

# ANALISIS WIRELESS LOCAL AREA NETWORK (WLAN) DAN PERANCANGAN MAC ADDRESS FILTERING MENGGUNAKAN MIKROTIK (STUDI KASUS PADA PT.GRAHA PRIMA SWARA JAKARTA)

*Kurani Mega Asteroid<sup>1</sup> Yayan Hendrian<sup>2</sup>*

**ABSTRACT** - PT. Graha Prima Swara has applied technology of WLAN in its company because of its superiority in probabilities and flexibilities to support company performances. In the computer network, ISP used is Maxindo with bandwidth 7Mbps which is connected to routerboard mikrotik 750 as center control of network. Access point which functions as base station of WLAN with security system is used WPA2-PSK. There is security slot in WPA2-PSK namely internet accessibilty for undeserved users who are still in wireless signal range and knowing the password. By applying MAC Address Filtering to mikrotik, the administrators can restrict users who are deserve to connect to the internet by registering MAC Address Client. Therefore, WLAN network at PT. Graha Prima Swara is able to work optimally, safely, and efficiently.

**INTISARI** - PT. Graha Prima Swara menerapkan teknologi WLAN (Wireless Local Area Network) pada kantornya karena keunggulannya dalam hal portabilitas dan fleksibilitas untuk mendukung kinerja perusahaan. Di dalam jaringan komputer tersebut, ISP yang digunakan adalah Maxindo dengan bandwidth 7Mbps yang terhubung pada routerboard mikrotik 750 sebagai pusat kontrol jaringan. Access point digunakan sebagai base station jaringan WLAN dengan sistem keamanan yang digunakan adalah WPA2-PSK. Terdapat celah keamanan pada WPA2-PSK yaitu selama masih berada dalam jangkauan sinyal wireless dan mengetahui passwordnya, maka orang lain yang tidak berhak dapat mengakses internet. Dengan menggunakan MAC Address filtering pada mikrotik, admin dapat membatasi user yang berhak terkoneksi dengan cara mendaftarkan MAC Address client. Sehingga jaringan WLAN pada PT.Graha Prima Swara dapat bekerja optimal, aman dan efisien.

**Keywords** : WLAN , MAC Address Filtering

<sup>1</sup>Program Studi Teknik Komputer AMIK BSI Jakarta, Jl. R.S Fatmawati No. 24, Pondok Labu, Jakarta Selatan DKI Jakarta (Telp: 021-75914760 fax:021-75313790 email: [kuranimega@gmail.com](mailto:kuranimega@gmail.com))

<sup>2</sup> Program Studi Teknik Komputer AMIK BSI Jakarta, Jl. R.S Fatmawati No. 24, Pondok Labu, Jakarta Selatan DKI Jakarta (Telp: 021-75914760 fax:021-75313790 email: [yayan.yhn@bsi.ac.id](mailto:yayan.yhn@bsi.ac.id))

## I. PENDAHULUAN

Jaringan komputer tanpa kabel yang dikenal sebagai Wireless LAN (WLAN) atau juga disebut dengan istilah Wi-Fi (Wireless Fidelity), merupakan sebuah jaringan lokal yang menggunakan teknologi gelombang radio untuk pertukaran data. Teknologi WLAN menjadi daya tarik tersendiri bagi para pengguna komputer untuk mengakses suatu jaringan komputer atau internet karena menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Pengguna yang berada dalam daerah jangkauan Wi-Fi dapat dengan mudah berpindah tempat tanpa harus terikat dengan tersedia atau tidaknya kabel untuk koneksi ke jaringan komputer. Teknologi Wi-Fi banyak diaplikasikan untuk kampus, hotel, bandara dan perkantoran. Seperti halnya pada PT.Graha Prima Swara, yang bergerak pada bidang industri musik. PT Graha Prima Swara menerapkan teknologi Wireless Local Area Network (WLAN) di perusahaannya. Hal tersebut diterapkan karena jaringan ini kompatibel di dalam suatu pekerjaan yang membutuhkan desktop, notebook, atau PDA dalam melakukan aktivitas kerja seperti mengolah data, sharing resources maupun mencari informasi penting lainnya.

Keamanan jaringan WLAN sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan WLAN harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Dari segi keamanan, jaringan WLAN dengan sistem keamanan WPA2-PSK mudah ditembus oleh user lain yang tidak mempunyai hak untuk mengakses internet diarea tersebut. Atas dasar permasalahan tersebut, penulis ingin menganalisa keamanan jaringan WLAN pada PT.Graha Prima Swara. Sehingga jaringan WLAN PT.Graha Prima Swara dapat dimanfaatkan secara optimal dan juga memiliki keamanan jaringan yang aman.

## II. KAJIAN LITERATUR

### A. Jaringan Wireless

Menurut Kustanto dan Saputro (2008:25) “Jaringan wireless adalah jaringan komputer yang menggunakan gelombang radio untuk transfer datanya”. Perangkat yang digunakan adalah access point. Access point berfungsi sebagai base

station, yaitu pusat pemancar dan penerima untuk sinyal radio. Teknologi wireless memiliki standar yang telah ditetapkan oleh Institute of Electrical and Electronic Engineers (IEEE). Standar IEEE untuk teknologi wireless menurut Madcoms (2011:2) diantaranya:

1. Standar IEEE 802.11a, merupakan standar dengan frekuensi 5Ghz dengan kecepatan 54 Mbps. Keuntungan standar 802.11a adalah kapasitas yang cukup tinggi, mencapai 12 channel dan mendukung aplikasi yang membutuhkan performa tinggi. Standar 802.11a tidak kompatibel dengan standar 802.11b/g.
2. Standar IEEE 802.11b, merupakan standar dengan frekuensi 2.4 Ghz dengan kecepatan 11 Mbps.
3. Standar IEEE 802.11g, merupakan standar dengan frekuensi 2.4 Ghz dengan kecepatan 54 Mbps.
4. Standar IEEE 802.11n, ditujukan untuk WLAN dengan kecepatan transfer 100Mbps dan bekerja pada frekuensi 2.4 Ghz.

**Tabel 1.**  
**Spesifikasi Wi-Fi**

Spek	Kecepatan (Mbps)	Frekuensi (GHz)	Kompabilitas
802.11b	11	2,4	A
802.11a	54	5	B
802.11g	54	2,4	b,g
802.11n	100	2,4	b,g,n

Sumber: Winarno dkk (2014:107)

### B. WAP (Wireless Access Point)

Access point menurut Yani (2008:126) “Adalah sebuah node yang telah dikonfigurasi untuk menghubungkan jaringan lokal dengan jaringan wireless. Access point bertindak sebagai pusat pemancar dan penerima untuk sinyal-sinyal radio WLAN”.

Access point mengeluarkan sinyal SSID (Service Set Identification) yang merupakan nama sinyal radio yang diberikan pada jaringan nirkabel. Agar dapat terhubung dengan access point, maka semua komputer yang akan terhubung harus diisikan SSID yang dikeluarkan oleh Access Point. Penamaan standar SSID menggunakan nama default, namun dapat diganti sesuai kebutuhan user.



Sumber : <http://www.tp-link.co.id/res/images/products/gallery/TL-WA701ND-02.jpg>

**Gambar 1. Wireless Access Point (WAP)**

Pada bagian depan Wireless Access point terdapat beberapa lampu LED indikator yang menunjukkan kerja dari Access Point yang sedang bekerja, yaitu:

1. Power : Apabila lampu LED menyala berarti ada daya yang masuk ke AP.
2. System : Apabila lampu LED berkedip maka AP bekerja dengan baik
3. LAN : Apabila lampu LED menyala berarti AP terhubung ke hub atau switch
4. WLAN : Apabila lampu LED berkedip berarti radio wireless aktif.

Sedangkan pada bagian belakang AP terdapat beberapa port, yaitu:

1. Port LAN : untuk menghubungkan AP dengan hub atau switch dengan menggunakan kabel UTP dan konektor RJ45.
2. Socket Power : untuk menghubungkan AP dengan adaptor
3. Tombol Reset : untuk mengembalikan konfigurasi AP ke konfigurasi default.

### C. Perangkat Lunak Jaringan

Menurut Wahana (2010:20) “Sistem operasi merupakan perangkat lunak yang bertugas mengontrol dan mengatur manajemen perangkat keras serta operasi-operasi dasar sistem”. Berikut adalah sistem operasi yang sering digunakan untuk server dan client yaitu:

1. Windows Server.  
Windows server menurut Wahana (2010:20) “Merupakan OS yang digunakan untuk komputer server. Pada jaringan Client Server, dibutuhkan sebuah PC yang digunakan sebagai server. Salah satu sistem operasi yang banyak digunakan adalah Windows Server 2008”.
2. MikroTik.  
Menurut Wahana (2010:28) “Router OS adalah sistem operasi dan perangkat lunak yang mampu membuat PC berbasis Intel atau AMD mampu melakukan fungsi Router, Bridge, Firewall,

Bandwidth management, Proxy, Hotspot dan masih banyak fungsi lainnya". MikroTik RouterOS™, merupakan sistem operasi yang didesain untuk memberikan kemudahan bagi penggunaannya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standar, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

Fasilitas pada mikrotik antara lain sebagai berikut:

- a. Protokol routing RIP, OSPF, BGP.
  - b. Statefull firewall
  - c. HotSpot for Plug-and-Play access
  - d. Remote winbox GUI admin
3. Windows 7. Menurut Abidin dan Arifin (2010:11) "Windows 7 adalah sistem operasi dari microsoft yang digunakan untuk keperluan komputer pribadi, seperti komputer dekstop, laptop, netbook, tablet PC dan media center PC". Windows 7 mulai dirilis untuk uji coba pada juli 2009, dan mulai dipasarkan secara umum pada 22 oktober 2009. Selain windows 7, versi sistem operasi lainnya dari Microsoft Windows yang banyak digunakan untuk komputer client diantaranya Windows XP, Windows Vista dan Windows 8.

#### D. Sistem Keamanan Jaringan

Menurut Gondohanindijo (2012:142) "Kelemahan jaringan wireless terletak pada kelemahan pada konfigurasi dan jenis enkripsi yang digunakan. Dengan kemudahan dalam mengkonfigurasi sebuah jaringan wireless, di tambah dengan banyaknya vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user atau password untuk administrasi wireless tersebut."

Model-model penanganan keamanan pada pemakaian jalur komunikasi yang menggunakan teknologi wireless menurut Gondohanindijo (2012:145) antara lain:

1. WEP . WEP merupakan standar keamanan dan enkripsi pertama yang digunakan pada wireless. WEP (Wired Equivalent Privacy) adalah suatu metoda pengamanan jaringan nirkabel disebut juga dengan shared key authentication. Enkripsi WEP menggunakan kunci yang dimasukkan oleh

administrator ke client maupun access point. Kunci ini harus cocok dari yang diberikan access point ke client, dengan yang dimasukkan client untuk autentikasi menuju access point. WEP terdiri dari dua tingkatan, yakni kunci 64 bit dan 128 bit. WEP memiliki berbagai kelemahan antara lain:

- a. Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
  - b. WEP menggunakan kunci yang bersifat statis
  - c. Masalah initialization vector (IV) WEP
  - d. Masalah integritas pesan Cyclic Redundancy Check (CRC-32).
2. WPA-PSK. WPA-PSK atau Wi-Fi Protected Access-Pre Shared Key. WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. WPA-PSK bisa di crack yakni dengan metode brute force attack, yaitu dengan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang digunakan wireless tersebut memang terdapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang (satu kalimat).
3. WPA2-PSK. WPA2-PSK singkatan dari Wi-Fi Protected Access 2-Pre Shared Key. WPA-PSK menggunakan protokol enkripsi yang lebih baik dibandingkan dengan WEP maupun WPA-PSK. WPA2-PSK menggunakan algoritma enkripsi AES dan otentikasi 802.1X. Sehingga menjamin keamanan data dan kontrol akses jaringan lebih baik dibandingkan WEP dan WPA-PSK. Kelebihan WPA2-PSK yaitu merupakan versi 32 baru untuk keamanan wireless dan menggunakan algoritma enkripsi lebih baik. Kekurangannya umumnya didukung oleh hardware baru (hardware keluaran 2003 atau yang lebih baru). Untuk cara pengaturannya ada pada wireless security yang berkaitan dengan aspek keamanan jaringan pada access point. Dan disarankan untuk mengaktifkan fitur enkripsi paling optimal saat ini yaitu WPA2-PSK. Gunakan password yang akan digunakan oleh para pengguna komputer yang akan login.
4. MAC Address Filtering. MAC Address Filtering merupakan metode filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti:
- a) Pencurian PC card dalam MAC filter dari suatu access point atau router.
  - b) Sniffing terhadap WLAN

Pemfilteran MAC Address merupakan pemfilteran di atas standar 802.11b untuk mengamankan jaringan. Dalam hal ini setiap MAC Address client memiliki

alamat fisik yang pasti berbeda untuk setiap cardnya. Cara kerja sistem ini yaitu mendaftarkan alamat MAC Addressnya agar mendapat otorisasi dari access point atau router saat akan berasosiasi.

### III. METODE PENELITIAN

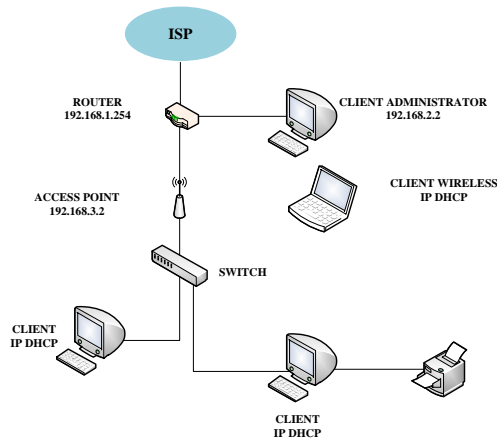
Untuk memperoleh data yang penulis butuhkan, penulis menggunakan metode penelitian sebagai berikut:

1. Observasi  
Penulis mengumpulkan data yang diperoleh dengan cara melakukan riset di PT.Graha Prima Swara selama satu bulan.
2. Wawancara  
Penulis melakukan wawancara dengan Bapak Ryan Azwin Harza, selaku pembimbing di PT.Graha Prima Swara Jakarta secara langsung untuk memperoleh informasi secara jelas dan detail.
3. Studi Kepustakaan  
Penulis melakukan studi kepustakaan yaitu dengan mengumpulkan data-data teoritis dan mempelajari buku-buku atau literatur dan artikel jurnal melalui internet yang dapat digunakan sebagai landasan teori untuk menunjang penelitian ini.

- sebanyak 7Mbps. Bandwidth tersebut dibagi lagi, 2 Mbps untuk client administrator, dan 5 Mbps sisanya di alokasikan untuk client yang terhubung melalui access point dan switch.
- b) Port 2 pada router terhubung dengan sebuah PC client. PC ini digunakan sebagai administrator jaringan komputer pada PT.Graha Prima Swara.
  - c) Port 3 pada router terhubung dengan wireless access point TL-WR841HP untuk membuat jaringan wireless pada kantor PT.Graha Prima Swara.
  - d) Port 4 pada router dikonfigurasi DHCP server dengan range 192.168.4.10- 192.168.4.40
  - e) Access point terhubung dengan switch D-LINK 8 PORT [DES-1008A] untuk membuat jaringan wired pada kantor PT.Graha Prima Swara.
  - f) Pada jaringan komputer di PT.Graha Prima Swara, client PC terkoneksi melalui terminal switch dengan media transmisi kabel UTP Cat 5e. Sedangkan client laptop terkoneksi melalui access point.
  - g) Terdapat 3 buah printer di PT.Graha Prima Swara, yang di setting sharing printer agar bisa digunakan bersama-sama.
  - h) Topologi yang digunakan pada PT.Graha Prima Swara adalah topologi star, IP Address yang digunakan adalah kelas C.

## IV. HASIL DAN PEMBAHASAN

### 4.1 Analisis Skema Jaringan Komputer



Gambar 2. Skema Jaringan PT.Graha Prima Swara

Dari skema jaringan diatas, dapat penulis jabarkan hasil analisisnya sebagai berikut:

- a) ISP Maxindo terhubung dengan RouterBoard Mikrotik 750 pada port 1. Router ini berfungsi mengubah IP Address public yang didapat dari Maxindo menjadi IP Lokal. Sedangkan bandwidth pada kantor PT.Graha Prima Swara yang diberikan oleh Maxindo untuk jalur data internet

Tabel 2. Daftar IP Address PT. Graha Prima Swara

No	Perangkat Keras	IP Address	Subnet
1.	Routerboard	192.168.1.254	255.255.255.0
2.	Access point	192.168.3.2	255.255.255.0
3.	Client Administrator or	192.168.2.2	255.255.255.0
4.	Client	192.168.4.10 – 192.168.4.40 (DHCP)	255.255.255.0

### 4.2 Analisis Keamanan Jaringan Komputer

Dari hasil pengamatan penulis, keamanan jaringan komputer pada PT.Graha Prima Swara menggunakan firewall yang di aplikasikan di dalam router, serta antivirus Norton yang sudah terinstal pada setiap PC dan laptop. Sedangkan keamanan access point menggunakan WPA2-PSK. User yang ingin terkoneksi harus melakukan autentikasi, dengan cara user login ke jaringan dengan cara memasukkan password. Menurut pendapat penulis, keamanan jaringan WLAN yang digunakan pada PT.Graha Prima Swara masih belum aman. Karena, selama masih dalam wilayah jangkauan sinyal wireless dan mengetahui password, maka orang lain yang

tidak berhak dapat mengakses internet pada kantor PT.Graha Prima Swara.

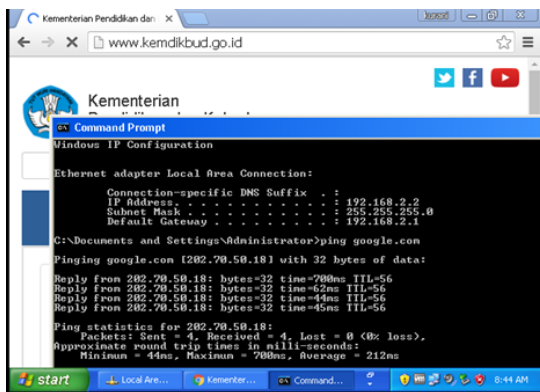
### 4.3 Permasalahan Pokok

Berdasarkan hasil analisis terhadap jaringan komputer yang ada di PT. Graha Prima Swara dapat penulis simpulkan beberapa permasalahan pokok, sebagai berikut:

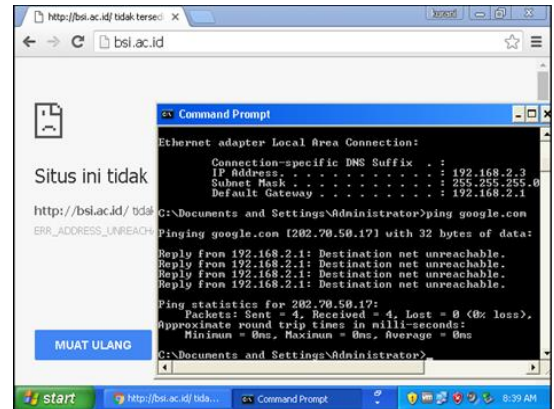
- 1) Dari segi keamanan, jaringan WLAN pada PT.Graha Prima Swara yang hanya menggunakan WPA2-PSK masih kurang aman karena mudah ditembus oleh orang lain yang tidak mempunyai hak untuk mengakses internet di area tersebut.
- 2) Dari segi infrastruktur, jaringan komputer pada PT.Graha Prima Swara kurang optimal, karena switch terhubung pada port access point dan bukan pada router yang berperan untuk pusat kontrol jaringan.

### 4.4 Pemecahan Masalah

- 1) Sebagai solusi dari permasalahan keamanan jaringan WLAN pada PT.Graha Prima Swara, penulis menyarankan untuk menggunakan fitur MAC Address filtering pada router mikrotik. Hasil uji koneksi pada client adalah sebagai berikut:



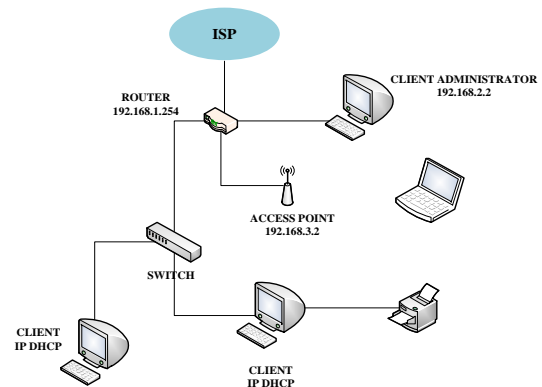
Gambar 3. Tampilan client yang terdaftar mac addressnya



Gambar 4. Tampilan client yang tidak terdaftar mac addressnya

- 2) Solusi untuk permasalahan kedua, yaitu masalah jaringan komputer yang kurang optimal, penulis mengusulkan agar switch yang semula dikoneksikan ke port access point dirubah ke port router, karena router yang berperan sebagai pusat kontrol jaringan akan membagi akses internet dari ISP ke PC admin, access point dan switch. Dengan usulan jaringan ini diharapkan jaringan komputer pada PT.Graha Prima Swara dapat bekerja lebih optimal.

### 4.5. Jaringan Usulan



Gambar 5. Skema Jaringan Usulan untuk PT.Graha Prima Swara

Dari skema jaringan usulan pada gambar 5. penulis mengubah letak switch yang awalnya terhubung dengan port access point, kini terhubung pada port router. Port 1 pada router untuk ISP, port 2 terhubung dengan PC administrator jaringan, port 3 terhubung pada access point dan port 4 terhubung pada switch. Dari segi keamanan jaringan WLAN, penulis menambahkan MAC Address filtering. Sehingga, diharapkan jaringan komputer pada PT.Graha Prima Swara dapat bekerja lebih optimal, aman dan efisien.

## V. PENUTUP

#### 4.1. Kesimpulan

Berdasarkan hasil dari analisa sistem jaringan WLAN pada PT. Graha Prima Swara, penulis menyimpulkan bahwa:

- 1) Pada PT.Graha Prima Swara memiliki koneksi internet menggunakan layanan dari ISP Maxindo dengan bandwidth 7Mbps.
- 2) RB 750 mikrotik sebagai pusat kontrol jaringan komputer pada PT.Graha Prima Swara di setting beberapa konfigurasi yaitu DHCP server, bandwidth management dan firewall.
- 3) Topologi yang digunakan adalah topologi star dan menggunakan IP Address kelas C.
- 4) Sistem keamanan wireless menggunakan WPA2-PSK. Untuk transmisi wirelessnya bertipe 802.11n dengan frekuensi radio 2,4 GHz dan kecepatan data maksimum mencapai 100 Mbps.
- 5) Kabel yang digunakan pada PT.Graha Prima Swara adalah UTP Cat 5e dengan konektor RJ-45.

#### 4.2. Saran

Hasil dari analisa ini penulis mencoba menuangkan pemikiran untuk solusi dari permasalahan yang terdapat di dalam jaringan WLAN PT.Graha Prima Swara, saran-saran yang dapat penulis berikan antara lain adalah:

- 1) Selain menggunakan WPA2-PSK, MAC Address filtering juga dapat diterapkan untuk menambah keamanan jaringan wireless pada PT.Graha Prima Swara sehingga keamanan lebih terjamin
- 2) Disarankan untuk menyambungkan port switch pada router agar jaringan komputer dapat berfungsi lebih optimal.
- 3) Selalu menjaga dan mengganti password admin secara berkala untuk keamanan jaringan wireless dari penyusup yang ingin mengakses jaringan pada PT.Graha Prima Swara.
- 4) Melakukan maintenance pada jaringan wireless secara berkala untuk menjaga serta meningkatkan kinerja jaringan tersebut.

#### REFERENSI

- [1] Arifin, Hasnul dan Zainal Abidin. 2010. Kupas Tuntas Windows 7. Yogyakarta: Penerbit MediaKom.
- [2] Gondohanindijo, Jutono. 2012. Sistem Keamanan Jaringan NIRKABEL. Jakarta: Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei.
- [3] MADCOMS. 2011. Membangun Sistem Jaringan Wireless Untuk Pemula. Yogyakarta: Penerbit Andi.
- [4] Saputro, Daniel T, Kustanto. 2008. Membangun Server Internet dengan Mikrotik OS. Yogyakarta: Gava Media..
- [5] Wahana Komputer. 2010. Membangun Warnet dan Game Center Sendiri. Yogyakarta: Penerbit Andi.
- [6] Winarno, Edy, Ali Zaki dan SmitDev Community. 2014. Membuat Jaringan Komputer di Windows dan Linux. Jakarta: PT Elex Media Komputindo.
- [7] Yani, Ahmad. 2008. Panduan Membangun Jaringan Komputer. Bandung: PT Kawan Pustaka.



Kurani Mega Asteroid, A.Md. Tahun 2016 Lulus Program Diploma III (D3) Program Studi Teknik Komputer AMIK Bina Sarana Informatika Jakarta. Saat ini bekerja sebagai Instruktur di BSI.



Yayan Hendrian, S.T.,M.Kom. Tahun 2009 Lulus Program Strata Satu (S1) Program Studi Teknik Elektro Universitas Tama Jagaraksa. Tahun 2012 Lulus Program Strata Dua (S2) Program Studi Ilmu Komputer STMIK Nusa Mandiri Jakarta. Saat ini bekerja sebagai tenaga pengajar program studi Teknik Komputer di AMIK BSI Jakarta.