Implementasi *Protected Extensible Authentication Protocol* (PEAP) menggunakan *Remote Access Dial In User Service (RADIUS)*

Yosua John Muskitta[1], Banu Wirawan Yohanes[2], Hartanto Kusuma Wardana[3]

Program Studi Sistem Komputer,
Fakultas Teknik Elektronika dan Komputer,
Universitas Kristen Satya Wacana, Salatiga
[1]622009015@student.uksw.edu, [2]banu.yohanes@staff.uksw.edu,
[3]hartanto.kusuma@staff.uksw.edu

Ringkasan

Perkembangan teknologi jaringan nirkabel memungkinkan kita melakukan komunikasi tanpa harus dibatasi oleh panjangnya kabel. Namun teknologi nirkabel rentan dari sisi keamanan karena pesan dikirimkan secara *broadcast*. Oleh karena itu dibutuhkan metode pengaman komunikasi pada jaringan nirkabel. *Protected Extensible Authentication Protocol* (PEAP)merupakan salah satu metode keamanan jaringan komputer pada layer link OSI sebagai ekstensi dari EAP dengan mengintegrasikan fitur *Transport Layer Security* (TLS). Makalah ini membahas implementasi PEAP menggunakan *Remote Access Dial In User Service (RADIUS)*, mulai dari perancangan arsitektur jaringan komputer nirkabel berbasis klien-server, konfigurasi perangkat jaringan komputer dan sistem,sampai dengan pengujian hasil *capture* paket data PEAP dan analisis paket jaringan komputer. Hasil pengujian menunjukan pentingnya menambahkan fitur keamanan pada komunikasi data nirkabel.

Kata kunci: PEAP, RADIUS, Klien-server

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi saat ini telah sampai pada era *broadband*. Berbeda dengan era sebelumnya dimana akses Internet bukan saja lambat, kapasitasnya juga relatif kecil, sehingga berbagai konten yang berkembang juga masih terbatas. Namun kinidiperkirakan akan lebih banyak berkembang aplikasi-aplikasi baru yang membutuhkan *bandwidth* yang besar.

Banyak orang lebih memilih teknologi *mobile* (bergerak) agar dapat mempermudah aktifitas mereka. Maka teknologi nirkabel diciptakan untuk area jaringan yang langsung bersentuhan dengan orang-per-orang, yaitu jaringan nirkabel. Teknologi ini sangat mendukung tingkat produktivitas di tengah mobilitas yang tinggi. Teknologi tersebut lebih dikenal sebagai *Wireless Local Area Network* (WLAN) atau *Wireless-Fidelity* (*Wi-Fi*).

Peningkatan tersebut telah membawa kepada tuntutan kebutuhan suatu sistem keamanan jaringan komputer yang baik. Salah satu metode keamanan untuk menanggulangi masalah ini adalah dengan menggunakan sistem autentikasi. Sistem ini akan melakukan proses pengesahan identitas pengguna yang biasanya diawali dengan pengiriman kode unik yang dapat berupa *username* dan *password* untuk memastikan pengguna yang sah.

Wired Equivalent Privacy (WEP) adalah standar keamanan dan enkripsi pertama yang digunakan pada jaringan nirkabel. WEP disebut juga sebagai*shared key authentication*. Enkripsi WEP menggunakan kunci yang diberikan oleh administrator kepada klien dan*Access Point*(AP). Persoalan kunci statik yang lemah dan penggunaan algoritma enkripsi RC4 sudah using karena mudah dipecahkan membuat WEP tidak lagi digunakan [1].

Wi-fi Protected Access (WPA) adalah teknologi yang digunakan untuk menggantikan WEP. WPA dirancang untuk menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik dengan menggunakan *Temporal Key Integrity Protocol* (TKIP). Proses autentikasi WPA menggunakan standar 802.1X dan *Extensible Authentication Protocol* (EAP) [RFC3748].

Protected EAP (PEAP)merupakan salah satu metode EAP. PEAP adalah tipe protokol autentikasi yang berbasis *username* dan *password* untuk mengamankan proses autentikasi. PEAP kebanyakan digunakan pada jaringan LAN nirkabel, tetapi dapat juga digunakan pada autentikasi kabel, *Network Access Protection* (NAP), bahkan *Virtual Private Network* (VPN). PEAP memerlukan sertifikat digital pada sisi server saja untuk membuat TLS *tunnel* yang aman untuk melindungi autentikasi *user*. PEAP menggunakan *server-side public key certificates* untuk mengautentikasi server. Kemudian membuat TLS *tunnel* antara klien dan server autentikasi. PEAP adalah pilihan yang baik untuk protokol autentikasi karena kompatibel dengan banyak perangkat keras dari berbagai vendor, misalnya Microsoft, CISCO, dan Funk.

Makalah ini membahas implementasi *Remote Authentication Dial-in User Service* (RADIUS) pada sistem keamanan jaringan WLAN menggunakan *Free Radius*[2] dengan protokol *Protected Extensible Authentication Protocol* (PEAP).

2. Implementasi PEAP

Bagian ini menjelaskan persiapan implementasi PEAP yang dimulai dengan perancangan dan konfigurasi jaringan komputer nirkabel, server autentikasi, dan AP.

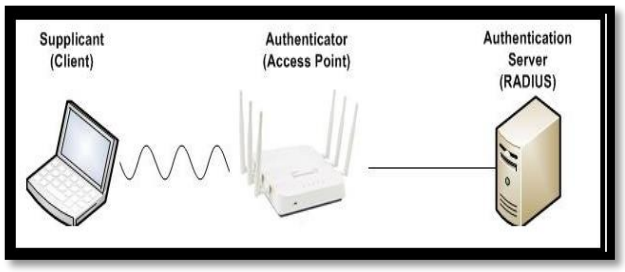
2.1. Arsitektur Jaringan Komputer Nirkabel

Infrastruktur jaringan komputer nirkabel yang dibuat terdiri dari 3 buah perangkat, yaitu komputer personal (PC) klien sebagai *supplicant*, AP sebagai autentikator, dan server autentikasi RADIUS. Ketiga perangkat tersebut harus berada dalam sebuah WLAN seperti ditunjukkan pada Gambar 1.

2.2. Pemodelan *Authentication, Authorization,* dan *Accounting*(AAA)

Klien memperoleh akses data dan sumber daya jaringan melalui berbagai perangkat baik switch ethernet, AP, dan server VPN. Ketika perangkat tersebut digunakan untuk mengendalikan akses ke jaringan, misalnya AP dengan fitur keamanan jaringan WPA2 Enterprise atau switch ethernet dengan 802.1x (EAP) mengaktifkan autentikasi berbasis port [3], keduanya dirujuk sebagai *Network Access Server* (NAS). Seluruh perangkat tersebut memerlukan pengendali untuk memastikan keamanan yang baik.

Persyaratan pada keamanan jaringan itu yang sering disebut sebagai *Authentication, Authorization,* dan *Accounting* (AAA) [RFC2903].



Gambar 1. Arsitekturjaringan komputer nirkabel

Authentication adalah tahapan awal untuk mendapat akses dalam sebuah jaringan. Autentikasi mengkonfirmasi apakah klien berhak mendapatkan layanan atau tidak. Cara yang paling umum untuk membuktikan identitas klien adalah dengan *username* dan *password*. Cara lain adalah dengan menggunakan sertifikat, PIN, dan token.

Authorization adalah pengalokasian layanan yang berhak diakses oleh klien pada jaringan. Autorisasi dilakukan ketika klien telah dinyatakan berhak untuk menggunakan jaringan atau setelah tahap autentikasi selesai dilakukan.

Accounting merupakan proses yang dilakukan oleh NAS dan server AAA yang mencatat semua aktivitas klien dalam jaringan, seperti kapan klien mulai menggunakan jaringan, kapan klien mengakhiri koneksinya dengan jaringan, berapa lama klien menggunakan jaringan, berapa banyak data yang diakses klien dari jaringan, dan lain sebagainya. Informasi yang diperoleh dari proses akunting disimpan pada server AAA dan dapat digunakan untuk berbagai keperluan seperti *billing*, *auditing*, atau manajemen jaringan.

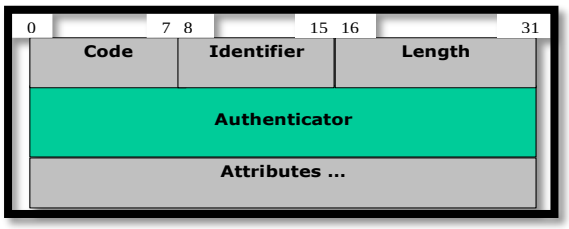
2.3. *Remote Authentication Dial-in User Service* (RADIUS)

RADIUS merupakan protokol keamanan jaringan komputer untuk manajemen akses kontrol pada jaringan yang besar. RADIUS merupakan bagian dari solusi AAA yang dikembangkan oleh Livington Enterprises kepada Jaringan Merit pada tahun 1991 [2].

RADIUS melakukan autentikasi, autorisasi, dan akunting akun pengguna secara terpusat untuk mengakses sumber daya jaringan. Caranya dengan memastikan bahwa pengguna yang mengakses jaringan adalah pengguna yang sah. RADIUS berbasis standar IEEE 802.1X dan sering disebut sebagai autentikasi berbasis port. RADIUS merupakan protokol klien-server yang berada pada layer aplikasi pada OSI layer dengan protokol transport berbasis *User Datagram Protocol* (UDP)[4, 5].

RADIUS menggunakan paket UDP untuk komunikasi data antara klien dan server. Berikut penjelasan format paket data RADIUS yang ditampilkan pada Gambar 2:

1. ***Code***: Memiliki panjang satu oktet dan digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan berdasarkan daftar kode pada Tabel 1.
2. *Identifier*: Berfungsi untuk memeriksa*request* dan *response*
3. *Length*: Panjang data dari paket yang dikirim termasuk *Code*, *Identifier*, *Length*, *Authenticator*,dan *Attribute*.
4. *Authenticator*: 16 oktet yang menunjukan *request* dan *response*dari autentikator.
5. ***Attributes***: Berisikan informasi yang dibawa pesan RADIUS. Setiap pesan dapat membawa satu atau lebih atribut. Contoh atribut RADIUS adalah *username*, *password*, *CHAP-password*, alamat IP AP, dan pesan balasan.



Gambar 2. Format paket data RADIUS [2]

Tabel 1. Daftar keterangan kode paket data RADIUS

Kode	Keterangan
1	*Access-Request*
2	*Access- Accept*
3	*Access-Reject*
4	*Accounting-Request*
5	*Accounting-Response*
11	*Access-Challenge*
12	*Status-Server (experimental)*
13	*Status-client (experimental)*
255	*Reserved*

2.4. Konfigurasi Jaringan Komputer Nirkabel

Setelah perangkat keras dan lunak tersedia, maka ketiga perangkat pada jaringan komputer nirkabel perlu dikonfigurasi untuk dapat saling berkomunukasi satu sama lain.

Konfigurasi pada sisi server dimulai dengan mengisi nama *database* yang digunakan, info koneksi berisi nama server dan port yang digunakan, data login *database*, dan tabel *database* yang digunakan pada file konfigurasi *sql.conf*. Kemudian sertakan file *sql.conf* tersebut pada file konfigurasi RADIUS, *Radius.conf* menggunakan baris perintah *$INCLUDERadius.conf*. Kemudian konfigurasi alamat IP pada server RADIUS.

Untuk konfigurasi pada sisi klien isikan kata kunci rahasia dan nama jaringan nirkabel pada file *clients.conf*. Tentukan jenis EAP pada file *eap.conf*, yaitu PEAP. Kemudian konfigurasi penggunaan enkripsi data dan metode autentikasi yang kuat pada file *mschap*. Berikut contoh konfigurasi alamat IP server autentikasi RADIUS dan sebuah PC klien di laboratorium jaringan komputer BB5:

Konfigurasi IP *address* server RADIUS

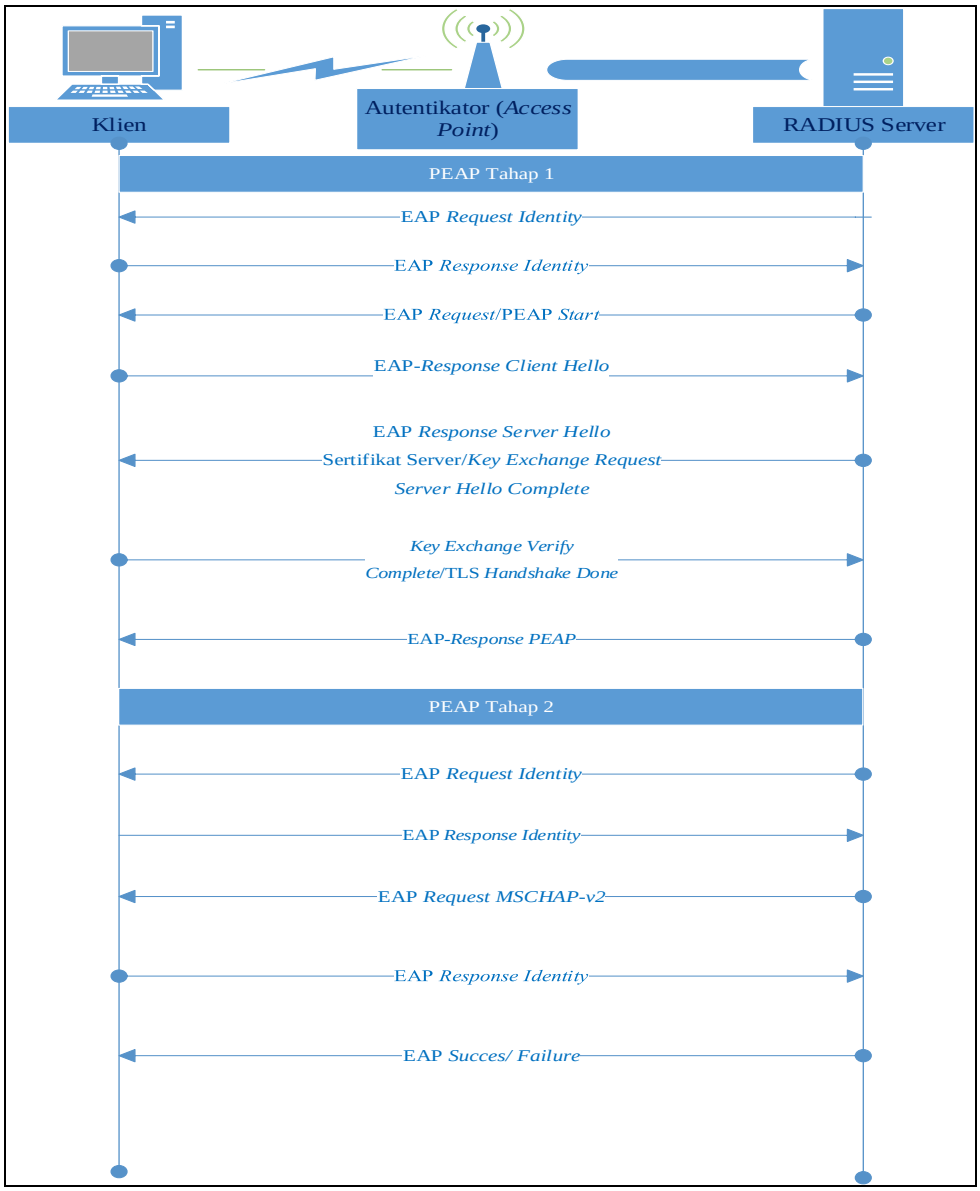
```
auto eth0
iface eth0 inet static
address 192.168.5.2
netmask 255.255.255.0
network 192.168.5.0
broadcast 192.168.5.255
gateway 192.168.5.1
dns-nameservers 192.168.5.1
```

Konfigurasi *fileclients.conf*

```
Client 192.168.5.1/24 {
secret      = testing123
shortname   = BB5
}
```

Konfigurasi pada AP dilakukan untuk mendukung proses autentikasi dengan metode PEAP. Berikut contoh konfigurasi AP yang sesuai dengan konfigurasi server autentikasi RADIUS dan klien sebelumnya adalah sebagai berikut:

```
SSID                : BB5
Region              : Indonesia
Channel             : 7
Mode                : 54 Mbps (802.11g)
Security Type       : WPA/WPA2
Security Options    : Automatic
Encryption          : AES
RADIUS Server IP    : 192.168.5.2
RADIUS Password     : testing123
```



Gambar 3. Aliran paket data PEAP tahap 1 dan 2

3. Hasil Pengujian dan Analisis

Cara kerja PEAP dibagi menjadi 2 tahap seperti ditunjukkan pada Gambar 3, yaitu:

1. Pembuatan tunnel *Transport Layer Security* (TLS)
   a. Klien mengirimkan EAP *start message* kepada AP.
   b. AP membalas dengan pesan EAP *request identity*.
   c. Klien mengirimkan mengirimkan *username* sebagai balasan.
   d. AP melanjutkan *username* tersebut kepada RADIUS server dengan pesan RADIUS *access request*.
   e. RADIUS server membalas dengan mengirimkan sertifikat digital.
   f. Klien melakukan verifikasi sertifikat tersebut.
2. Autentikasi menggunakan EAP-MSCHAPv2 yang merupakan pengembangan dari protokol autentikasi *Challenge Handshake Authentication Protocol* (CHAP) yang dikembangkan oleh Microsoft.
   a. Klien dan server bernegosiasi untuk membuat *tunnelTransport Layer Security* (TLS) yang terenkripsi.
   b. Pertukaran pesan dalam *tunnel* menggunakan EAP-MSCHAPv2.
   c. RADIUS server mengirimkan pesan RADIUS *accept*.

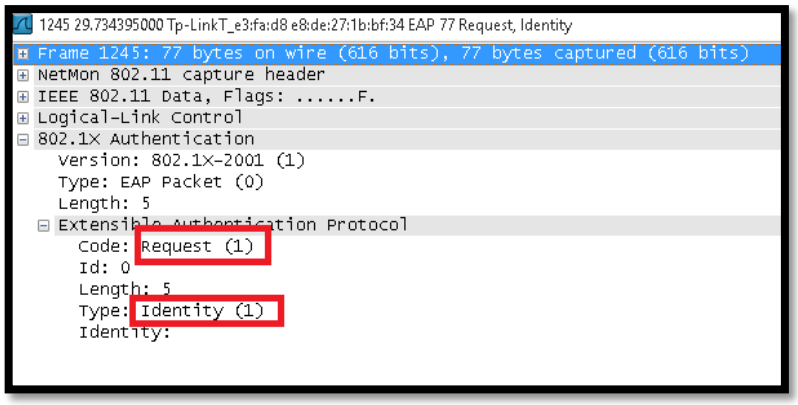
Untuk melakukan *capture* paket data yang dikirimkan maka dibuat skenario klien melakukan proses autentikasi sambil menjalankan perangkat lunak Wireshark pada *monitor mode.* Contoh hasil *capture* pada autentikasi PEAP antara klien dengan alamat *Media Access Control* (MAC) E8:DE27:1B:BF:34 dan AP TP Link ditampilkan pada Gambar 4a., b., dan c. Kemudian besar ukuran pesan pada paket PEAP ditunjukkan pada Tabel 2.

Gambar 4a. menunjukkan bahwa paket sebesar 5 *Bytes* dikirimkan oleh AP kepada klien untuk meminta identitas dari klien secara opsional. *Code* menunjukan bahwa paket tersebut merupakan paket *request* dengan Id 0 dan tipe *identity*.

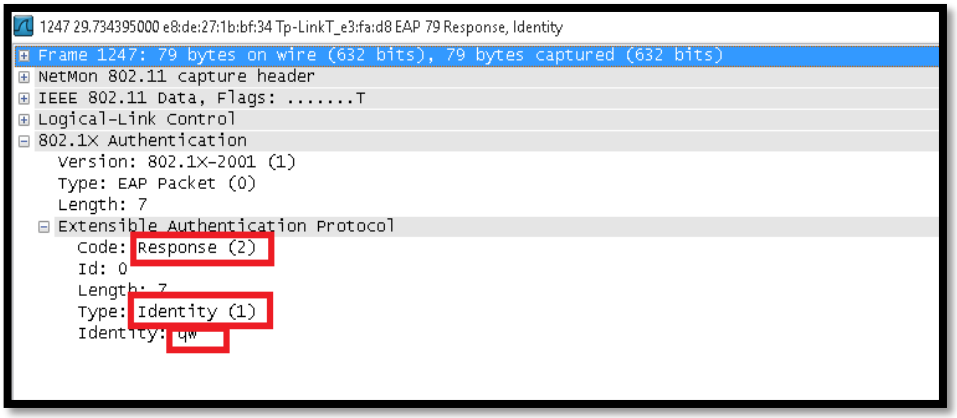
Gambar 4b. menunjukkan bahwa paket dikirimkan oleh klien kepada AP sebagai balasan dari paket EAP *request identity* yang dikirimkan oleh AP kepada klien sebelumnya pada Gambar 4a. Kali ini klien mengisi identitas dengan *anonymus identity* yaitu 'qw'. Paket ini memiliki panjang 7 *Bytes*. *Code* menunjukan bahwa paket ini merupakan paket *response* (2) dengan Id 0 dan tipe*identity*. Pada baris Id menunjukan angka 0 yang berarti merupakan balasan dari paket sebelumnya yang dikirimkan oleh server RADIUS melalui AP yaitu EAP *request identity.*

Gambar 4c. menampilkan paket *request type*-PEAP sebesar 6 *Bytes* yang menyatakan bahwa proses autentikasi server menggunakan metode PEAP. *Code*menunjukkan bahwa paket ini merupakan paket *request* (1) pada bagian Id tertulis angka 1 yang berarti paket ini bukan merupakan serangkaian sesi dari EAP *request identity* dan EAP *response identity*,melainkan pada sesi baru. Tipemenunjukkan metode EAP yang akan digunakan pada kondisi ini, yaitu metode *Protected*-EAP (PEAP).

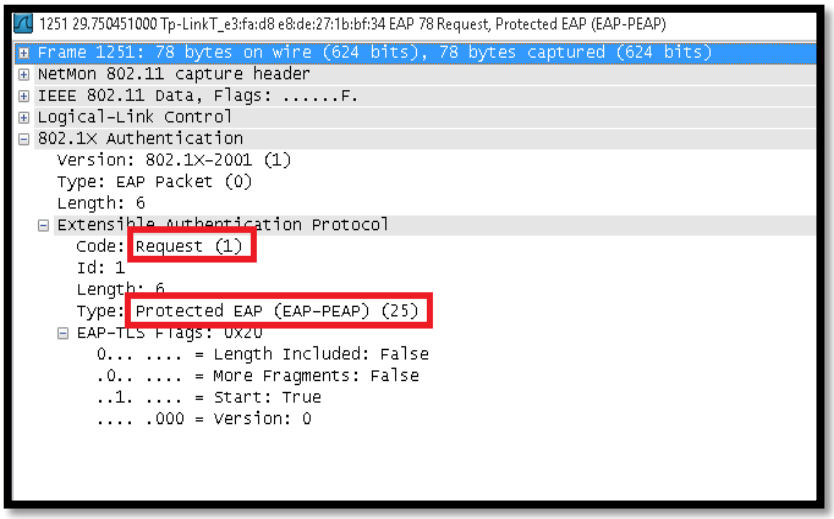
Pada tahap selanjutnya akan digunakan protokol SSL untuk membuat *tunnel* yang mengenkripsi identitas klien. Seluruh pengujian dilakukan di laboratorium jaringan komputer BB5. Berdasarkan hasil *capture* paket data PEAP sesuai dengan format data PEAP dan urutan transmisi data PEAP sesuai dengan cara kerja PEAP, demikian juga dengan besarnya ukuran data yang digunakan.



(a)



(b)



(c)

Gambar 4a. Paket EAP *Request Identity*; 4b. Paket EAP *Response Identity*; 4c. Paket EAP *Request Protected* EAP (PEAP)

Tabel2. Ukuran paket data PEAP yang di-*capture*

No Paket	Pengirim	Tujuan	Nama Paket Data	Ukuran Paket Data (*Byte*)
1	Server	Klien	EAP- *Request Identity*	5
2	Klien	Server	EAP - *Response Identity*	7
3	Server	Klien	EAP - *Request type* : PEAP	6
4	Klien	Server	*Client Hello*	219
5	Server	Klien	*Server Hello*	1024
6	Klien	Server	*Client key exchange, change chiper spec, encrypted handshake message*	144
8	Klien	Server	EAP - *Response Protected* EAP (PEAP)	6
9	Server	Klien	*Application Data*	43
10	Klien	Server	*Application Data*	80
11	Server	Klien	*Application Data*	59
12	Klien	Server	*Application Data*	144
13	Server	Klien	*Application Data*	91
14	Klien	Server	*Application Data*	80
15	Server	Klien	*Application Data*	43
16	Klien	Server	*Application Data*	80
17	Server	Klien	*Application Data*	43
18	Server	Klien	EAP *Success*	4

4. Kesimpulan

PEAP merupakan salah satu metode EAP yang menggunakan 2 tahap autentikasi. Prinsip dari PEAP serupa dengan EAP-TLS dimana keduanya menggunakan TLS untuk mengamankan seluruh pertukaran pesan dalam komunikasi. Namun PEAP menggantikan autentikasi menggunakan sertifikat pada klien dengan kombinasi *username* dan *password*. Salah satu kelebihan PEAP dibandingkan EAP-TLS adalah klien dapat mengakses menggunakan perangkattanpa harus terinstal sertifikat klien terlebih dahulu. Dengan membuat *tunnel* TLS dan memuat percakapan pesan EAP di dalamnya. PEAP menyediakan enkripsi autentikasi, integritas, dan proteksi terhadap percakapan pesan EAP.

Berdasarkan hasil pengujian implementasi PEAP menggunakan RADIUS terdapat beberapa keuntungan menggunakan PEAP dibaningkan tanpa PEAP, yaitu:

1. Proteksi identitas: Dengan mengenkripsi pertukaran identitas pada *tunnel* TLS, PEAP menyediakan *confidentiality* bagi identitas *user*.
2. Perlindungan negosiasi: Pertukaran pesan EAP dengan metode PEAP dibalas per paket dan dienkripsi.
3. Perlindungan saat koneksi terputus: PEAP melindungi pertukaran pesan EAP ketika koneksi terputus karena PEAP mengirim pesan *success/failure* di dalam *tunnel* TLS.

Daftar Pustaka

[1] S. Riley, "*Wireless LAN Security with 802.1x, EAP-TLS, and PEAP*," Senior Consultant, MCS Trustworthy Computing Services, 2003

[2] D. Van der Walt, "*FreeRADIUS Beginner's Guide*," Packt Publishing, 2011.

[3] L. Strand, "*802.1X Port-Based Authentication HOWTO*," 2004.

[4] B. Aboba, P. Calhoun, "*RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*," RFC 3579, DOI 10.17487/RFC3579, 2003, <http://www.rfc-editor.org/info/rfc3579>.

[5] C. Rigney, S. Willens, A.Rubens, dan W. Simpson, "*Remote Authentication Dial In User Service (RADIUS)*," RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.