Quality Of Service Filtering Dengan Metode *Filtering Mac Address* Jaringan Wireless

Aziz Setyawan Hidayat[1) *)], Ulin Nuha[2)], Yamin Nuryamin[3)], Suleman[4)]

[1)]Teknologi Komputer, Universitas Bina Sarana Informatika PSDKU Kota Tegal
[2) 3)]Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri
[4)]Teknik dan Informatika, Universitas Bina Sarana Informatika PSDKU Kota Tegal
[*)]Correspondence Author: aziz.aiz@bsi.ac.id, Jakarta, Indonesia
DOI: https://doi.org/10.37012/jtik.v7i1.502

Abstrak

Keamanan jaringan wireless saat ini menjadi sebuah hal yang penting. Jaringan wireless yang bersifat broadcast menyebabkan rentannya celah keamanan dari sistem jaringan nirkabel ini. Maka dari itu diterapkanlah keamanan ganda di dalam sistem keamanan jaringan wireless dengan menerapkan keamanan WPA/WPA2 serta dengan filtering MAC Address. Dengan menerapkan keamanan berlapis ini diharapkan mampu untuk menjaga kualitas dan layanan dari jaringan wireless pada Kantor LPSE POLRI. Nantinya setiap pengguna yang ingin terhubung kedalam jaringan haruslah melakukan pendaftaran MAC Address dari perangkat yang akan digunakan. Filtering MAC Address diharapkan mampu mengatasi kelemahan keamanan perangkat wireless. Walaupun terdapat pengguna yang mengetahui password dari keamanan jaringan wireless namun jika perangkatnya tidak didaftarkan maka perangkat tersebut tidak akan terkoneksi ke jaringan LPSE POLRI. Pengimplementasian filtering MAC Address mampu mengoptimalkan keamanan jaringan wireless dikarenakan menggunakan keamanan jaringan berlapis. Selain menggunakan keamanan verifikasi password terhadap WPA/WPA2, firewall rule MAC Address dapat membatasi hak akses berdasarkan MAC Address perangkat.

Kata kunci: Keamanan Jaringan, MAC Address Filtering, wireless

Abstract

Today's wireless network security has become an important thing. Broadcast wireless networks are vulnerable to security holes in this wireless network system. Therefore, dual security is applied in the wireless network security system by implementing WPA / WPA2 security and MAC address filtering. By implementing this layered security it is hoped that it will be able to maintain the quality and service of the wireless network at the POLRI LPSE Office. Later, every user who wants to connect to the network must register the MAC address of the device to be used. MAC Address filtering is expected to be able to overcome security weaknesses of wireless devices. Even though there are users who know the password of the wireless network security, if the device is not registered, the device will not be connected to the POLRI LPSE network. The implementation of MAC Address filtering is able to optimize wireless network security because it uses layered network security. In addition to using password verification security against WPA / WPA2, MAC Address firewall rules can limit access rights based on device MAC addresses.

Keywords: *network security, MAC Address Filtering, Wireless*

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.

Manajemen Wireless Access Point Pada Hotspot Server Menggunakan Contoller Access Point System Management. Pada penelitian yang dilakukan oleh Bakhtiar Rifai dan Aji Sudibyo tahun 2018, menyimpulkan bahwa: Untuk penerapan dan implementasi Controller Access Point System Management (CAPsMAN) dibutuhkan parameter-parameter konfigurasi terlebih dahulu pada sisi router yang akan di gunakan sebagai Controller access point system management (CAPsMAN). CAPsMAN harus memiliki kemampuan wireless controller dan dari sisi access point yang akan digunakan untuk mendistribusikan wireless yang bisa disebut dengan Controller Access Point (CAP). Penerapan Controller access point system management (CAPsMAN) ialah dengan membuat konfigurasi Bridge interface, configurations, Channels, Data paths, Security Configurations pada system management Controller Access Point (CAP).

Implementasi Controller Access Point System Manager (CAPSMAN) Dan Wireless Distribution System (WDS) Jaringan Wireless Di SMK Terpadu Al Ishlahiyah Singosari Malang. Pada penelitian yang dilakukan oleh Santi Dwi Ratnasari, Eni Farida, Nasrul Firdaus tahun 2017 menyimpulkan bahwa: Banyaknya SSID yang tersedia akan mengganggu kinerja user, dikarenakan saat berpindah tempat harus login kembali. Selain itu, kemananan jaringan di SMK Al Ishlahiyah sangatlah kurang sehingga dengan mudah dapat diterobos oleh user yang mengakses jaringan secara illegal. Dengan menggunakan sistem keamanan jaringan WPA2-PSK, dapat membantu mengatasi masalah keamanan jaringan wireless pada SMK Al Islahiyah agar tidak mudah diterobos oleh user yang tidak bertanggung jawab. Selanjutnya untuk menangani banyaknya SSID yang tersedia diterapkan fitur CAPsMAN dan WDS, dapat mempermudah user yang mendapatkan ijin akses secara legal tidak sering login kembali jika berpindah tempat. Selain itu dilakukan bandwidth management dengan menggunakan metode Queue Tree dan Per Connection Queue (PCQ) yang disertai penambahan mangle, agar bandwidth yang tersedia tidak terbuang begitu saja.

Berdasarkan penelitian yang telah dilakukan terhadap Perbandingan Kinerja Fitur Mikrotik CAPsMAN dengan Konfigurasi Tunnel dan Tanpa Menggunakan Tunnel Pada Router Mikrotik, maka dapat disimpulkan bahwa paket data yang dilewatkan pada jaringan

wireless tanpa menggunakan tunnel lebih cepat dari pada menggunakan tunnel, karena paket data yang dilewatkan pada jalur ini tidak terjadi pemerikasaan dan penambahan paket data header terhadap data yang dikirim. Sementara pada saat melakukan pengiriman paket pada jalur tunnel terjadi pemeriksaan dan penambahan paket data header disetiap protokol yang dilewatinya. Dalam melakukan pengujian download data di ambil dua jenis sampel data, yaitu data ISO dan RAR dengan rata-rata selisih waktu 3 menit 6 detik dengan rata-rata bandwidth 61,66 Kbps.

METODE

Data diperoleh dengan melakukan riset secara langsung dalam prosedur yang sistematik dan standar sehingga mendapatkan data-data yang baik dan benar dengan model pengumpulan data sebagai berikut:

1. Observasi

   Metode ini sebagai sarana pengambilan data-data terkait jaringan yang ada, dimana metode ini merupakan hasil peninjauan langsung dari objek yang diamati, yaitu LPSE Polri. Observasi dilakukan selama 3 hari, untuk melihat bagaimana jaringan itu bekerja dari ISP sampai setiap pengguna yang terdapat di kantor tersebut.

2. Wawancara

   Metode penelitian ini dilakukan dengan menanyakan secara langsung baik kepada pembimbing ataupun staf yang sedang bertugas guna mendapatkan informasi dan data serta menambah wawasan keilmuan terkait hal yang belum diketahui.

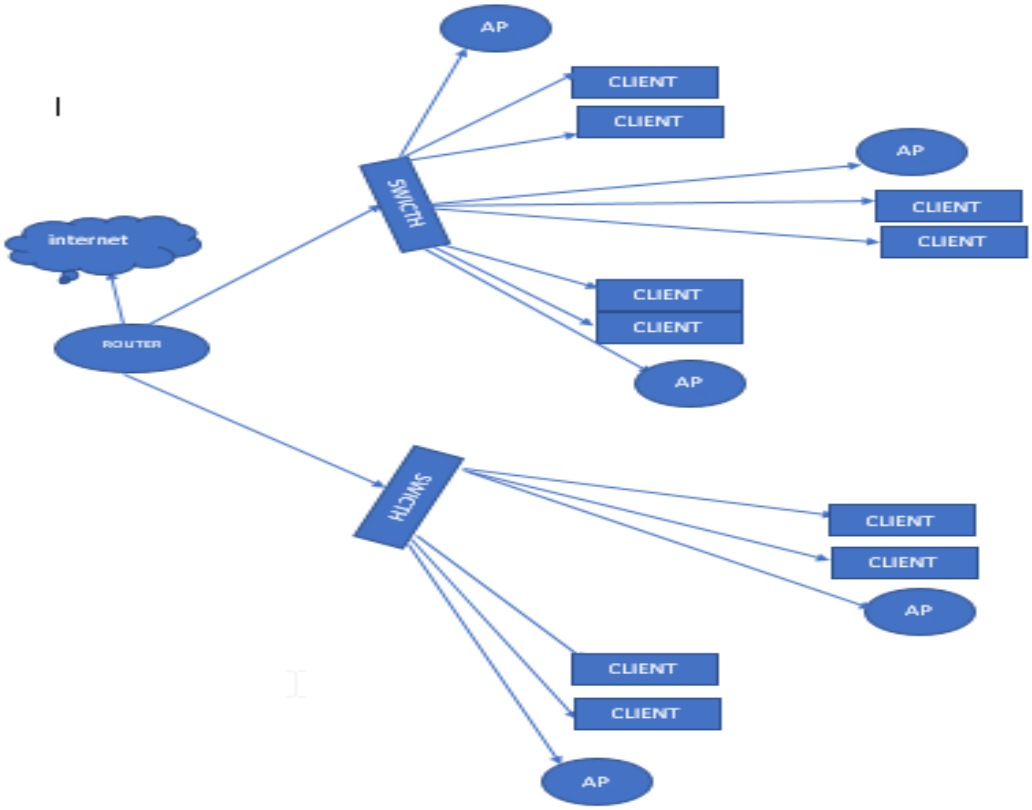
3. Studi Pustaka

   Metode ini digunakan untuk menambah informasi berupa teori atau hasil kajian dibidang ilmu yang sama dengan bertumpu pada buku-buku dan referensi-referensi yang berhubungan dengan penelitian yang dilakukan.

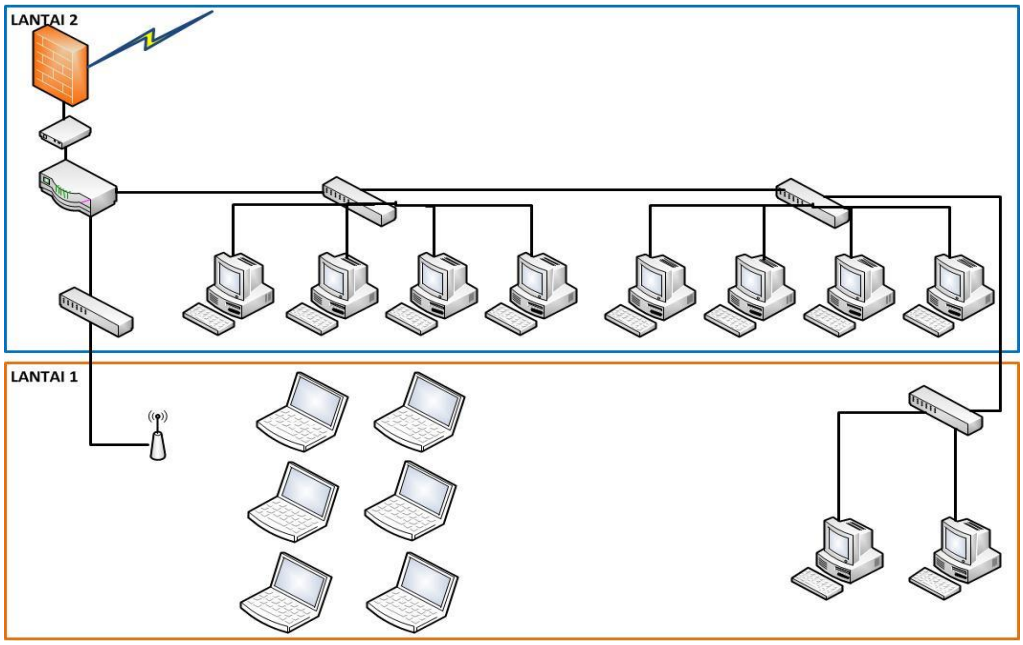
HASIL DAN PEMBAHASAN

Pada sistem jaringan komputer LPSE_Polri, secara umum menggunakan jaringan sebuah *provider* yang menyediakan jasa *internet* dengan kecepatan *bandwidth* 100Mbps, yang kemudian dialirkan ke semua bagian-bagian atau *client* dengan perantara *router*. Kemudian di hubungkan ke *switch* yang terbagi menjadi 3 *switch* dan beberapa *access point*, selain itu juga di dalam transmisi data LPSE_Polri menggunakan *Access Point* yang memberikan kemudahan bagi para *client* yang menggunakan jasa *Wireless* LAN melalui laptop atau

Mobile Phone. Cara tersebut memberikan kemudahan yang dapat meningkatkan kinerja dan hasil.



Gambar 1. Skema Jaringan



Gambar 2. Skema jaringan wireless lantai 1

Pada tabel 1 merupakan spesifikasi IP address yang digunakan pada LPSE POLRI. Terdapat 1 buah routerborad mikrotik dengan mengunakan 3 (tiga) buah ether yang

digunakan untuk membentuk sebuah layanan jaringan dan terdapat 10 client dengan pengimplementasian IP Address secara static. Serta untuk client yang terhubung kedalam jaringan wireless akan mendapatkan alokasi IP Address secara otomatis dengan menerapkan fitur DHCP Server pada Mikrotik.

Tabel 1.

Spesifikasi IP *Address*

NO	DEVICE	INTERFACE	IP ADDRESS	Subnetmask
1.	Mikrotik Routerboard	Ether 1	IP Public Static	255.255.255.248
		Ether 2	192.168.2.1/24	255.255.255.0
		Ether 3	192.168.10.1/24	255.255.255.0
2.	Komputer Client 1	NIC	192.168.2.2	255.255.255.0
3.	Komputer Client 2	NIC	192.168.2.3	255.255.255.0
4.	Komputer Client 3	NIC	192.168.2.4	255.255.255.0
5.	Komputer Client 4	NIC	192.168.2.5	255.255.255.0
6.	Komputer Client 5	NIC	192.168.2.6	255.255.255.0
7.	Komputer Client 6	NIC	192.168.2.7	255.255.255.0
8.	Komputer Client 7	NIC	192.168.2.8	255.255.255.0
9.	Komputer Client 8	NIC	192.168.2.9	255.255.255.0
10.	Komputer Client 9	NIC	192.168.2.10	255.255.255.0
11.	Komputer Client 10	NIC	192.168.2.11	255.255.255.0
12.	Access Point	NIC	DHCP Server	
13.	Laptop Client	Wireless Card	192.168.10.2 s/d 192.168.10.20	255.255.255.0

Dari hasil pengamatan, keamanan jaringan komputer pada LPSE POLRI 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 memasukkan *password*. Keamanan jaringan WLAN yang digunakan pada LPSE POLRI 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 LPSE POLRI.

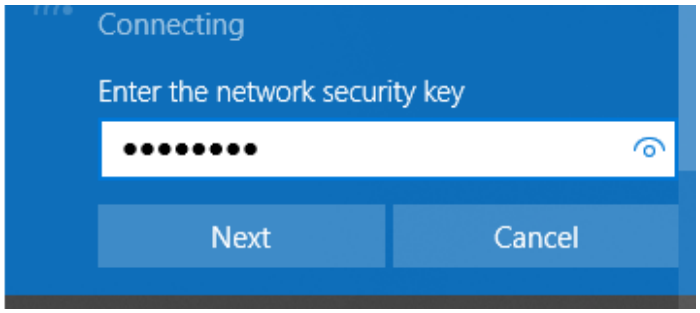
Selain menggunakan keamanan terhadap jaringan local wireless. LPSE POLRI menerapkan keamanan firewall guna melakukan pembatasan akses dari pihak luar jaringan yang akan melakukan akses kedalam jaringan local LPSE POLRI. Hal ini bersinkronisasi dengan belum maksimalnya keamanan terkait batasan pengguna pada komputer yang terhubung.

Sebagai solusi dari permasalahan keamanan jaringan WLAN pada LPSE POLRI, adalah menggunakan fitur MAC *Address filtering* pada *router* mikrotik. Solusi selanjutnya, yaitu

masalah jaringan komputer yang kurang optimal, diusulkan 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 LPSE POLRI dapat bekerja lebih optimal.

1. Uji Coba Jaringan Berjalan

Sebelum diterapkannya sistem keamanan dengan metode MAC-*address* sebagai *security* pada LPSE POLRI. Masih terdapat banyaknya *user* yang seharusnya tidak berhak untuk mengakses ke dalam sebuah jaringan computer, masih dapat mengakses ke dalam jaringan yang berjalan.

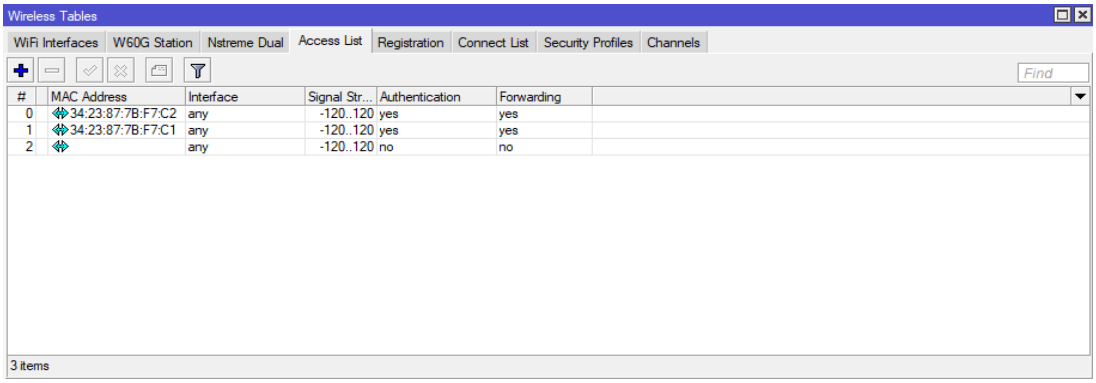


Gambar 3. Layar input Network Security key

Pada gambar 3 dapat dijelaskan mode keamanan jaringan ketika menggunakan WEP/WPA2 hanya menggunakan 1 kali verifikasi password. Hal ini dapat menyebabkan mudahnya diketahui password yang digunakan.

2. Uji Coba Jaringan Usulan

Setelah diterapkannya sistem keamanan menggunakan *Filtering MAC Address* maka setiap *client* yang akan terhubung kedalam jaringan komputer LPSE POLRI harus mendaftarkan MAC *Address* dari perangkat yang akan digunakan.



Gambar 4. Mac Address terdaftar

Tabel 2.

Hasil Manejemen Jaringan Usulan

MAC Address	WPA/WPA2	Sebelum Usulan	Sesudah Usulan
0A-00-27-00-00-02	1234567890	OK	OK
0E-00-A4-EF-00-ED	1234567890	OK	GAGAL
E6-00-4E-00-14-0E	1234567890	OK	GAGAL

Guna memastikan pengimplementasian jaringan filtering MAC Address terhadap jaringan wireless, dilakukan percobaan terhadap beberapa client yang sudah didaftarkan dan belum didaftarkan MAC Address. Terlihat pada tabel 2 client dengan MAC Address 0A-00-27-00-00-02 sudah dapat terhubung kedalam jaringan wireless dikarenakan MAC Address dari client tersbut sudah dimasukan kedalam MAC Address table routerboard mikrotik. Dan dua client lainnya dengan MAC Address 0E-00-A4-EF-00-ED dan E6-00-4E-00-14-0E walaupun mengetahui password dari jaringan wireless LPSE POLRI tidak dapat melakukan akses kedalam jaringan computer LPSE POLRI dikarenakan MAC Address dari perangkat tersebut belum dimasukan kedalam MAC Address table routerboard mikrotik.

KESIMPULAN DAN REKOMENDASI

Pengimplementasian filtering MAC Address mampu mengoptimalkan keamanan jaringan wireless dikarenakan menggunakan keamanan jaringan berlapis. Selain menggunakan keamanan verifikasi password terhadap WPA/WPA2, firewall rule MAC Address dapat membatasi hak akses berdasarkan MAC Address perangkat. Jika terdapat user yang melakukan percobaan akses kedalam jaringan komputer akan tetapi perangkat user tersebut tidak didaftarkan maka perangkat dari user tersebut tidak akan terkoneksi kedalam jaringan internet.

REFERENSI

Khosrow-Pour, D.B.A., Mehdi. "Dictionary of Information Science and Technology (2nd Edition)." 1-1010 (2013), accessed May 08, 2018. doi:10.4018/978-1-4666-2624-9

Krishan, R. (2016). Performance Enhancement Of IEEE 802.11 Wireless Local Area Network (WLAN), 1–25.

Muchamad, Arifin. Triono, R. A. (2013). Rekayasa dan Manajemen Jaringan WAN SMK Alhikmah Tanon. *Ijns*, *2*, 38–45.

Nuryanto, L. E. (2015). Konsep Subnetting IP Address Untuk Efisiensi Internet, *11*(1), 68–73.

Rahmadani, M. A., Rizal, M. F., Gunamawan, T., Terapan, F. I., Telkom, U., & Wireless, H. (2017). Implementasi Hacking Wireless Dengan Kali Linux Menggunakan Kali Nethunter Wireless Hacking Implementation Using Kali Linux Kali Nethunter, *3*(3), 1767–1774.

Ratnasari, S. D., Farida, E., & Firdaus, N. (2017). Implementasi Controller Access Point System Manager (CAPSMAN) Dan Wireless Distribution System (WDS) Jaringan Wireless Di SMK Terpadu Al Ishlahiyah Singosari Malang, (September), 624–635.

Rifai, B., & Sudibyo, A. (2018). Manajemen Wireless Access Point Pada Hotspot Server Menggunakan Controller Access Point System Management, *14*(1), 111–116.

Samsumar, L. D., Gunawan, K., Program, D., Manajemen, S., Program, D., & Komputerisasi, S. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (WIRELESS LAN); *Studi Ilmiah Teknologi Informasi Terapan*, *IV*(1), 73–82.

Sarkar, N. I. (2013). Enhancing Teaching and Learning Wi-Fi Networking using Limited Resources to Undergraduates, *8*(December), 1–18.

Warman, I., & Nofrizal. (2016). Analisa Perbandingan Kinerja Fitur Mikrotik CAPSMAN Dengan Konfigurasi Tunnel dan Tanpa Menggunakan Tunnel pada Router Mikrotik RB951-2N. *Vol. 4 No. 2 Oktober 2016*, *4*(2), 96–105.