EXPERT

Jurnal Sistem Informasi

ISSN : 2088-5555

Write To Be Experts

ISSN 2088-5555

Expert

Jurnal Manajemen Sistem Informasi Dan Teknologi

Volume 05, Nomor 02, Desember 2015

Fakultas Ilmu Komputer
Universitas Bandar Lampung

JMSIT	Volume 05	Nomor 02	Lampung Desember 2015	ISSN 2088-5555

TIM PENYUNTING

Alamat Penerbit/Redaksi:
Pusat Studi Teknologi Informasi
Fakultas Ilmu Komputer
Universitas Bandar Lampung
Gedung Business Center Lt.2
Jl,Zainal Abidin Pagar Alam No.26
Bandar Lampung
Telp.0721 – 774626
Email: Journal.expert@ubl.ac.id

MENGAMANKAN WIRELESS DENGAN MENGGUNAKAN *TWO FACTOR, PASSWORD* DAN *MAC ADDRESS FILTERING*

Didi Susianto[#1], Iis Yulianti[*2]

*[#1*2]Laboratorium Jaringan Komputer*
Akademi Manajemen Informatika dan Komputer
Dian Cipta Cendikia Bandar Lampung

Abstrak

Di era globalisasi sekarang penggunaan internet semakin berkembang pesat, dapat kita lihat bahwa hampir di seluruh belahan bumi ini sudah terkoneksi internet. Wireless merupakan jaringan tanpa kabel (nirkabel), yang mempunyai banyak keuntungan dibandingkan dengan menggunakan media kabel. Banyak organisasi dan perusahaan menyediakan layanan hotspot untuk anggota atau karyawan tetapi karena sistem keamanan masih menggunakan password WPA sehingga banyak orang walaupun bukan anggota atau karyawan menggunakan layanan hotspot. Tentunya hal ini sangat merugikan pihak organisasi maupun perusahaan. Dalam penelitian ini akan menggunakan metode The Security Policy Development Life Cycle (SPDLC). (Goldman, James E, and Rawles, Philip T) yang memiliki enam tahapan, yaitu identifikasi, analisis, perancangan, implementasi, audit, dan evakuasi.Dengan menggunakan two factor ini memiliki beberapa kelebihan dibandingkan dengan menggunakan keamanan pada WPA-nya saja, karena dengan menggunakan dua otentikasi ini jika ada seseorang yang ingin mengakses ke hotspot harus memiliki password WPA-PSK dan mendaftarkan Mac Address perangkatnya ke Administrator.

Kata Kunci *: Wireless, Hotspot, Password, Two Factor*

1. Latar Belakang

Dalam era globalisasi sekarang penggunaan internet semakin berkembang pesat, dapat kita lihat bahwa hampir di seluruh belahan bumi ini sudah terkoneksi internet. Dahulu untuk melakukan koneksi ke internet hampir semua orang menggunakan media kabel, tetapi sekarang untuk koneksi ke internet sudah bisa menggunakan *wireless*. *Wireless* merupakan jaringan tanpa kabel (nirkabel), yang mempunyai banyak keuntungan dibandingkan dengan menggunakan media kabel (LAN). Keuntungan diantaranya yaitu *user* bisa melakukan koneksi internet kapan saja dan dimana saja asal masih berada dalam ruang lingkup *hotspot*, selain itu dalam segi biaya pembangunan, *wireless* jauh lebih murah bila dibandingkan dengan kabel. Walaupun demikian, *wireless* memiliki lebih banyak kelemahan dibandingkan dengan kabel, khususnya dari segi keamanan.

Saat ini perkembangan teknologi *wireless* sangat signifikan sejalan dengan kebutuhan sistem informasi yang *mobile*. Banyak penyedia jasa *wireless* seperti *hotspot* komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan *wireless* pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut. Hal ini membuat para *hacker* menjadi tertarik untuk mengexplore keamampuannya untuk melakukan berbagai aktifitas yang ilegal dengan menggunakan *wifi* yang tersedia.

Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan *wireless* cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi *wireless* default bawaan vendor. Sering sekali ditemukan wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi yang tidak terenkripsi, dan bahkan tanpa user/password untuk administrasi wireless tersebut.

Banyak organisasi dan perusahaan menyediakan layanan *hotspot* untuk anggota atau karyawan tetapi karena sistem keamanan masih menggunakan *password* WPA sehingga banyak orang walaupun bukan anggota atau karyawan menggunakan layanan *hotspot*. Tentunya hal ini sangat merugikan pihak organisasi maupun perusahaan karena harus berbagi koneksi internet yang sama dengan pengguna lain yang tidak punya kewenangan.

Berdasarkan penjelasan di atas, sehingga dipandang perlu mencari alternatif untuk meningkatkan keamanan jaringa, salah satunya dengan menggunakan cara *two factor, password dan filtering mac address*, Mac address filtering merupakan metode filtering untuk membatasi hak akses dari MAC Address yang bersangkutan.

2. Tujuan

Pada penelitian ini akan dilakukan studi dan implementasi yang bertujuan untuk mengatur

keamanan wireless menggunakan keamanan pada WPA-PSK dan *Mac Address filtering*.

3. Landasan Teori

a. Pengertian Wireless

Hotspot (*Wi-Fi*) adalah satu standar *Wireless Netwoking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan. [Priyo Utomo, 2012: 1].

Wifi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat *Wireless Local Area Network* (*WLAN*). [Jubilee Interprise: 2012; 27].

Wifi adalah singkatan dari *Wireles Fidelity*, yaitu seperangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (*Wireless Local Area Network-WLAN*). yang didasari pada spesifikasi IEEE 802.11. [Zainal Arifin ; 2008; 7].

Ditinjau secara umum Wifi merupakan singkatan dari *Wireless Fidelity*, yang memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (*Wireless Local Area Networks* - WLAN) yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.16 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya.

b. Standar Wireless

Teknologi wifi memiliki standar yang ditetapkan oleh sebuah instusi internasional yang bernama institute of electrical and electronic engineers (IEEE), yang secara umum sebagai berikut : [Heriadi,D.2005]

a) Standar IEEE 802.11a yaitu wifi dengan frekuensi 5 Ghz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 300 m
b) Standar IEEE 802.11b yaitu wifi dengan frekuensi 2,4 Ghz yang memiliki kecepatan 11 mbps dan jangkauan jaringan 100 m
c) Standar IEEE 802.11g yaitu wifi dengan frekuensi 2,4 GHz yang memiliki kecepatan 54 mbps dan jangkauan jaringan 300 m
d) Standar IEEE 802.11 n, yaitu wifi yang memiliki kecepatan 108 – 120 Mbps.

c. Tipe Jaringan Wireless

Seperti halnya Ethernet-LAN (jaringan dengan kabel), jaringan *wifi* juga dikonfigurasikan ke dalam dua jenis jaringan, yaitu :

a) Jaringan *peer to peer / Ad Hoc wireless LAN*
   Sistem *Ad-hoc* adalah sistem *peer-to-peer*, dalam arti satu komputer dihubungkan ke satu komputer dengan saling mengenal SSID. Bila digambarkan mungkin lebih mudah membayangkan sistem koneksi langsung dari satu komputer ke satu komputer lainnya dengan menggunakan *twist pair cable* tanpa perangkat HUB.
b) Jaringan *server based/wireless* infrastruktur
   Sistem infrastruktur membutuhkan sebuah komponen khusus yang berfungsi sebagai access point.
   Untuk menggambarkan koneksi pada infrastruktur dengan akses point, sebuah jaringan wireless network minial harus memiliki satu titik pada tempat dimana komputer lain yang mencari/ menerima sinyal dapat masuk kedalam jaringan agar dapat berhubungan.

d. Komponen Utama jaringan WIFI

Terdapat empat komponen utama untuk membangun sebuah jaringan *wifi*, (Efvy Zamidra, 2014:5) yaitu :

a) *Access Point*, komponen yang berfungsi menerima dan mengirimkan data dari adapter *wireless*, *Access Point* mengonversi sinyal frekuensi radio menjadi sinyal digital atau sebaliknya komponen tersebut bertindak layaknya sebuah *hub/switch* pada jaringan Ethernet. Satu *Access Point* secara teori menampung beberapa sampai ratusan klien. Walaupun demikian, *Access Point* direkomendasikan dapat menampung maksimal 40-klien.
b) *Wireless-LAN device*, komponen yang dipasangkan di Mobile/Dekstop PC.
c) Mobile/Dekstop PC, Komponen akses untuk klien, mobile PC pada umunya sudah terpasang port PCMCIA (*Personal Computer Memory Card International Association*), sedangkan Dekstop PC harus ditambahkan PCI (Peripheral Componen Interconnect) Card, serta USB (*Universal Serial Bus*) Adapter
d) Ethernet LAN, Jaringan kabel yang sudah ada.

e. Two Factor

Otentikasi dua faktor adalah proses keamanan di mana pengguna menyediakan dua sarana identifikasi, salah satunya adalah biasanya tanda fisik, seperti kartu, dan lainnya yang biasanya sesuatu yang hafal, seperti kode keamanan. Dua faktor yang terlibat. Sebuah contoh umum dari dua faktor otentikasi adalah kartu bank, kartu itu sendiri adalah item fisik dan momor identifikasi pribadi (PIN) adalah data yang harus selalu ada bersama kartu bank itu sendiri.

2FA adalah suatu fitur keamanan yang difungsikan sebagai verifikasi apakah pengguna yang akan login benar – benar orang yang memiliki akun tersebut. Two factor atau dua faktor merupakan otentikasi yang menyediakan jelas identifikasi pengguna dengan menggunakan kombinasi dua komponen yang berbeda, komponen ini sesuatu yang pengguna tahu, sesuatu yang pengguna miliki atau sesuatu yang tak terpisahkan dari pengguna. Konsep 2FA sangatlah mudah, selain username (atau email) dan password akan ditambahkan satu langkah lagi yang

dibutuhkan untuk login. Inilah yang dimaksud cara verifikasi pemilik akun. Pengguna dua factor otentikasi untuk membuktikan identitas didasarkan pada pendekatan dua factor, factor yang digunakan harus benar, jika salah satu komponen hilang atau salah digunakan maka secara otomatis tidak bisa diakses

f. Password

Password adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Kata sandi juga dapat diartikan sebagai kata rahasia yang digunakan sebagai pengenal.

Kekuatan kata sandi adalah satu tolok ukur terhadap kekuatan, kerumitan dan keamanan dari suatu kata sandi rahasia yang digunakan sebagai pengenal Kekuatan suatu kata sandi bergantung pada kombinasi, kerumitan dan panjang dari kata sandi tersebut. Walaupun kata sandi memegang peranan yang penting dalam keselamatan komputer, kata sandi perlu digunakan secara wajar dan masuk akal dan berfungsi kepada pengguna. Kata sandi yang terlalu kuat akan sangat sulit untuk diingat dan biasanya akan ditulis dalam media kertas dan hal itu akan meningkatkan risiko kebocoran kata sandi tersebut.

g. WPA-PSK (WIFI Protected Access, Pre-Shared Key)

Pre-Shared Key (PSK) adalah metode otentikasi klien yang menggunakan passphrase, mengandung sampai 133 karakter, untuk menghasilkan kunci enkripsi yang unik untuk setiap klien nirkabel. PSK adalah salah satu dari dua metode otentikasi yang tersedia digunakan untuk WPA dan WPA2 enkripsi pada jaringan nirkabel Juniper Networks. PSK bukanlah metode otentikasi default saat membuat profil Layanan WLAN karena pilihan lain, otentikasi 802.1X, standar WLANyang baik adalah 802.11 dan lebih kuat.

Ada dua bentuk enkripsi yang tersedia saat menggunakan Direktur Jaringan, Wi-Fi Protected Access (WPA) dan WPA2 baru. PSK dapat digunakan dengan metode enkripsi : WPA / WPA2 Enterprise (membutuhkan server RADIUS) dan menyediakan cakupan untuk entitas besar. Dan WPA / WPA2 Personal (juga dikenal sebagai WPA-PSK) yang sesuai untuk digunakan di sebagian besar pengaturan bisnis perumahan kecil.

Dengan WPA-PSK, kita mengkonfigurasi setiap node WLAN (access point, router nirkabel, adaptor klien, jembatan) tidak dengan kunci enkripsi, melainkan dengan passphrase polos-Inggris yang berisi hingga 133 karakter. Menggunakan teknologi yang disebut TKIP (Temporal Key Integrity Protocol), passphrase yang, bersama dengan SSID jaringan, digunakan untuk menghasilkan kunci enkripsi yang unik untuk setiap klien nirkabel. Orang-orang kunci enkripsi secara konstan berubah. Ketika klien terhubung, pengguna otentikasi WPA-PSK memberikan password untuk memverifikasi apakah akan memungkinkan mereka akses ke jaringan. Selama password cocok, klien diberikan akses ke WLAN.

Perbedaan utama antara WPA dan WPA2-Personal adalah cipher enkripsi yang digunakan untuk mengamankan jaringan. WPA hanya dapat menggunakan enkripsi cipher Temporal Key Integrity Protocol (TKIP). Sedangkan WPA2-Personal dapat menggunakan TKIP, tetapi karena kunci keamanan TKIP kurang aman, protokol WPA2 biasanya menggunakan Advanced Encryption Standard (AES), AES menggunakan algoritma enkripsi canggih yang tidak bisa dikalahkan oleh alat-alat yang mengatasi keamanan TKIP, membuatnya menjadi metode enkripsi yang jauh lebih aman.

h. MAC Address

MAC Address (*Media Access Control Address*) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. MAC Address juga sering disebut sebagai *Ethernet address, physical address, atau hardware address.*

i. MAC Address Filtering

MAC Address Filtering merupakan metode filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti pencurian pc card dalam MAC filter dari suatu access point *sniffing* terhadap WLAN.

j. Fungsi MAC Address Filtering

Fitur MAC Address Filter ini berfungsi untuk membantu anda untuk mencegah pengguna asing (tidak diinginkan) yang berniat untuk mengakses masuk ke jaringan router nirkabel anda. Dengan menerapkan fitur ini, maka hanya perangkat nirkabel yang memiliki alamat MAC yang telah terdaftar (ditetapkan) saja yang dapat memperoleh akses ke router nirkabel.

Wireless LAN dapat memfilter berdasarkan MAC address dari *station/client*, hampir semua access point mempunyai kemampuan untuk memfilter berdasarkan MAC address. Administrator jaringan dapat mengompilassi, mendistribusikan, dan memelihara daftar MAC address yang diizinkan

dan memprogram masing-masing access point, jika sebuah PC card atau client lain dengan sebuah MAC address yang tidak terdaftar mencoba untuk mengakses *wifi*, kemampuan MAC address filtering tidak akan mengizinkan client berhubungan dengan access point.

4. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini menggunakan *The Security Policy Development Life Cycle* (SPDLC). (Goldman, James E, and Rawles, Philip T) yang memiliki enam tahapan, yaitu :

a. Identifikasi
   Pada tahapan ini penulis mengidentifikasi masalah yang berhubungan dengan keamanan wireless.
b. Analisis
   Tahapan ini penulis menganalisis resiko keamanan, ancaman, dan vulnerabilities.
c. Perancangan
   Yang dilakukan penulis dalam tahapan perancangan ini yaitu mengatur keamanan pada wireless dengan menggunakan keamanan pada WPA-PSK dan keamanan pada Mac Address filtering.
d. Implementasi
   Setelah setting keamanan pada wireless selesai dikerjakan, penulis melakukan uji coba terhadap sistem keamanan tersebut sehingga sistem keamanan tersebut dapat diimplementasikan atau diterapkan.
e. Audit
   Memeriksa sistem keamanan yang diterapkan.
f. Evaluasi
   Mengevaluasi sistem keamanan yang telah diterapkan.

Karena keterbatasan waktu dan wewenang yang ada, maka tahap Audit dan Evaluasi tidak akan di bahas akan tetapi diterjemahkan sebagai proses pengujian dan analisisnya.

5. Hasil, Pembahasan dan Kesimpulan

a. Hasil

Dua faktor keamanan dalam penelitian ini menggunakan keamanan WPA-PSK dan dengan menggunakan Mac Address Filtering, yang berarti jika ada sesorang yang ingin mengakses wifi harus mempunyai dua otentikasi, karena apabila hanya memiliki password WPA-PSK-nya saja maka tetap tidak akan bisa terkoneksi karena mac address pada perangkatnya tidak terdaftar. Dalam penelitian ini penulis menggunakan wireless TP-LINK TL-WR1043ND.

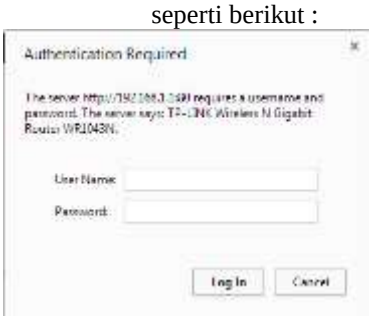
b. Pembahasan

Setting WPA-PSK di wireless TP-LINK TL-WR1043ND

a) Langkah pertama, Buka web browser, kemudian ketik alamat ip router default 192.168.1.1 ke address bar dan enter

Gambar 1 Langkah Pertama

Kemudian akan tampil halaman login seperti berikut :

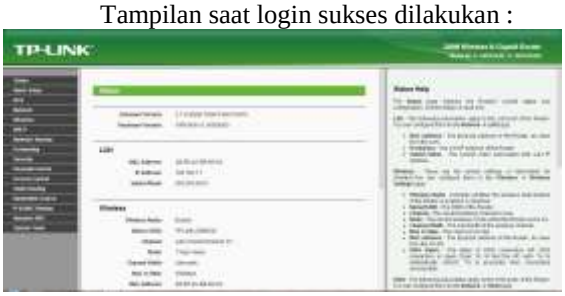


Gambar 2 Halaman Login

b) Langkah ke 2, ketik username dan password dalam halaman login, username dan password default keduanya adalah admin, lalu klik log in untuk login ke perangkat.

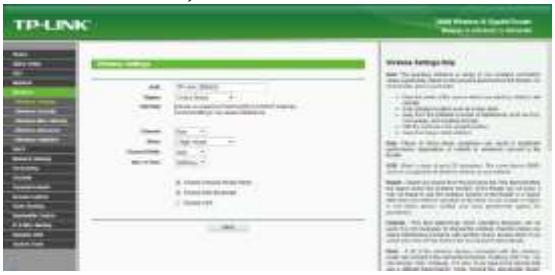
Gambar 3 Langkah ke Dua

Tampilan saat login sukses dilakukan :



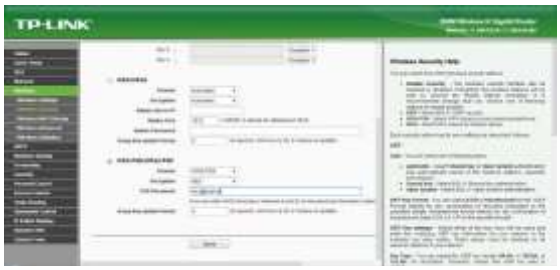
Gambar 4 Tampilan Login Sukses

c) Langkah ke 3, klik pada wireless setting di sisi kiri untuk membuka halaman pengaturan keamanan,



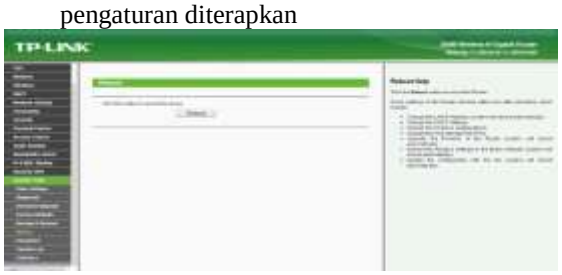
Gambar 5 Langkah ke Tiga

d) Langkah 4, setting keamanan nirkabel jaringan, akan ditampilkan sebagai berikut : Pilih WPA-PSK atau WPA2-PSK untuk jaringan otentikasi, pilih TKIP atau AES untuk enkripsi WPA, Kemudian masukan sandi/kunci ke kotak kunci WPA Pre-Shared, dan save.



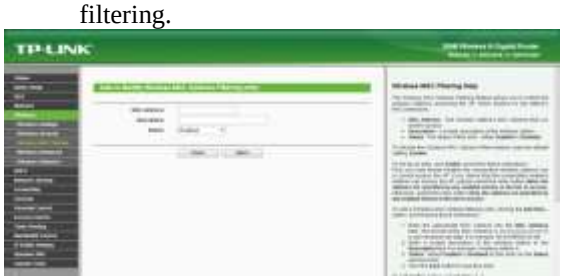
Gambar 6 Langkah ke Empat

e) Pilih sistem tool -> Reboot pada menu sebelah kiri. Reboot router untuk membuat semua pengaturan diterapkan



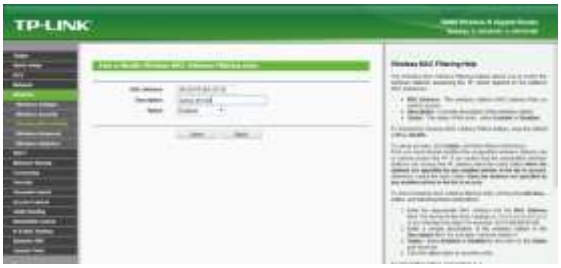
Gambar 7 Pilihan Sistem Tool

1. Setting Mac Address Filtering di wireless TP-LINK TL-WR1043ND
   1) Langkah pertama sama halnya dengan setting WPA-PSK, buka web browser, kemudian ketik alamat ip router default 192.168.1.1 ke address bar, enter dan login.
   2) Langkah selanjutnya pilih wireless disisi kiri untuk membuka halaman Wireless Mac filtering.



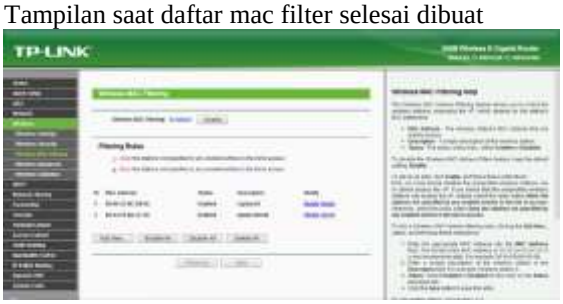
Gambar 8 Setting Mac Address Filtering di wireless TP-LINK TL-WR1043 ND

   3) Langkah ke 3, pilih enable Mac filtering, kemudian klik add new untuk menambahkan Mac Address perangkat yang akan ditambahkan ke daftar filter dan save.



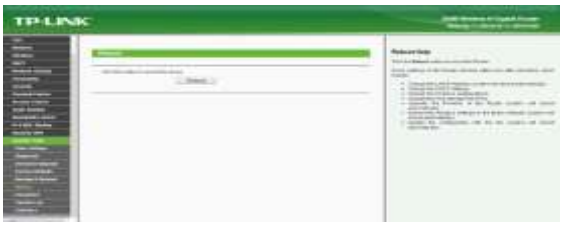
Gambar 9 Pilihan Enable Mac Filtering

Tampilan saat daftar mac filter selesai dibuat



Gambar 10 Tampilan saat daftar Mac Filter selsai

   4) Pilih sistem tool -> Reboot pada menu sebelah kiri. Reboot router untuk membuat semua pengaturan diterapkan.



Gambar 11 Reboot Router

a) Dengan menggunakan keamanan two factor, memiliki beberapa kelebihan dibandingkan dengan menggunakan keamanan pada WPA-nya saja, karena dengan menggunakan dua otentikasi ini jika ada seseorang yang ingin mengakses ke hotspot harus memiliki password WPA-PSK dan mendaftarkan Mac Address perangkatnya ke Administrator, karena jika tidak memenuhi persyaratan keduanya atau salah satunya tidak akan bisa terkoneksi.

6. Kesimpulan

a) Two factor authentication dapat diterapkan untuk meningkatkan keamanan wifi, yaitu dengan dua tahapan otentikasi password, dan Mac address filtering.

7. Daftar Pustaka

[1] Membuat Jaringan Wireless, Elex Media Komputindo, (2014).
[2] Jubilee Enterprise, Trik Membuat Jaringan Komputer dan Wi-fi,Elex Media Komputindo, (2014).
[3] Zainal Arifin, Sistem Pengamanan Jaringan Wireless, Andi Yogyakarta, 2008Wireless Tanpa Teknisi, Andi Publisher, (2012).
[4] Heriadi,D. Jaringan Internet Wi-Fi.CV Andi Offset.Yogyakarta. (2005).

Redaksi :
Pusat Studi Teknologi Informasi (PSTI).
Gedung Business Center Lt 2
Jl. Zainal Abidin No. 26 Bandar Lampung
Telp. 0721 - 774626
SistemInformasi@ubl.ac.id