JustIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
DOI: 10.26418/justin.v11i1.53745
Vol. 11, No. 1, Januari 2023

Implementasi Protokol Keamanan Dan Segmentasi Jaringan Dalam Project Pembangunan WLAN Untuk PT Pan Pacific Insurance

Riyan Almakhi[a1], Ade Surya Budiman[a2], Rachmawati Darma Astuti[a3]
[a]*Program Studi Teknologi Komputer, Universitas Bina Sarana Informatika*
Jl. Kramat Raya No. 98, Jakarta Pusat, DKI Jakarta
[1]riyanalmakhi@gmail.com
[2]ade.aum@bsi.ac.id
[3]rachmawati.rcd@bsi.ac.id

Abstrak

Keamanan data dan perangkat jaringan merupakan hal esensial dalam pengembangan suatu jaringan komputer. Tidak terkecuali dalam pembuatan jaringan komputer baru, maupun pengembangan dari jaringan komputer yang telah ada. PT. Pan Pasific Insurance sebagai sebuah perusahaan yang memegang data dalam jumlah besar disertai dengan infrastruktur jaringan komputer pendukungnya, menitikberatkan aspek keamanan selain aspek performa dalam jaringan komputernya. Untuk mendapatkan fleksibilitas jaringan komputernya, perusahaan mengembangan jaringan *wireless local area network* (WLAN) seiring pemindahan lokasi kantor pusatnya. Jaringan komputer berjalan perusahaan perlu dikembangkn dengan jaringan WLAN yang tidak hanya dapat meningkatkan kinerja karyawan, namun juga harus memberikan keamanan terbaik terhadap data perusahaan. Untuk itu dalam pengembangan jaringan komputer di lokasi baru ini, penulis menerapkan penggunaan Cisco *Wireless* LAN *Controller* (WLC), Cisco *Access Point* dan menerapkan Protokol keamanan WPA+WPA2 PSK untuk SSID yang digunakan karyawan, sehingga dengan protokol tersebut pada saat karyawan hendak terhubung dengan jaringan *wireless* akan dipaksa mengetikan *password* yang sudah diatur. Selain menerapkan protokol keamanan tersebut penulis juga menerapkan protokol keamanan *Web Policy Authentication* untuk SSID yang digunakan oleh tamu. Sehinga tamu yang hendak terhubung dengan jaringan *wireless* akan di arahkan ke *web browser* untuk diminta memasukan *username* dan *password* terlebih dahulu. Serangkaian protokol keamanan tersebut, juga ditambahkan dengan segmentasi jaringan pada masing-masing SSID untuk menggunakan *network address* yang berbeda. Dengan demikian, esensi keamanan dan performa jaringan diharapkan dapat meningkat. Dari hasil pengujian yang dilakukan, didapatkan jaminan keamanan pada jaringan PT. Pan Pasific Insurance dengan berhasil mengarahkan setiap *user* yang terhubung ke jaringan sebagai bagian dari protokol keamanan yang diterapkan. Selanjutnya dengan adanya segmentasi jaringan, trafik pada *user* lebih terkendali karena *guest* mendapatkan segmentasi jaringan tersendiri, sehingga tidak mengganggu trafik jaringan *user* atau staf perusahaan dalam operasional perusahaan.

Kata kunci: Protokol Keamanan Jaringan, Segmentasi Jaringan, *Wireless* LAN *Controller* , WPA+WPA2 PSK, *Web Policy Authentication*

Implementation of Security Protocols and Network Segmentation in WLAN Development Projects for PT. Pan Pasific Insurance

Abstract

Security of data and network devices is essential in the development of a computer network, either in the creation of new computer networks or in the development of existing computer networks. PT. Pan Pacific Insurance as a company that holds large amounts of data along with its supporting computer network's infrastructure, focuses on security aspects in addition to performance aspects in its computer network. To get the flexibility of its computer network, the company developed a wireless local area network (WLAN) in line with the relocation of its head office. The Existing company's network needs to be improved with a WLAN network, so it does not only improve employee performance and provides the best security for company data. For those purposes, the authors applied the use of Cisco Wireless LAN Controller (WLC), Cisco Access Point and applied the WPA+WPA2 PSK security protocol for the SSID used by employees. Using this protocol when employees want to connect to the

network wireless, they will be forced to type the password that has been set. In addition to implementing the security protocol, the author also applies the Web Policy Authentication security protocol for the SSID used by guests. So that guests who want to connect to a wireless network will be directed to a web browser to be asked to enter a username and password first. A series of security protocols, also added with network segmentation on each SSID to use a different network address. Thus, the essence of network security and performance is expected to increase. From the results of the tests carried out, obtained security guarantees on the PT. Pan Pacific Insurance successfully directs every user connected to the network as part of the security protocol implemented. Furthermore, with network segmentation, user traffic is more controlled because guests get their network segmentation, so they don't interfere with network traffic for users or company staff in company operations..

Keywords: Network Security Protocol, Network Segmentation, *Wireless* LAN *Controller* , WPA+WPA2 PSK, *Web Policy Authentication*

I. PENDAHULUAN

A. Latar Belakang

Jaringan komputer lokal nirkabel atau Wireless Local Area Network (WLAN) dipilih sebagai solusi untuk membangun jaringan komputer yang fleksibel dan dapat dikembangkan sesuai dengan kebutuhan pengguna dan lokasi fisik jaringan. Jaringan berbasis wireless menjadi alternatif terbaik dalam membangun jaringan komputer dalam sebuah organisasi, karena fleksibilitas dan mobilitas yang tinggi[1]. Akan tetapi karena sifat media transmisi nirkabel pada WLAN yang *unguided*, maka tentunya pengetatan protokol keamanan sangat penting untuk diperhatikan[2]. Hal ini untuk mencegah masuknya *user* yang tidak berhak masuk ke dalam jaringan dan dapat berimbas pada bocornya data perusahaan serta turunnya performa jaringan komputer secara keseluruhan.

Untuk itu dalam pembangunan ataupun pengembangan jaringan komputer baru di suatu perusahaan atau institusi sangat diperlukan perhatian besar terhadap aspek keamanan pada perusahaan atau institusi tersebut. Perusahaan asuransi, PT Pan Pasific Insurance sebagai perusahaan yang memegang data nasabah dan data karyawan dalam jumlah besar, tentunya tidak dapat mengabaikan pentingnya memastikan keamanan data dan infrastruktur jaringannya.

Pemindahan kantor pusat menuju lokasi baru berimbas pada penyesuaian kembali infrastruktur keamanan jaringan mereka dengan lingkungan baru yang berada di gedung bersama (gedung perkantoran yang dipergunakan oleh banyak perusahaan/institusi). Penambahan jaringan WLAN yang ditujukan untuk menngkatkan fleksibilitas karyawan dan tamu menjadi keniscyaan yang diikuti dengan konfigurasi keamanan yang harus diperkuat (*hardening*) pula.

Selain itu, untuk memastikan *flow* atau trafik data yang lebih baik dalam jaringan komputer perusahaan, PT. Pan Pasific Insurance juga membutuhkan jaringan yang tersegmentasi atau memisahkan antara trafik jaringan karyawan dan trafik jaringan tamu perusahaan.

Setiap perusahaan dengan jaringan komputer masing-masing memiliki spesifikasi lingkungan yang berbeda pula. Hal ini demi untuk menyesuaikan dengan dinamika lingkungan dimana jaringan komputer tersebut berada. Hal ini diantaranya terkait dengan seberapa luas jaringan komputer yang akan dibangun, seberapa banyak user yang terdapat di perusahaan tersebut, kondisi infratruktur jaringan komputer yang telah ada (*existing network*) di perusahaan ataupun digedung bersama tersebut, jenis media transmisi apa yang akan digunakan dan sebagainya.

Seiring dengan pemindahan lokasi kantor pusat PT Pan Pacific Insurance, perusahaan ini telah memiliki jaringan berjalan (*existing network*), yang menggunakan media kabel (*wired*) yang terhubung ke setiap komputer pada meja karyawan sedangkan untuk koneksi tanpa kabel (*wireless*) belum tersedia. Untuk kebutuhan koneksi internet pada ruang meeting dan ruang tamu belum tersedia. Sehingga karyawan yang sedang melakukan meeting atau sedang ada kunjungan tamu yang membutuhkan koneksi internet tidak bisa terpenuhi. Tentunya hal ini menyebabkan ketidakpuasan untuk layanan TI pada kantor tersebut. Disamping itu dengan masih menggunakan satu segmen jaringan untuk keseluruhan pengguna, tentunya akan mengurangi performa dan keamanan jaringan komputer di perusahaan tersebut.

Dalam penelitian ini, penulis melakukan pengembangan jaringan untuk memastikan ketersediaan akses jaringan WLAN yang aman serta segmentasi pada jaringan, sehingga diharapkan dapat meningkatkan performa dan keamanan jaringan komputer PT. Pan Pasific Insurance di lokasi barunya. Tentunya sebelum dapat memilih konfigurasi dan skema jaringan yang tepat, perlu dilakukan observasi sistematis untuk menghasilkan dan menguji konfigurasi nyata sebelum diterapkan pada jaringan komputer PT. Pan Pasific Insurance di lokasi kantor pusatnya yang baru. Tentunya hal ini juga terkait dengan kepastian konfigurasi dan skema dari *existing network*, seperti apa kebutuhan jaringan dan seperti apa kebutuhan dari pengguna jaringan komputer di perusahaan tersebut.

B. Tinjauan Literatur

Ancaman keamanan pada jaringan komputer berbasis nirkabel sedikit banyak dipengaruhi pula oleh organisasi yang menerapkan *Bring Your Own Device* (BYOD), sehingga karyawan dan tamu yang datang ke lingkungan kerja membawa *device* mereka[3]. Komunikasi antar perangkat pada jaringan WLAN terbentuk melalui frekuensi radio, konsekuensinya adalah munculnya potensi bahaya *eavesdropping* yang lebih besar daripada yang mungkin terjadi pada jaringan kabel [4].

Kelemahan pada jaringan WLAN dapat dibagi menjadi dua jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Hal ini membuka celah keamanan pada beberapa layer dalam jaringan. Celah keamanan dalam jaringan jenis WLAN terjadi pada layer fisik, layer jaringan, layer pengguna dan layer aplikasi [5].

Cukup banyak teknik keamanan yang dapat diterapkan untuk memperkuat keamanan pada jaringan WLAN,

diantaranya adalah MAC Filtering, Hidden SSID dan WPA2 [6].

WPA2-PSK (*Pre-Shared Key*) merupakan evolusi dari protokol WPA, dimana mekanisme ini menerapkan suatu algoritma keamanan yang berbasiskan sebuah kunci keamanan berjumlah 8 sampai dengan 63 karakter, yang dipergunakan sebagai parameter, kemudian kunci keamanan yang baru akan dibuat secara acak (*randomly generated*) [7].

Selain mempergunakan WPA2-PSK, penebalan keamanan pada jaringan WLAN adalah dengan menambah komputer *server* yang digunakan sebagai *server user authentication* yang berbasis *Remote Access Dial In User Service* (RADIUS). Pengujian aplikasi *user authentication* berbasis RADIUS dilakukan dengan dua cara. Cara pertama dilakukan dengan melakukan proses pengujian *authentication* pada sisi *server* RADIUS dan cara kedua dilakukan pengujian *authentication* pada sisi *user* jaringan *wireless* melalui *captive* portal [8].

Sementara itu, serangan jenis *Dictionary Attack, Man-in-the-Middle Attack* serta permasalahan akurasi dalam transmisi data pada RADIUS Server, dapat diperbaiki dengan mode otentikasi pada EAP *authentication*[9].

Pembangunan jaringan nirkabel di PT. Pan Pasific Insurance menggunakan pendekatan siklus kerja PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize), yang rinciannya dapat dilihat pada bab Metodologi. Siklus PPDIOO dipergunakan untuk memastikan keselerasan antara kebutuhan perencanaan, pengembangan hingga optimasi jaringan pasca operasional. Metode PPDIOO sangat relevan dipergunakan untuk pengembangan jaringan skala besar, seperti pada jaringan data center[10], maupun pada jaringan skala menengah, pada lingkup sekolah [11].

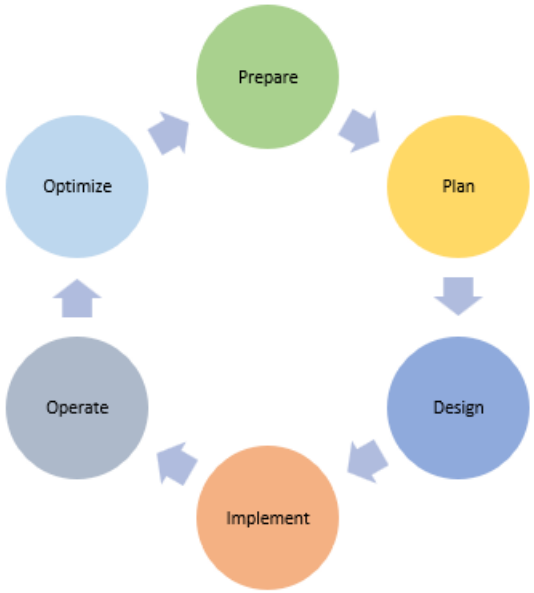
II. METODOLOGI

Secara umum, metodologi penelitian ini dibagi kedalam dua fase, yaitu fase pengumpulan data dan fase pembangunan jaringan WLAN. Pengumpulan data dilakukan dengan melakukan observasi dan wawancara terhadap *stakeholder*, dalam hal ini manajemen dan staf bidang teknologi informasi di PT. Pan Pasific Insurance.

Observasi dan wawancara ini bertujuan untuk menggali network requirement dari manajemen dan perusahaan secara umum sebagai pengguna jaringan. Penelaahan ini termasuk kepada performa dan keamanan yang diharapkan ada dari jaringan nantinya.

Fase berikutnya adalah tahap utama dalam pembangunan jaringan yang disebut sebagai bagian dari metode PPDIOO[12], yang siklusnya diperlihatkan didalam gambar 1. Gambar 1 tersebut diadaptasi dari siklus kerja pembangunan jaringan yang disingkat sebagai PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize).

Siklus PPDIOO yang pertama adalah Prepare, yang secara umum bertujuan untuk mendapatkan gambaran kebutuhan dari organisasi dan *stakeholder* perusahaan dimana jaringan komputer akan dibangun/dikembangkan. Namun, secara umum siklus awal ini penerapannya dapat berbeda-beda tergantung kepada *initial state* dari kegiatan pembangunan jaringan tersebut.



Gambar 1. Metode PPDIOO Untuk Pengembangan Jaringan Komputer di PT. Pan Pasific Insurance

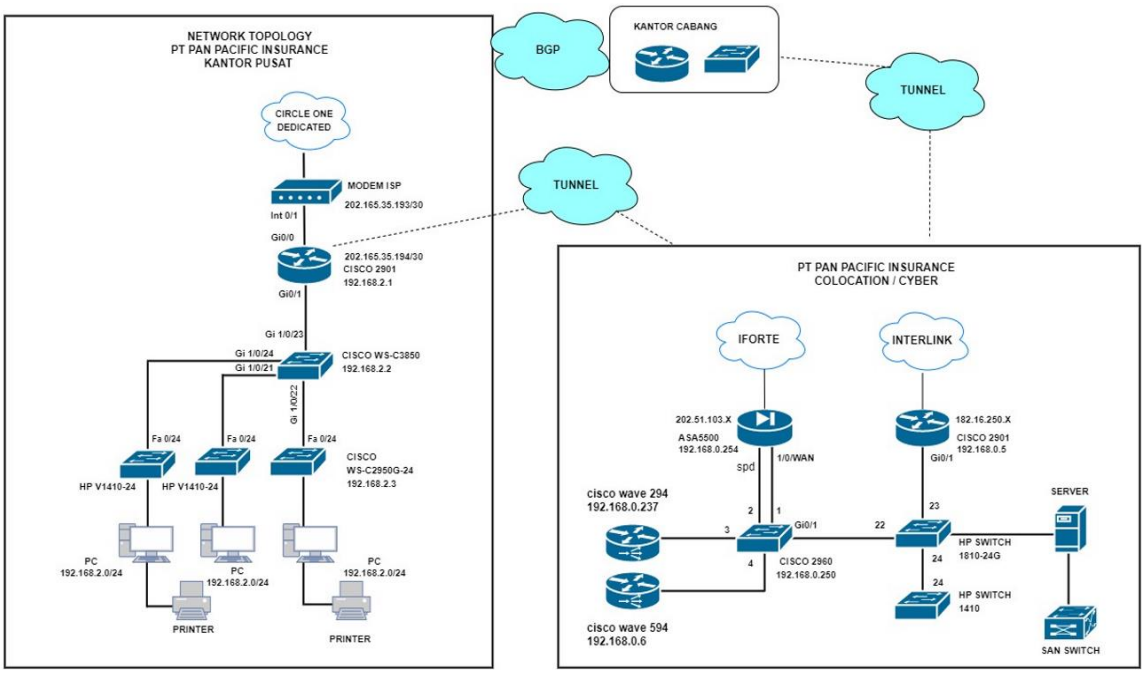
Untuk itu, dalam penelitian ini, penulis menggunakan tahap pertama penelitian berupa observasi dan wawancara tadi, guna mendapatkan gambaran kebutuhan dari pengguna jaringan. Penggunaan metode PPDIOO dipilih karena *total cost of ownership (TCO)* yang rendah, serta meningkatkan *network availability* melalui disain jaringan solid[13].

III. HASIL DAN PEMBAHASAN

A. *Analisa Jaringan Berjalan (Existing Network)*

Analisa pada suatu jaringan komputer sangatlah penting supaya kita dapat mengetahui kelebihan dan kelemahan pada sistem jaringan komputer yang sedang berjalan pada suatu perusahaan. Selain mengetahui kelebihan dan kelemahan yang ada pada sistem jaringan tersebut, juga dapat mengetahui perangkat apa saja yang digunakan dalam membuat sistem jaringan komputernya.

Kantor pusat PT. Pan Pacific Insurance yang berada di *Treasury Tower* lantai 20 kawasan SCBD Jakarta, memiliki jaringan komputer sesuai dengan yang digambarkan didalam blok jaringan yang diperlihatkan dalam gambar 2. Di jaringan tersebut terdapat sebuah modem dari ISP yang terkoneksi dengan layanan internet *dedicated* terhubung dengan router, kemudian dari *router* terhubung dengan *core switch.* Dari *core switch* terhubung dengan 3 *access switch* dan kemudian diteruskan ke PC *client* dan dari PC *client* ke *printer*. Semua *server* berada di data *center* gedung *cyber*. Sehingga semua data tersimpan pada satu tempat.



Gambar 2. Skema Existing Network PT. Pan Pasific Insurance

Secara detail, jaringan komputer pada PT. Pan Pasific Insurance memiliki spesifikasi sebagai berikut:

1. Layanan internet yang digunakan pada PT. Pan Pacific Insurance menggunakan jasa dari *Internet Service Provider* (ISP) Circle One dengan *dedicated bandwidth* 50 Mbps 1:1
2. Modem ISP digunakan untuk menghubungkan router dengan layanan internet.
3. PT. Pan Pacific Insurance menggunakan router tipe 2901 dari vendor cisco yang didukung dengan 10 Gigabit Ethernet *interfaces*, 1 *terminal line*, 1 *Virtual Private Network* (VPN) *Module*, 4 *Voice* FXO *interfaces*. Perangkat yang terhubung langsung ke router dengan media kabel yaitu *core switch* dan modem ISP. Untuk detail *interface* yang sudah terpakai di router bisa dilihat pada gambar skema jaringan.
4. Core Switch yang digunakan dari *vendor* cisco dengan tipe WS-C3850-24 dan merupakan *layer 3 switch*. Switch ini difungsikan untuk menghubungkan antara *switch access* yang terkoneksi ke PC Client.
5. *Access Switch* yang digunakan ada 2 jenis, yaitu *managed switch* dan *unmanaged switch*. *Managed switch* menggunakan perangkat dari vendor cisco dengan tipe WS-C2950G-24-EI-DC dan dua unit *unmanaged switch* yang digunakan menggunakan perangkat dari *vendor* HP dengan tipe HP-V1410-24.
6. Pada kantor pusat PT Pan Pacific Insurance, terdapat satu segmentasi network yang sedang berjalan. IP 192.168.2.0/24 digunakan untuk koneksi PC client sehinga semua komputer yang terkoneksi ke *switch access* akan mendapatkan IP 192.168.2.0/24.
7. Jaringan komputer di kantor utama PT Pan Pacific Insurance untuk komputer *client* masih mengandalkan sistem keamanan *firewall* bawaan perangkat dan anti *virus* kaspersky, sedangkan untuk keamanan *server* pada *colocation* menggunakan *firewall* cisco asa 5500 *series*.

Kebutuhan interface yang lebih banyak menjadi alasan yang mendasari penggantian *router* 2901 yang hanya

Dalam tabel 1 diperlihatkan rincian konfigurasi IP *Address* yang terdapat pada jaringan komputer PT. Pan Pasific Insurance.

TABEL I
KONFIGURASI IP ADDRESS PT. PAN PASIFIC INSURANCE

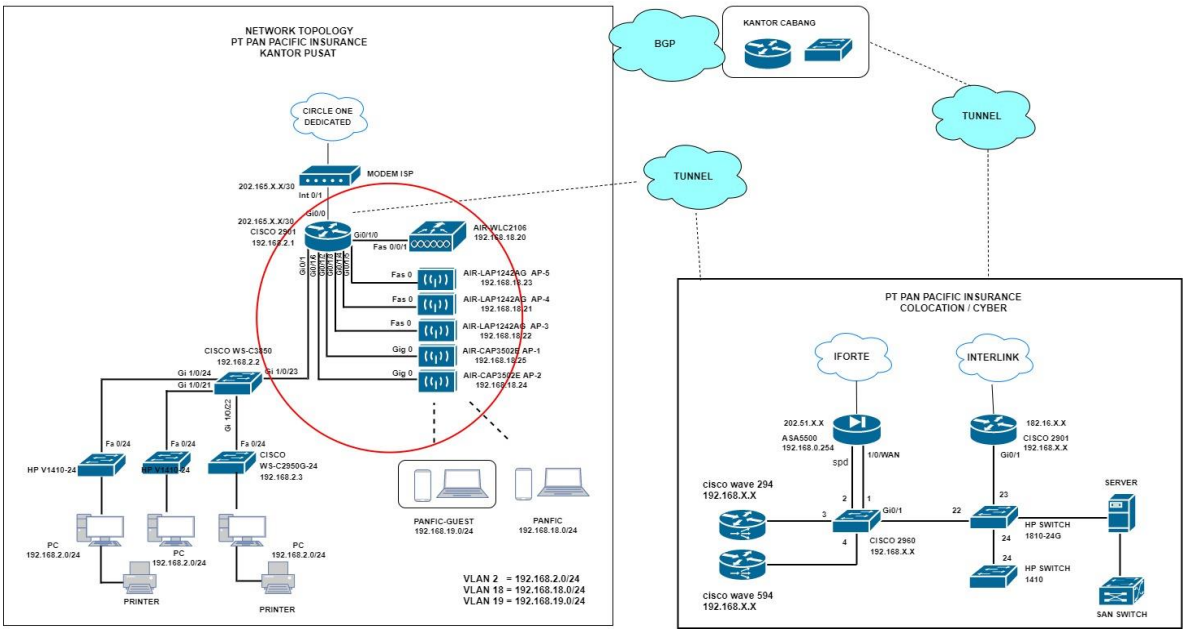
Nama Perangkat	Tipe	IP Address	Subnetmask
Router	Cisco 2901	192.168.2.1	255.255.255.0
Switch	Cisco WS-C3850-24T	192.168.2.2	255.255.255.0
Switch	Cisco WS-C2950G-24-EI-DC	192.168.2.3	255.255.255.0
Switch	HP-V1410-24 (J9663A)	-	-
Switch	HP-V1410-24 (J9663A)	-	-
PC *Client*	-	192.168.2.11-192.168.2.254	255.255.255.0

B. Skema Usulan

Pada skema jaringan usulan yang diperlihatkan pada gambar 3, penulis mengganti cisco *router* 2901, menambahkan satu buah *Wireless LAN Controller* dan lima buah *wireless Access Point*, yang digunakan sebagai media penghantar koneksi internet pada kantor utama PT Pan Pacific Insurance tanpa menggunakan media kabel. *Wireless LAN Controller* berfungsi untuk mengatur lima buah *Access Point* yang ada dan untuk mengatur konfigurasi SSID beserta *authentication*nya. Sedangkan *Access Point* berfungsi untuk membroadcast SSID yang dibuat pada *controller*.

memiliki 2 buah *Interface GigabitEthernet* dengan *router* 2901 yang memiliki 10 buah *Interface GigabitEthernet*,

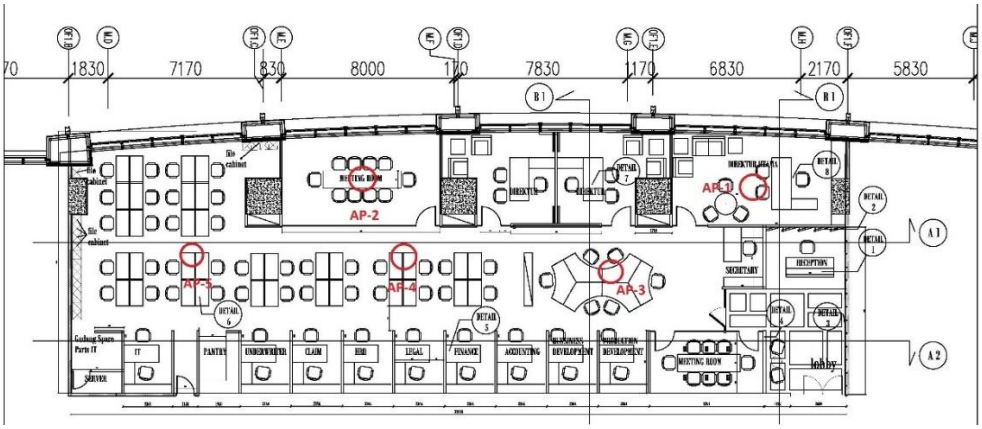
tujuan perubahan perangkat ini karena perangkat penggantinya memiliki 8 port tambahan yang mendukung PoE sehingga dapat digunakan sebagai power untuk menghidupkan *access point* dan juga menghemat biaya. Selain mengganti *router*, juga melakukan penambahan perangkat *wireless* berupa 1 buah *Wireless Lan Controller* (WLC) dan 5 buah *Wireless Access Point*.



Gambar 3. Skema Jaringan Usulan di PT. Pan Pasific Insurance

Wireless LAN Controller merupakan perangkat untuk mengelola suatu *Lightwieght Access Point* (LAP). LAP merupakan *Access Poi*nt yang didesain *stand-alone* alias membutuhkan sebuah *controller* untuk mengkonfigurasinya. LAP akan mengunduh konfigurasi dari WLC seperti SSID, jenis autentikasi, VLAN-ID, dll.

Penggunaan kabel UTP sebagai pendukung bagi jaringan *wireless* juga menjadi perhatian penulis, hal ini karena banyak organisasi masih mempergunakan kabel UTP sebagai media transmisi yang dipergunakan sebagai penghubung antar Access Point[14]. *Wireless Access Point* ditempatkan pada area yang sudah ditentukan sebelumnya untuk memenuhi kebutuhan koneksi *wireless.* SSID yang di buat sebanyak 2 buah yaitu SSID untuk karyawan dengan nama PANFIC dan SSID untuk tamu dengan nama PANFIC-GUEST. Untuk masing masing SSID menggunakan segmentasi IP *Address* yang berbeda. Sehingga disini penulis juga menambahkan 2 buah VLAN baru yang dikonfigurasikan pada *router*. VLAN 18 dengan IP 192.168.18.0/24 digunakan untuk *user* yang terkoneksi ke SSID PANFIC dan VLAN 19 dengan IP 192.168.19.0/24 digunakan untuk tamu. Sementara itu untuk koneksi LAN masih menggunakan IP sebelumnya yaitu IP 192.168.2.0/24 untuk VLAN 1. Semua pembagian IP dilakukan secara otomatis (DHCP) untuk konfigurasi dilakukan pada *router* cisco 2901. Pada gambar 4, diperlihatkan skema atau *lay out* fisik penempatan jaringan WLAN di lokasi kantor PT. Pan Pasific Insurance yang baru.



Gambar 4. *Layout* Pengembangan Jaringan LAN dan WLAN di PT. Pan Pasific Insurance

Motode *authentication* yang digunakan untuk SSID PANFIC menggunakan protokol keamanan WPA+WPA2 *Authentication* PSK sehingga jika ada *user* yang akan terkoneksi ke SSID tersebut akan diminta untuk memasukan *password* terlebih dahulu sebelum bisa menggunakan layanan. Sementara untuk SSID PANFIC-GUEST menggunakan protokol keamanan *Web Policy Authentication*. *Web Policy Authentication* merupakan otentikasi web (WebAuth) yang menjadi keamanan Layer 3[15]. Hal ini memberikan fitur keamanan yang ramah kepada pengguna dan berfungsi di semua perangkat yang menjalankan browser. WebAuth juga dapat digabungkan dengan *key security* yang dibagikan sebelumnya (PSK) Meskipun kombinasi WebAuth dan PSK mengurangi porsi ramah pengguna secara signifikan dan tidak sering digunakan, namun tetap memiliki keuntungan untuk mengenkripsi lalu lintas di sisi *client*. WebAuth adalah metode otentikasi tanpa enkripsi. Dengan protokol keamanan ini jika ada tamu yang akan terkoneksi ke SSID tersebut akan otomatis diarahkan ke *web browser* untuk diminta memasukan *username* dan *password*. Untuk *username* dan *password* ini nantinya akan ada pesan pada halaman *browser* untuk meminta akses kepada *receptionist*.

C. Konfigurasi dan Pengujian

Untuk konfigurasi IP *address* dan NAT pada *router*, NAT berfungsi untuk mentranslasikan IP *privat* ke IP *public* sehingga jaringan local bisa terkoneksi dengan internet. Dalam kasus ini, *interface GigabitEthernet*0/0 merupakan *interface* yang terkoneksi ke internet dan *interface GigabitEthernet*0/1 merupakan *interface* yang terkoneksi ke *switch* pada jaringan lokal.

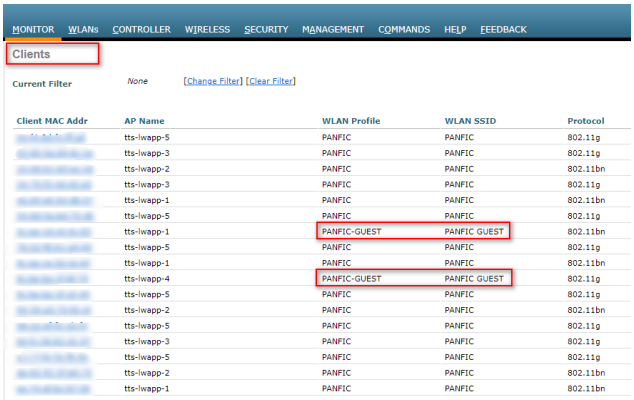
Konfigurasi *trunking* pada *interface GigabitEthernet* 0/1/0 dan *access vlan 18* pada *interface GigabitEtherne* 0/1/1 – 0/1/7, *interface* tersebut digunakan untuk menghubungkan *router* dengan WLC dan *access point*. Tujuan melakukan konfigurasi *trunking* karena di dalam WLC terdapat 2 buah VLAN ID. Sedangkan konfigurasi *access* vlan bertujuan supaya *access point* mendapatkan IP DHCP VLAN 18. *Router* ini memiliki 8 port *GigabitEthernet* tambahan karena menambahkan 2 buah modul. Jadi total ada 10 *GigabitEthernet* pada *router* ini.

Pada *router*, dibuat konfigurasi 2 DHCP *Server* tambahan yaitu supaya *access point* bisa *register* ke WLC, untuk Karyawan menggunakan *network* (VLAN 18) dengan IP 192.168.18.0/24 dan untuk tamu menggunakan *network* (VLAN 19) dengan IP 192.168.19.0/24. Sedangakan untuk karyawan yang menggunakan koneksi kabel tetap mendapatkan *network* (VLAN 1) dengan IP 192.168.2.0/24.

Saat pengujian jaringan awal dengan cara melakukan koneksi ke kedua SSID yang sudah dibuat, tentunya dengan kedua SSID tersebut belum diatur keamananya. Sehingga semua orang bisa terkoneksi dengan bebas tanpa harus memasukan *password* ketika akan terkoneksi ke SSID tersebut. Hal ini sangat tidak aman sehingga harus dibuatkan keamanan untuk mengaksesnya.

Dalam pengujian jaringan akhir, penulis memastikan apa yang dibuat sudah ada dan bisa digunakan. Yang pertama adalah pastikan access point sudah terdaftar pada WLC. Berikutnya dipastikan SSID yang sudah dibuat ada pada WLC dan dengan keamanan sesuai yang direncanakan. Dari rangkaian pengujian ini, komputer berhasil terkoneksi ke SSID PANFIC GUEST serta mendapatkan IP *Address* yang sesuai dan berhasil terkoneksi ke internet.

Melalui monitoring yang dilakukan, seperti terlihat di gambar 5 menunjukkan *client* yang menggunakan koneksi jaringan *wireless* pada kantor utama PT Pan Pacific Insurance. Jika dilihat pada gambar, terdapat 2 perangkat yang terkoneksi ke SSID PANFIC GUEST, sedangkan yang terkoneksi ke SSID PANFIC jumlahnya lebih banyak.



Gambar 5. Monitoring Perangkat Yang Terhubung di WLAN PT. Pan Pasific Insurance

IV. KESIMPULAN

Implementasi perangkat jaringan sudah selesai dikerjakan dan hasilnya sesuai dengan apa yang direncanakan. Karyawan dan tamu PT Pan Pacific Insurance sekarang sudah bisa menggunakan layanan internet dengan media *wirelless* diarea manapun selama masih dalam cakupan sinyal. Sekarang terdapat 3 VLAN yang sedang berjalan. VLAN 1 untuk koneksi menggunakan kabel dengan IP 192.168.2.0/24. VLAN 18 dan 19 untuk koneksi *wireless*. IP 192.168.18.0/24 digunakan untuk SSID PANFIC dan IP 192.168.19.0/24 digunakan untuk SSID PANFIC GUEST. SSID PANFIC menggunakan protokol keamanan WPA+WPA2 *Authentication* PSK, serta SSID PANFIC GUEST menggunakan protokol keamanan *Web Policy Authentication*.

DAFTAR PUSTAKA

[1] M. Rusdan and M. Sabar, “Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication,” *JOINT (Journal of Information Technology)*, vol. 2, no. 1, pp. 17–24, 2020.

[2] A. N. Kadhim and S. B. Sadkhan, “Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends,” Jul. 2021.

[3] M. A. Abo-Soliman and M. A. Azer, “Enterprise WLAN Security Flaws: Current Attacks and relative Mitigations,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Aug. 2018, pp. 1–8. doi: 10.1145/3230833.3230836.

[4] Y. Valaboju, “A Comprehensive Overview of WLAN Security Attacks,” *International Journal of Scientific*

Research & Engineering Trends, vol. 7, no. 1, pp. 244–251, Jan. 2021.

[5] Baihaqi, Y. Yanti, and Zulfan, "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi," *Serambi Engineering*, vol. III, no. 1, pp. 248–254, 2018.

[6] Z. Akram, M. A. Saeed, and M. Daud, "Real Time Exploitation of Security Mechanisms of Residential WLAN Access Points," in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Mar. 2018, pp. 1–5. doi: 10.1109/ICOMET.2018.8346378.

[7] A. Acosta-Lopez, E. Y. Melo-Monroy, and P. A. Linares-Murcia, "Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools," *Revista Facultad de Ingeniería*, vol. 27, no. 47, pp. 71–78, Sep. 2018, doi: 10.19053/01211129.v26.n46.2017.7309.

[8] M. Rusdan and M. Sabar, "Pengembangan Jaringan Wireless Menggunakan User Authentication Berbasis Radius Dalam Industri 4.0," *INFOTECH Journal*, vol. 5, no. 1, pp. 44–52, 2019.

[9] Y. Ma and H. Ning, "Improvement of EAP Authentication Method Based on Radius Server," in *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, Oct. 2018, pp. 1324–1328. doi: 10.1109/ICCT.2018.8600077.

[10] M. Ghazian, M. T. Kurniawan, and U. Y. K. S. Hediyanto, "Analisis dan Perancangan Security System Dalam Rancangan Berdasarkan Standar EN506002-5 Dengan Metode PPDIOO Life-Cycle Approach," in *e-Proceeding of Engineering*, 2018, pp. 3140–3147.

[11] M. F. Fahlepi, C. Iswahyudi, and E. Sutanta, "Analisis dan Perancangan Jaringan Nirkabel (WLAN) Studi Kasus di Jogjakarta Montessori School Menggunakan Metodologi PPDIOO," *Jurnal JARKOM*, vol. 5, no. 2, 2017.

[12] R. Froom, Sivasubramanian, and E. Frahim, *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning for SWITCH 642-813*. Cisco Press, 2010.

[13] D. Yuliana and I. K. A. Mogi, "Computer Network Design Using PPDIOO Method With Case Study of SMA Negeri 1 Kunir," *Jurnal Elektronik Ilmu Komputer Udayana*, vol. 9, no. 2, pp. 235–240, 2020.

[14] M. F. Rahmat, E. Rohadi, I. Sirrajudin, and F. Chrissandy, "Study and Analysis of Network Topology Performance Using Wireless Distribution System Technology," *Journal of Information Technology and Computer Science*, vol. 6, no. 2, pp. 130–136, 2021, [Online]. Available: www.jitecs.ub.ac.id

[15] N. Darchis, "Web Authentication on WLAN Controller," *Cisco Systems Inc.*, 2022. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html (accessed Mar. 18, 2022).