BAB 5
Kesimpulan

5.1 Kesimpulan

Dari semua jabaran bab dahulu, bahwa penulis menentukan suatu pendapat yang dapat dijabarkan dibawah ini :

1. Penerapan aplikasi *Free*RADIUS diimplementasikan pada pengamanan jaringan *wireless* ini sebagai RADIUS *server* yaitu penggunaan AAA (*Authentication, Authorization, Accounting*), penerapan tersebut mendukung dalam penggunaan protokol EAP-TTLS dan otentikasi MSCHAPv2 pada jaringan *wireless*.
2. Penerapan pada protokol EAP-TTLS (Tunneled TLS-EAP) dan *inner* otentikasi MSCHAPv2 ini dapat digunakan dengan baik serta dapat digunakan dalam menangani proses keamanan otentikasi pada suatu jaringan *wireless*.
3. Dengan otentikasi *user* secara terpusat dapat mempermudah administratornya dalam *monitoring* serta mengatur sumber daya jaringan pada jaringan *wireless* tersebut.
4. Protokol keamanan jaringan *wireless* LAN dengan menggunakan EAP-TTLS dengan otentikasi MSCHAPv2 mampu menangani tipe penyerangan *dictionary attack* dari pada keamanan jaringan yang menggunakan WPA2-*Personal* dengan otentikasi *Pre-Shared Key*.

5.2 Saran

Dalam penelitian lebih lanjut, yang berkaitan dengan pengamanan otentikasi terpusat dengan menggunakan protokol EAP-TTLS dan MSCHAPv2 penulis memberikan saran sebagai berikut:

1. Pada penerapan protokol keamanan EAP-TTLS dan MSCHAPv2 ini dipengaruhi oleh spesifikasi *hardware* yang digunakan, sehingga akan lebih

bagus bila PC *server* memiliki spesifikasi *hardware* yang tinggi agar dapat menjaga kualitas kinerja.

2. Untuk pengembangan berikutnya pada proses otentikasi dengan menggunakan EAP-TTLS dan MSCHAPv2 ini tidak hanya diterapkan pada jaringan *wireless* LAN atau nirkabel, namun juga diterapkan pada jaringan LAN atau dengan kabel.