NetStumbler* mendeteksi sinyal *access point* baru, GPS akan mengirimkan informasi perkiraan lokasi *access point*. Proses seting dan indikator aktif tidaknya GPS dapat dilihat pada gambar 7.



Gambar 7 Seting GPS pada NetStumbler

Beberapa peralatan wardriving (PCMCIA dan antena luar) pernah dipakai pada penelitian yang dilakukan Dani Adhipta (2004). Teknologi *wireless* yang ada pada tahun penelitian tersebut baru 802.11 b, sehingga PCMCIA yang digunakan hanya dapat mendeteksi *data rate* maksimal 11 MBps. Tetapi kemampuan untuk mendeteksi sinyal *access point*, selain *data rate*, masih dapat diandalkan. Sedangkan GPS pada penelitian ini adalah GPS bluetooth receiver. Penyetingan GPS dengan mendeteksi port com yang dideteksi laptop melalui bluetooth adapter eksternal, sebagai input pada *NetStumbler*. Koneksifitas GPS *bluetooth receiver* dan adapter *bluetooth* eksternal tergantung dari jarak dan halangan diantara keduanya. Sebelum melakukan *wardriving*, tidak dilakukan kalibrasi lokasi awal survei. Hanya melihat masuk tidaknya data GPS pada NetStumbler.SNR tertinggi yang terukur. Berikut ini adalah hasil *wardriving*:

Chan	Speed	Vendor	Type	Encr...	SNR	Signal+	SNR+	Latitude	Longitude
1	11 Mbps	(Fake)	AP			4	4	S7°46'28.39"	E110°22'23.10"
6	11 Mbps	D-Link	AP			11	11	S7°45'56.24"	E110°22'39.92"
1	11 Mbps		AP			2	2	S7°46'0.41"	E110°23'2.87"
11	11 Mbps	(Fake)	AP			13	13	S7°46'28.97"	E110°22'50.27"
13	2 Mbps		AP			18	18	S7°45'53.98"	E110°22'31.85"
6	11 Mbps	(Fake)	AP			10	10	S7°46'30.41"	E110°22'46.13"
6	11 Mbps	(Fake)	AP	WEP		20	20	S7°46'29.95"	E110°22'49.84"
1	11 Mbps	Sercomm	AP	WEP		13	13	S7°46'28.39"	E110°22'23.10"
6	11 Mbps	(Fake)	AP	WEP		21	21	S7°46'2.83"	E110°22'28.47"
11	11 Mbps	(User-defined)	Peer			19	19	S7°45'53.10"	E110°22'34.66"
11	11 Mbps	(Fake)	AP			26	26	S7°46'5.12"	E110°22'44.27"
9	11 Mbps	AboCom	AP	WEP		26	26	S7°46'29.92"	E110°22'22.46"
7	11 Mbps	SMC	AP	WEP		29	29	S7°46'30.26"	E110°22'22.34"
10	11 Mbps	(Fake)	AP			44	44	S7°46'4.55"	E110°22'42.22"
6	11 Mbps	(Fake)	AP			5	5	S7°46'3.17"	E110°23'10.57"
6	11 Mbps	Sonic	AP			20	20	S7°46'6.26"	E110°23'4.72"
11	11 Mbps	(Fake)	AP			26	26	S7°46'5.81"	E110°23'15.11"
8	11 Mbps	(Fake)	AP			9	9	S7°46'10.22"	E110°22'37.25"
6	11 Mbps	(Fake)	AP			7	7	S7°46'9.10"	E110°22'37.69"
6	11 Mbps	(Fake)	AP			30	30	S7°46'4.62"	E110°22'36.17"
6	11 Mbps	(Fake)	AP			23	23	S7°46'4.73"	E110°22'36.49"
7	11 Mbps	(Fake)	AP			15	15	S7°46'16.49"	E110°22'44.27"
6	11 Mbps	(Fake)	AP			33	33	S7°46'16.94"	E110°22'45.86"
10	11 Mbps	(Fake)	AP			19	19	S7°46'12.61"	E110°22'42.85"
3	11 Mbps	(Fake)	AP			13	13	S7°46'16.27"	E110°22'43.36"
9	11 Mbps	Linksys	AP			16	16	S7°46'16.55"	E110°22'44.17"
2	11 Mbps	(Fake)	AP			3	3	S7°46'16.59"	E110°22'44.33"
3	11 Mbps	(Fake)	AP			7	7	S7°46'16.91"	E110°22'45.72"
8	11 Mbps	(Fake)	AP			13	13	S7°46'13.85"	E110°22'42.58"
7	11 Mbps	(Fake)	AP			33	33	S7°46'18.11"	E110°22'49.66"
6	11 Mbps	SMC	AP			12	12	S7°46'16.78"	E110°22'45.35"
6	11 Mbps	SMC	AP			32	32	S7°46'16.38"	E110°22'43.68"
6	11 Mbps	SMC	AP			6	6	S7°46'16.77"	E110°22'41.92"
5	11 Mbps	SMC	AP			16	16	S7°46'19.26"	E110°22'41.12"
6	11 Mbps	SMC	AP			16	16	S7°46'16.79"	E110°22'45.01"
6	11 Mbps	SMC	AP			20	20	S7°46'20.62"	E110°22'42.75"

Tabel 1 Hasil scanning Wardriving

Total jaringan *wireless* yang terdeteksi di lingkungan kampus yaitu 274 jaringan dengan rincian 257 jenis topologi infrastruktur *access point* (2 diantaranya *hidden network*) dan 17 topologi adhoc.

Kemudian hasil wardriving di petakan melalui layanan yang disediakan di *http://www.gpsvisualizer.com/map?output_wifi* dengan memasukkan data NetStumbler ekstensi ns1. Output pemetaan dapat dipilih berbagai format seperti PNG, SVG, JPEG, Google Maps HTML, Google Earth KML, dan Yahoo! Flash. Untuk pemetaan ini, output yang dipilih Google Maps.

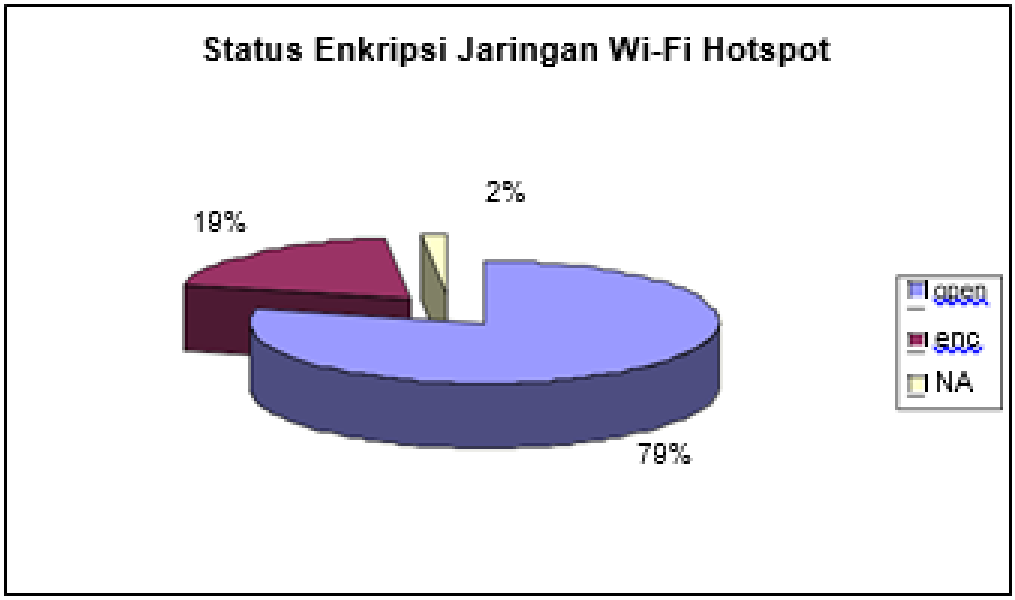
Wawancara dengan admin jaringan

Pengambilan data dengan wawancara dilakukan mulai tanggal 24 Oktober sampai 22 Desember 2023. Wawancara dilakukan dengan menyebarkan kuesioner yang berisi informasi SSID, channel, lokasi *access point* (AP), jangkauan jaringan *wireless* (baik dalam meter maupun daerah yang terjangkau) dan merek AP yang harus diisi oleh administrator jaringan. *Access point* ini di data baik dalam keadaan up, down, sedang dalam perbaikan, maupun rencana akan up. Penyusunan kuesioner berdasarkan informasi yang dibutuhkan dalam penelitian dan beberapa yang terdapat pada data *access point* dari UPT TIK.

Informasi enkripsi atau keamanan jaringan *wireless* diperoleh melalui NetStumbler, yaitu menggunakan password (WEP atau WPA) atau tidak. Dalam NetStumbler, keterangan jaringan *wireless* terenkripsi dapat diketahui dengan lambang kunci gembok pada ikon lingkaran di sebelah kiri SSID (seperti terlihat pada gambar 5). Jika tidak ada, jaringan *wireless* tersebut tidak terenkripsi. Ikon lingkaran ini digunakan sebagai informasi enkripsi pada tabel *access point*. Data data rate atau diperoleh dari informasi bandwidth pada NetStumbler.

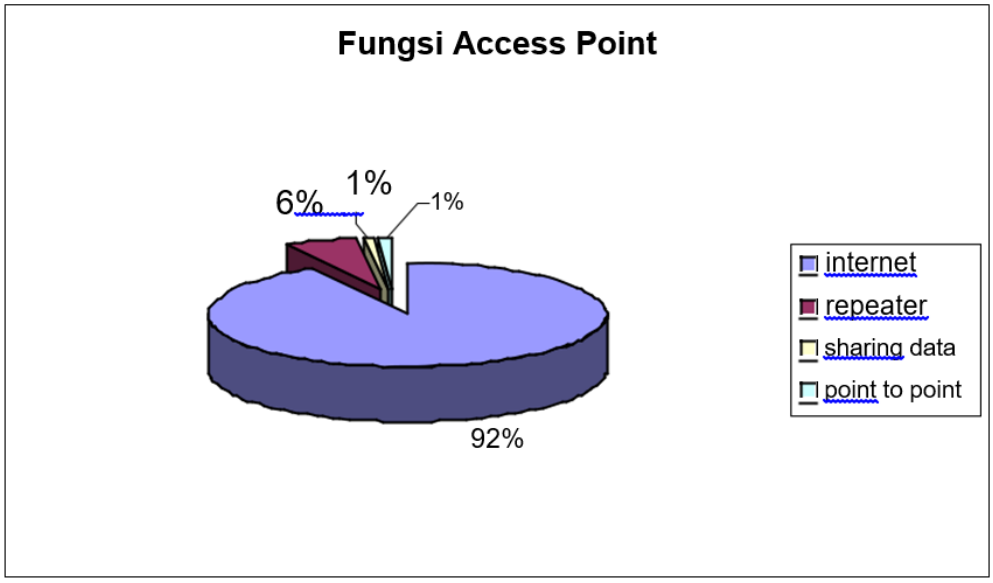
Keterangan untuk menginformasikan keadaan (off maupun rencana pemasangan), fungsi khusus *access point* selain untuk mengakses internet (seperti sharing data dan komunikasi antar gedung), dan keterangan lain. Hasil data wawancara dapat dilihat pada lampiran.

Hasil data wawancara diperoleh 196 *access point*. Berikut ini adalah rangkuman statistik penggunaan *Hardware access point*, status enkripsi jaringan dan penggunaan *Channel access point*. Keterangan N/A yang terdapat pada ketiga statistik berarti data untuk masing-masing statistik tidak terdata.



Gambar 8 Status Enkripsi Jaringan Wi-Fi Hotspot

Sebanyak 74 persen jaringan wi-fi *access point* tersebar pada beberapa jurusan, gedung administratif dan perpustakaan unit 1 belum terenkripsi. Status *open network* ini dalam keadaan tanpa autentikasi (langsung dapat mengakses internet) maupun membutuhkan autentikasi *user*.



Fungsi *access point pada* gambar 4.8 menunjukkan fungsi *access point* yang digunakan di lingkungan Fakultas/Jurusan, KPTU Pusat POLNEP dan perpustakaan unit 1. Sebanyak 92 % *access point* digunakan untuk akses internet. Fungsi *access point* sebagai *repeater* digunakan untuk memperluas jangkauan *signal access point*.

Kebijakan pengelola jaringan dalam membatasi jumlah *access point* untuk akses internet mempengaruhi penggunaan *access point*. Sehingga penambahan *access point* selain yang disediakan oleh pengelola jaringan tersebut hanya berfungsi sebagai *sharing data*.

Access point untuk komunikasi antar gedung (*point to point)* juga digunakan selain untuk akses internet. Pengaturan *point to point* ini dengan mendaftarkan MAC *address* dari kedua *access point* yang berkomunikasi, baik yang berfungsi sebagai pemancar maupun penerima.

Proses pengambilan data *access point* di POLNEP dengan wardriving bertujuan me-scanning jaringan *wireless* hotspot dan mendata jangkauan *access point* melalui signal strength yang diterima software NetStumbler. Kemampuan menangkap signal strength ini dipengaruhi dengan performa PCMCIA card yang digunakan. PCMCIA card masih bertipe b, sehingga hanya dapat mendeteksi output data rate maksimal dari *access point* 11 MBps. Tetapi, untuk mengukur jangkauan tergantung dari signal dan noise level PCMCIA card. Spesifikasi PCMCIA yang digunakan adalah signal level=-68 dBm noise level=-122 dBm yang berarti PCMCIA dapat mendeteksi sinyal *access point* dengan signal level paling rendah -68 dBm dan noise level -122dBm.

NetStumbler menangkap beacons saat wardriving dengan kekuatan spesifikasi PCMCIA card dan penguatan 7 dBi antena *wireless* LAN. Lokasi saat NetStumbler menangkap beacons dicatat oleh GPS receiver. GPS receiver membutuhkan keadaan langit yang clear view dan tidak bekerja di dalam ruangan atau under cover. wardriving database hanya terdiri dari perkiraan posisi beacons, karena posisi beacon di peroleh dari observasi yang diberikan oleh GPS. (LaMarca et al, 2005). Sehingga informasi *access point* berupa lokasi hanya berupa perkiraan GPS saat berkendara melewati daerah yang terdapat beacons di udara. Data signal strength yang diperoleh berupa Received Signal Strength Indicator (RSSI) yang dalam NetStumbler hanya menampilkan informasi signal strength, tidak dengan informasi noise. Tipe informasi ini berhubungan dengan tipe device yang digunakan untuk men-scanning yaitu NDIS 5.1

Pemetaan dari hasil wardriving dilakukan dengan me-upload file ns1 ke http://www.gpsvisualizer.com/map?output_wifi. Dengan memilih output dalam Google Maps (seperti penjelasan di bab 4.1), diperoleh lingkaran-lingkaran di latitude– longitude yang dicatat oleh GPS. Ukuran lingkaran – lingkaran ini sesuai dengan besar – kecil signal strength dari masing-masing SSID. Seting ukuran lingkaran memakai seting default, yaitu 0 – 12 pixel. Pemakaian warna untuk jaringan Wi-Fi.

access point menunjukkan status enkripsi jaringan atau status WEP. Warna hijau untuk open (tidak memakai enkripsi jaringan) dan warna merah untuk jaringan yang memakai WEP atau enkripsi.

Kalibrasi posisi data *access point* sebenarnya diperoleh dengan memadukan hasil wardriving dengan hasil wawancara dengan admin tentang posisi riil *access point* yang dipetakan secara manual di foto udara dan data spasial POLNEP. Posisi “riil” ini diperoleh dengan orientasi keruangan dari admin pada foto udara dan data spasial yang menampilkan foto lingkungan POLNEP tampak dari atas.

4. KESIMPULAN DAN SARAN

Jaringan wi-fi *access point* di Gedung teori Elektro tidak menggunakan enkripsi. Pengamanan yang dilakukan untuk *user* baru yaitu mendaftarkan MAC address dan memperoleh account untuk akses internet. Sehingga penggunaan internet via *wireless* terbatas pada civitas bersangkutan. Sebagian besar pengelola jaringan *wireless* belum menggunakan *nonoverlapping Channel* (*Channel* 1, 6 dan 11 sebanyak 7%, 32% dan 30%). Hal ini menunjukkan belum ada pengetahuan mengenai pemakaian channel. Penggunaan *nonoverlapping Channel* tidak berlaku pada *access point* yang berfungsi sebagai *repeater* internet dan komunikasi *point to point*. *Channel access point* yang digunakan dengan fungsi tersebut harus sama. Fungsi *access point* yang tersebar di

gedung Teori Elektro Polnep ada yang berperan sebagai *repeater* internet (6%), komunikasi *point to point* (1%). *Access point* yang terpasang di daerah penelitian sebagian besar bersifat tidak untuk umum. Sehingga dibutuhkan registrasi terlebih dahulu Terdapat beberapa daerah *blank spot* di daerah penelitian yang tidak terjangkau sinyal *access point*. Hal ini terjadi karena pemasangan *access point* di daerah penelitian belum merata dan *access point* yang tidak aktif setiap saat.

Secara keseluruhan belum ada koordinasi pemasangan *access point* antar pengelola di daerah penelitian dalam hal jangkauan *wireless* dan pemakaian channel. Sehingga banyak ditemukan pemakaian *Channel* yang overlap. Hasil *Site survey* di gedung Teknik Elektro meliputi jangkauan *access point*, pemakaian *Channel* dan uji konektifitas internet pada masing-masing *access point*. Ditemukan pemakaian *Channel access point* yang sama pada *access point* di lantai dua dan lantai satu. Gedung Jurusan Teknik Elektro menjadi daerah *blank spot* bagi *user* yang tidak memiliki hak akses. Sedangkan bagi *user* yang memiliki hak akses (*account proxy* dan WEP/WPA) tidak terdapat daerah *blank spot*. Performa sinyal *access point* dan koneksi internet yang baik adalah Ruang Jurusan, Lantai 1 dan Lantai 2 yang memiliki daerah jangkauan yang lebih luas baik horisontal maupun vertikal.

Hardware Ubiquiti Unifi memiliki jangkauan yang luas dan performa koneksi internet yang baik. Selama penelitian dan pengkajian saat pengambilan data, ada baiknya jika Pemetaan serta pemantauan jangkauan dan pemakaian *Channel access point* dilakukan periodik oleh pengelola internet pada jurusan. Baik yang dalam lingkungan autoritas admin maupun di lingkungan sekitar. Sehingga instalasi *access point* oleh pengelola atau pribadi dapat lebih terkendali dalam pengaturan jangkauan dan pemakaian *Channel* untuk mengurangi *interferensi*. Pengelola jaringan *wireless* sebaiknya memiliki peraturan mengenai *user* yang berhak akses dan pemasangan *access point* untuk kepentingan pribadi. Pemetaan *access point* dilakukan secara otomatisasi. Sehingga informasi *access point* di peroleh dalam keadaan *up to date*.

Pengaturan pemakaian *Channel access point* sebaiknya diubah menggunakan *Channel nonoverlap* pada semua *access point* yang sinyalnya saling *overlap* baik *access point* milik satu pengelola maupun dengan milik pengelola di sekitarnya. Agar performa jaringan *wireless* di masing-masing pengelola tidak saling merugikan seperti koneksi internet lambat. *Site survey* tidak hanya berdasarkan data *WiFi* saja. *Site survey* dengan data spektrum dapat diketahui dampak interferensi yang terjadi pada pemakaian *Channel* dan juga mendeteksi *noise* yang mengakibatkan performa sinyal menurun. Pemakaian *Channel* yang sama pada *access point* di lantai 2) sebaiknya diubah menjadi 6-1-6 dan 1-11.

DAFTAR PUSTAKA

[1]. Adhipta, D. 2004. Studi Keamanan Jaringan Komunikasi Data Nirkabel di Jogjakarta: Kajian Platform Teknis Menuju Potensi Grid Parasitik. Laporan Penelitian Tidak Terpublikasi. Yogyakarta: Jurusan Teknik Elektro POLNEP.

[2]. Barken, L., Ermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M., Koebrick, A. *Wireless* Hacking Projects for Wi-Fi Enthusiasts. 2004. Rockland, MA: Syngress Publishing, Inc.

[3]. Clincy, V., Sitaram, A., Odaibio, D., & Sogarwal, G. 2006. A Real-Time Study of 802.11b and 802.11g. IEEE [2023, July 3]

[4]. Cheng, YC., Chawathe, Y., LaMarca, A., Krumm, J., 2005. Accuracy Characterization for Metropolitan-scale Wi-Fi Localization. 3rd International Conference on Mobile Systems, Applications, and Services – Technical Paper [28 NovemberF 2023]

[5]. Flickenger, Rob. Building *Wireless* Community Networks. 2003. Sebastopol, CA: O'Reilly.

[6]. Garmin Ltd. 2007. What is GPS?. Available: http://www8.garmin.com/aboutGPS/ [4 Oktober 2023]

[7]. Geier, J. 4 Februari 2005. SNR Cutoff Recommendations. Available: http://wi-fiplanet.com/tutorials/article.php/3468771 [12 November 2007]Hills, A., Schlegel, J., & Jenkins, B.

2004. Estimating Signal Strengths in the Design of an Indoor *Wireless* Network. IEEE Transactions on *Wireless* Communications, vol.3, No.1 [2023, July 4]
[8]. Hurley, C., Puchol, M., Rogers, R., Thornton, F. 2004. WarDriving: Drive, Detect,
[9]. Defend: Guide to *Wireless* Security. Rockland, MA: Syngress Publishing.
[10]. Hyperlinktech. 2.4 GHz 7 dBi Compact Magnetic Mount Omni *Wireless* LAN Antenna Data Sheet. http://www.hyperlinktech.com/web/hg2407mgu.php [30 November 2023]
[11]. LaMarca A et al. Juni 2005. Place Lab: Device Positioning Using Radio Beacons in the Wild. Proceedings of International Conference on Pervasive Computing (Pervasive) [28 November 2007]
[12]. Milner, M. 2004. NetStumbler Version 0.4.0 Help. http://stumbler.net
[13]. Purbo, OW. 2002. Buku Pegangan *Wireless* Internet dan Hotspot. Jakarta: PT. Elex Media Komputindo.
[14]. Sundar, S. 7 April 2006. Introduction to NetStumbler and Kismet. http://csshyamsundar.wordpress.com/2006/04/07/introduction-toNetStumbler-and-kismet/ [4 September 2023]
[15]. U.S. Geological Survey (USGS). 2007, February 22. Geographic Information System. Available: http://erg.usgs.gov/isb/pubs/gis_poster/ [29 July 2023]