BAB 4 ANALISIS DAN PERANCANGAN

4.1 Analisis Kebutuhan

Dalam penelitian ini, pengimplementasian standar IEEE 802.1X sesuai dengan uraian pada batasan masalah yang ada pada bab sebelumnya. IEEE 802.1X memberikan layanan untuk proses autentikasi pengguna dalam mengakses jaringan lokal berbasis kabel.

4.1.1 Kebutuhan Fungsional

Kebutuhan fungsional sistem menjelaskan hal – hal yang harus dilakukan sebuah sistem. Kebutuhan fungsional bergantung pada jenis dari perangkat lunak atau keras yang dikembangkan, serta tujuan umum pengembangan perangkat lunak atau keras tersebut. Berdasarkan uraian layanan yang dimiliki oleh IEEE 802.1X pada analisis kebutuhan, berikut kebutuhan fungsional dari implementasi autentikasi mode multi-auth pada jaringan *Local Area Network* berbasis kabel menggunakan protokol IEEE 802.1X dan radius server:

1. *Supplicant* mengaktifkan protokol IEEE 802.1X pada sistem operasi perangkat pengguna jaringan untuk melakukan autentikasi.
2. *Supplicant* tidak mengaktifkan protokol IEEE 802.1X pada sistem operasi perangkat pengguna jaringan untuk melakukan autentikasi.
3. *Supplicant* switch hub meneruskan paket yang diberikan *supplicant* ke switch authenticator.
4. Switch authenticator me-*relay*-kan paket dari *supplicant* ke radius server.
5. Switch authenticator mengeksekusi apakah *supplicant* dapat mengakses jaringan lokal atau tidak.
6. Radius server bertindak sebagai penentu apakah suatu *supplicant* valid atau tidak.

4.1.2 Kebutuhan Non-Fungsional

Kebutuhan non-fungsional merupakan kebutuhan yang tidak terhubung secara langsung dengan layanan sistem dan penggunanya. Kebutuhan non-fungsional dapat diartikan sebagai batasan yang ada pada implementasi sistem seperti tertera pada batasan masalah yang ada pada bab sebelumnya serta membandingkan host-mode yang lebih kecil berdasarkan waktu autentikasi pada mode single-host dan multi-auth dan menguji integritas kredensial data yang dikirim oleh *supplicant* dan diterima oleh radius server.

4.1.3 Kebutuhan Perangkat Keras

Berikut merupakan perangkat keras pendukung implementasi autentikasi mode multi-auth pada jaringan *Local Area Network* berbasis kabel menggunakan standar protokol IEEE 802.1X dan radius server:

- Komputer Fisik (PC):
  - OS : Windows 10 Enterprise (64-bit)
  - Prosesor : Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
  - RAM : 8 GB
  - Jumlah : 3
  - Fungsi : Untuk *supplicant* dalam melakukan autentikasi IEEE 802.1X
- Laptop:
  - OS : Windows 10 Pro (64-bit)
  - Prosesor : Intel(R) Core(TM) i7-4500U CPU @ 1.80GHz
  - RAM : 4 GB
  - Jumlah : 1
  - Fungsi : Untuk menjalankan satu *Virtual Machine* sebagai Radius server
- Switch hub:
  - Merk : D-Link
  - Jenis : DES-1005A
  - Jumlah : 1
  - Fungsi : Untuk menghubungkan semua PC dan switch Menggunakan Kabel LAN
- Switch *Manageable*:
  - Merk : Cisco Catalyst
  - Jenis : WS-C2960CX-8TC-L
  - Jumlah : 1
  - Fungsi : Untuk menghubungkan semua PC, Switch Hub dan Laptop menggunakan Kabel LAN
- Kabel LAN:
  - Merk : Belden
  - Jenis : UTP + RJ45
  - Fungsi : Untuk menghubungkan perangkat keras dalam Jaringan

4.1.4 kebutuhan Perangkat Lunak

Berikut merupakan perangkat lunak pendukung implementasi autentikasi mode multi-auth pada jaringan *Local Area Network* berbasis kabel menggunakan standar protokol IEEE 802.1X dan radius server:

- Windows Server 2008 R2

  Sistem operasi ini di *install* pada sisi radius server untuk mendukung dalam implementasi autentikasi mode *multi-auth* pada jaringan *Local Area Network* berbasis kabel menggunakan protokol IEEE 802.1X dan radius server.

- Windows 10 Pro

  Sistem operasi yang di *install* pada sisi *supplicant* untuk mendukung dalam implementasi autentikasi mode *multi-auth* pada jaringan *Local Area*

Network berbasis kabel menggunakan protokol IEEE 802.1X dan radius server.

- VirtualBox

  Perangkat lunak ini digunakan untuk menjalankan sistem operasi secara virtual. Adapun spesifikasi dari *Virtual Machine* radius server yang digunakan adalah sebagai berikut:

  - OS : Windows Server 2008 R2 *(64-bit)*
  - RAM : 2 GB
  - Harddisk : 35 GB *(fixed)*
  - Jumlah : 1

- Network Policy Server

  Perangkat lunak yang digunakan sebagai server autentikasi dimana perangkat lunak ini akan menentukan apakah suatu *supplicant* valid atau tidak dalam mengakses jaringan lokal.

- Active Directory Domain Services

  Suatu layanan yang menyediakan layanan tempat menyimpan semua sumber daya jaringan di dalam server. Menyimpan informasi tentang *supplicant,* computer, dan device lain yang ada pada jaringan ke dalam suatu domain. *Resources* dan *supplicant* dari domain dapat mengakses informasi secara luas yang ada didalamnya secara aman.

- DNS Server

  Domain Name System suatu layanan yang digunakan untuk mengetahui IP Address suatu host lewat hostname-nya. Sistem dalam jaringan TCP/IP yang digunakan untuk penamaan komputer agar lebih *user friendly.*

- DHCP Server

  Perangkat Lunak yang dipakai untuk memudahkan pengalokasian alamat IP dalam suatu layanan jaringan. Sebuah jaringan lokal dibuat DHCP maka semua semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP.

- Active Directory Certificate Services

  Suatu layanan yang menyediakan untuk membuat dan mengelola *certificate public key* yang digunakan untuk keamanan pada beberapa aspek salah satu diantaranya digunakan untuk proses autentikasi menggunakan EAP.

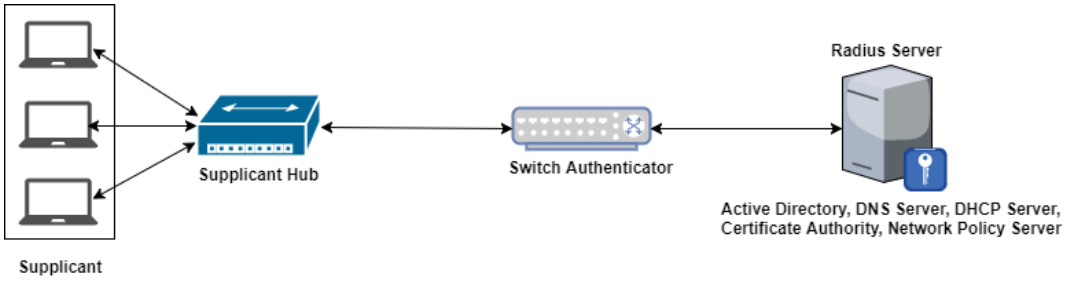
- Wireshark

  Wireshark adalah paket *analyzer* jaringan yang digunakan untuk menangkap paket jaringan dan menampilkan data paket secara rinci. Hal

Ini digunakan untuk memecahkan masalah jaringan, memeriksa masalah keamanan, implementasi protokol dan *debugging*. Untuk memantau pesan EAP yang mengalir di server autentikasi dan *supplicant*.

4.2 Gambaran Umum Proses Autentikasi

Proses autentikasi mode multi-auth yang diimplementasikan adalah berbasis *script* yang dikonfigurasi di dalam authenticator switch *manageable* yang mendukung standard IEEE 802.1X dan radius server sebagai *passive* server yang menerima data dari authenticator melalui protokol radius untuk mengetahui berhasil dan tidak berhasil dalam proses autentikasi. Gambaran umum topologi jaringan yang diimplementasikan dapat dilihat pada Gambar 4.1.

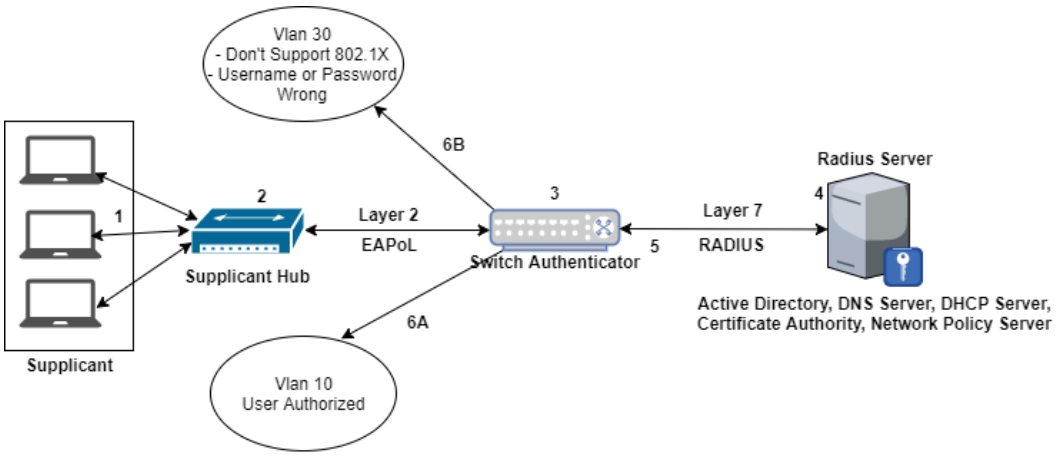


Gambar 4.1 Gambaran umum topologi jaringan mode multi-auth

Dari Gambar 4.1 ada beberapa komponen yang terlibat yaitu *supplicant*, *supplicant* hub, switch authenticator, dan radius server. *supplicant* merupakan perangkat yang akan melakukan autentikasi yang mengirimkan kredensial *supplicant* yang sesuai dengan *user* yang ada di active directory server. *Supplicant* hub merupakan perangkat perpanjangan dari *supplicant* agar nantinya mode multi-auth dapat diketahui secara fungsional berhasil atau tidaknya dalam pengimplementasiannya. Switch authenticator merupakan switch yang berperan sebagai perangkat akses jaringan yang memfasilitasi proses autentikasi dengan menyampaikan kredensial *supplicant* ke radius server. Radius server adalah server yang memvalidasi kredensial yang dikirimkan oleh *supplicant* dan menentukan hak akses jaringan apa yang akan diterima oleh *supplicant*.

4.3 Perancangan Topologi Autentikasi Jaringan

Perancangan topologi autentikasi mode multi-auth, jaringan dibuat dengan kondisi terdapat 3 komputer fisik sebagai *supplicant*, *supplicant* hub, authenticator switch dan radius server. Topologi pada Gambar 4.2 digunakan untuk melakukan implementasi dan pengujian pada penelitian ini.



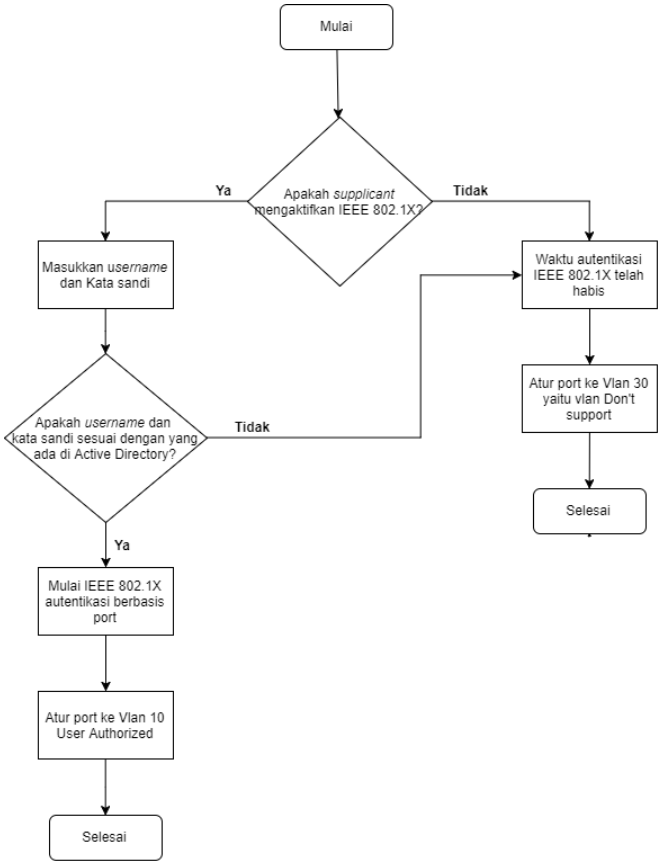
Gambar 4.2 Topologi jaringan mode *multi-auth*

Penjelasan topologi:

1. *Supplicant* mengaktifkan atau tidak protokol IEEE 802.1X pada sistem operasi perangkat pengguna jaringan untuk melakukan autentikasi pada jaringan lokal lalu mengirimkan trafik EAPoL ke *supplicant* hub.
2. *Supplicant* hub menerima trafik EAPoL dari *supplicant*, kemudian meneruskan trafik EAPoL yang diberikan *supplicant* ke switch authenticator.
3. Switch authenticator menerima trafik EAPoL dari *supplicant* selanjutnya switch authenticator me-*request* kredensial *username* dan kata sandi dari *supplicant* kemudian diteruskan ke radius server dengan me-rencapsulasi trafik EAP menjadi RADIUS lalu me-*relay*-kan ke radius server.
4. Radius server bertindak sebagai penentu apakah suatu *supplicant* valid atau tidak dalam mengakses jaringan.
5. Switch authenticator menerima hasil dari radius server, kemudian switch authenticator mengeksekusi apakah *supplicant* dapat mengakses jaringan lokal atau tidak.
6. *Supplicant* mendapat alamat IP dari salah satu VLAN yang dikonfigurasi.

4.4 Diagram Alir Autentikasi

Pada tahap perancangan diperlukan diagram alir autentikasi, dimana yang berguna untuk membantu mengetahui jalannya sistem autentikasi sesuai dengan skenario yang telah dirancang. Diagram alir pada Gambar 4.3 ini digunakan untuk mengetahui alur proses autentikasi dalam mengakses jaringan.



Gambar 4.3 Diagram alir autentikasi

Penjelasan diagram alir:

- *Supplicant* mengaktifkan atau tidak protokol IEEE 802.1X pada sistem operasi perangkat pengguna jaringan untuk melakukan autentikasi pada jaringan lokal.
- Jika *supplicant* tidak mengaktifkan protokol IEEE 802.1X pada sistem operasinya maka proses autentikasi dengan memasukkan *username* dan kata sandi tidak akan terjadi dikarenakan proses autentikasi memerlukan pengaktifan IEEE 802.1X, sehingga akan menunggu sampai waktu proses autentikasi yang diberikan switch authenticator habis kemudian *supplicant* akan diarahkan ke VLAN jaringan Don't Support.
- Jika *supplicant* mengaktifkan protokol IEEE 802.1X pada sistem operasinya maka proses autentikasi dengan memasukkan *username* dan kata sandi akan dilakukan.
- Ketika *username* dan kata sandi dikirim, switch authenticator selanjutnya meneruskan ke radius server. Radius server memeriksa apakah *username* dan kata sandi yang dimasukkan *supplicant* benar sesuai dengan pengguna yang ada di active directory.
- Jika *username* dan kata sandi yang dimasukkan *supplicant* adalah salah maka akan menunggu sampai waktu proses autentikasi yang diberikan

switch authenticator habis kemudian *supplicant* akan diarahkan ke VLAN jaringan Don't Support.

- Jika *username* dan kata sandi yang dimasukkan *supplicant* adalah benar maka autentikasi berbasis port berhasil dan mengizinkan *supplicant* mengakses jaringan lokal. *Supplicant* mendapat alamat IP dari VLAN 10 yang dikonfigurasi yang sesuai dengan pengguna yang dimasukkan.

4.5 Perancangan Skenario Pengujian

Terdapat tiga skenario pengujian yang dilakukan untuk mengukur waktu autentikasi host-mode. Adapun parameter uji setiap skenario yang digunakan antara lain mengukur perbandingan waktu autentikasi yang berhasil dan mengukur waktu autentikasi yang tidak berhasil dari mode single-host dengan multi-auth.

Dalam mengukur waktu autentikasi yang berhasil dan tidak berhasil, maka setiap host-mode memiliki masing-masing empat parameter yang digunakan sebagai parameter pengujian diantaranya untuk mode single-host ada mode "Single-host tunggal berhasil", "Single-host ganda berhasil", "Single-host tunggal tidak berhasil", "Single-host ganda tidak berhasil". Untuk mode multi-auth ada mode "Multi-auth tunggal berhasil", "Multi-auth ganda berhasil", "Multi-auth tunggal tidak berhasil", "Multi-auth ganda tidak berhasil".

4.5.1 Skenario Pengujian Integritas Pengiriman Data

Pengujian ini menggunakan algoritma enkripsi RSA dan algoritma SHA untuk hashing data yang bertujuan untuk mengetahui berhasil atau tidak berhasilnya enkripsi dan hashing integritas kredensial data yang dikirim.

4.5.2 Skenario Pengujian Mode Multi-Auth

Implementasi terdiri dari *supplicant*, *supplicant* hub, authenticator dan server autentikasi. *Supplicant* terhubung ke *supplicant* hub menggunakan kabel unshielded twisted pair (RJ45). *Supplicant* hub terhubung ke authenticator menggunakan kabel RJ45. Authenticator terhubung ke server autentikasi menggunakan kabel RJ45.

Dalam skenario ini, waktu autentikasi mode multi-auth yang digunakan dihitung dalam jaringan kabel. Untuk menghitung waktu autentikasi menggunakan *tool* Wireshark. Waktu autentikasi menyediakan total waktu yang dibutuhkan *supplicant* untuk mendapatkan autentikasi di jaringan. Pengujian berdasarkan perbandingan waktu autentikasi berhasil dan perbandingan waktu autentikasi tidak berhasil, dengan menggunakan *capture* waktu di mode multi-auth, waktu autentikasi dihitung dengan menggunakan rumus yang ada pada BAB 2 sub-bab 2.7.

4.5.3 Skenario Pengujian Mode Single-Host Dengan Multi-Auth

Dalam skenario ini, membandingkan waktu autentikasi mode single-host dan multi-auth. Pengujian berdasarkan perbandingan "waktu autentikasi tunggal

berhasil", "waktu autentikasi ganda berhasil", "waktu autentikasi tunggal tidak berhasil", "waktu autentikasi ganda tidak berhasil" dan "waktu autentikasi mode single-host dengan multi-auth" dengan menggunakan rumus yang ada pada BAB 2 sub-bab 2.7.