LAMPIRAN

Pada lampiran ini akan dibahas tentang implementasi autentikasi mode *multi-auth* pada jaringan *local area network* berbasis kabel menggunakan protokol IEEE 802.1X dan radius server

1. Sistem Keamanan Autentikasi Menggunakan Protokol IEEE 802.1X

Konfigurasi menggunakan Protected Extensible Authentication Protokol (PEAP) dengan Microsoft Challenge Handshake Authentication Protokol (MS-CHAP) version 2 di jaringan berbasis kabel dengan Microsoft Network Policy Server (NPS) sebagai Radius Server.

Kebutuhan komponen untuk mengimplementasikan *prototype* ini adalah:

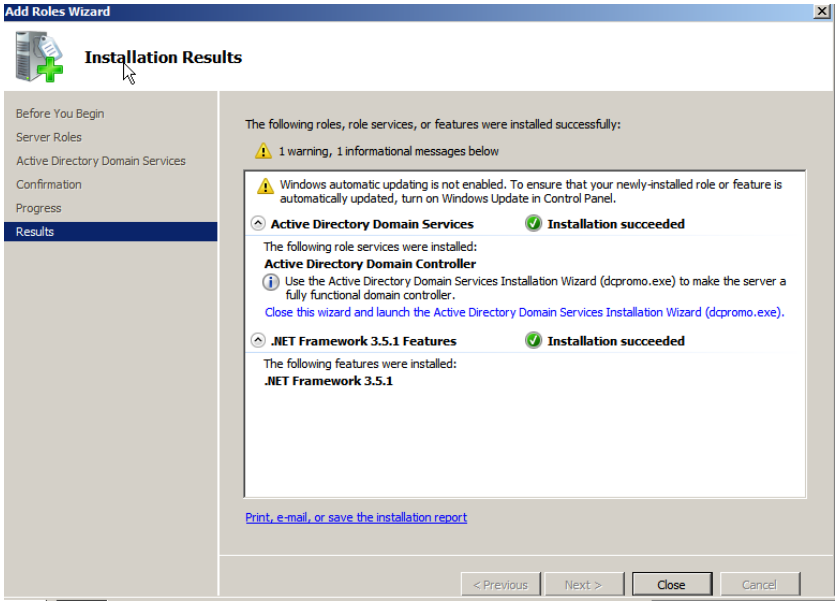
- Windows 2008 Enterprise Server dengan layanan Active Directory (AD), Certificate Authority (CA), Dynamic Host Control Protokol (DHCP), Domain Name System (DNS) dan Network Policy Server (NPS).
- *Managed* Switch Cisco Catalyst yang support protokol IEEE 802.1X.
- Microsoft Windows 10 sebagai *Supplicant* atau *suplicant*.

2. Konfigurasi Microsoft Windows Server 2008

2.1. Install dan Konfigurasi ADDS dan DNS Server

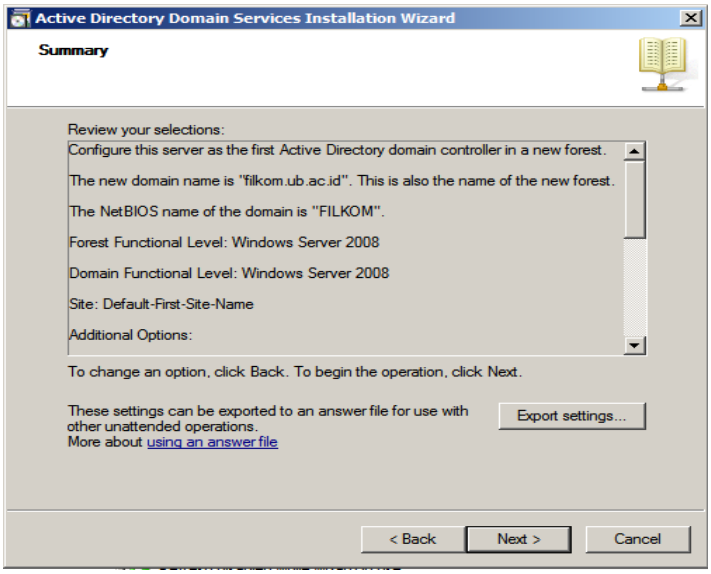
Install dan konfigurasi Domain Controller yang digunakan sebagai Active Directory. Langkah-langkah konfigurasi server Microsoft Windows 2008 sebagai Domain Controller:

1. Ubah jaringan yang ada di *Local Area Connection* menjadi IP Static.pilih “Start” kemudian pilih “Server Manager”, kemudian pilih “roles”, lalu pilih “Add Roles”.
2. Muncul informasi sebelum melakukan instalasi layanan yang ada.
3. Install layanan “Active Directory Domain Services”, maka ada fitur “Net Framework” yang dibutuhkan untuk install layanan tersebut. Lalu pilih “Add Required Features” untuk melakukan instalasi Net-Framework.
4. Setelah melakukan instalasi kebutuhan sebelumnya maka lanjutkan instalasi layanan, Pilih “Close this wizard and launch the Active Directory Domain Services Instalation Wizard (dcpromo.exe)” untuk melanjutkan instalasi dan konfigurasi dari Active Directory seperti pada Gambar lampiran 1.



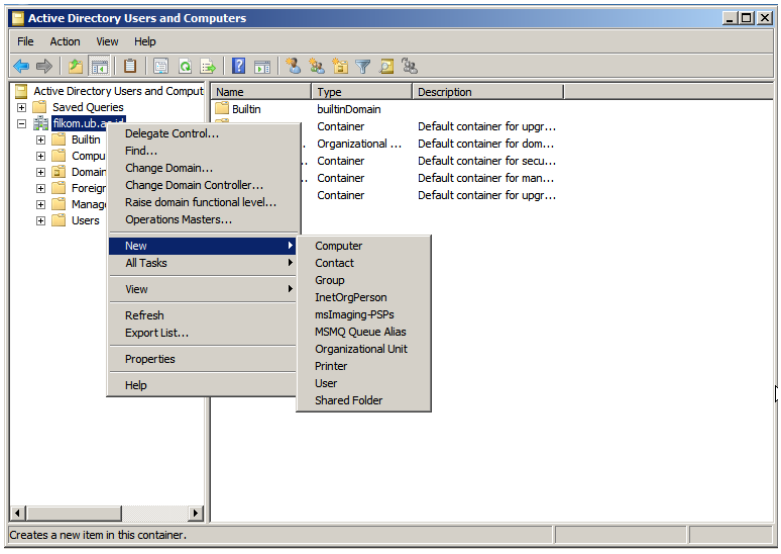
Gambar lampiran 1 Add Roles Wizard - Result

5. Pilih “Create a new domain in a new forest” dan pilih “Next” untuk membuat sebuah domain baru.
6. Masukkan nama DNS yang diinginkan untuk domain baru (contohnya filkom.ub.ac.id) dan pilih “Next”.
7. Pilih *Forest Functional Level* untuk domain yang diinginkan (contohnya windws server 2008 R2) dan pilih “Next”.
8. Pilih *Domain Functional Level* untuk domainnya dan pilih “Next”.
9. Pastikan DNS Server “tercentang”, kemudian pilih “Next”.
10. Pilih folder Active Directory file yang digunakan dan pilih “Next”.
11. Masukkan Kata sandi Administrator dan pilih “Next”.
12. Lalu periksa kembali pilihan yang sudah dibuat, dan pilih “Next” untuk menyelesaikan konfigurasi “Active Directory Domain Services”.



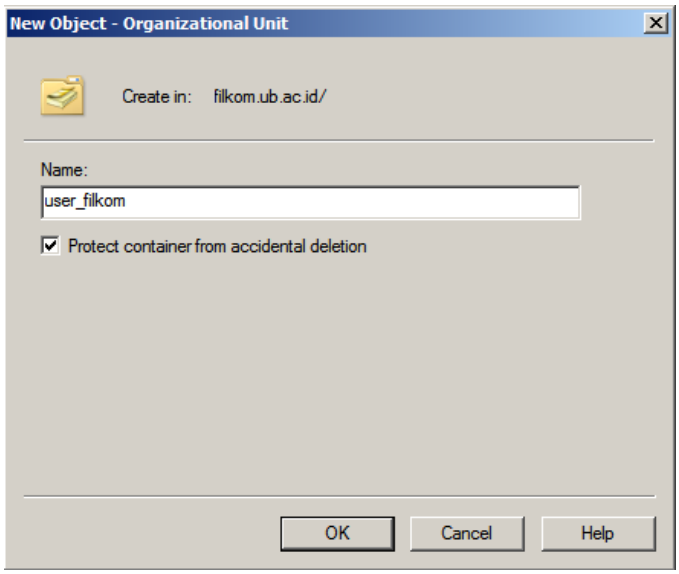
Gambar lampiran 2 Active Directory Domain Services - Summary

13. Selanjutnya, buat user di Active Directory yang akan digunakan sebagai kredensial autentikasi ke jaringan. Pilih “Start”, kemudian “administrative Tools”, pilih “Active Directory Users and Computers”.
14. Pilih domain, contoh disini filkom.ub.ac.id, klik kanan “filkom.ub.ac.id” pilih “New” lalu pilih “Organizational Unit”, organizational unit berfungsi untuk membuat sebuah grup active directory yang nantinya digunakan untuk tempat user kredensial berada seperti pada Gambar lampiran 3.



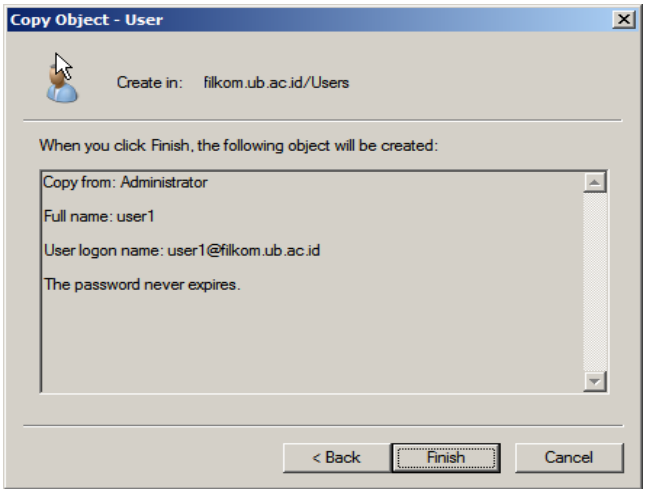
Gambar lampiran 3 Active Directory Users and Computers - Organizational Unit

15. Masukkan nama foldernya contohnya “User_filkom”, lalu pilih “Ok” seperti pada Gambar lampiran 4.



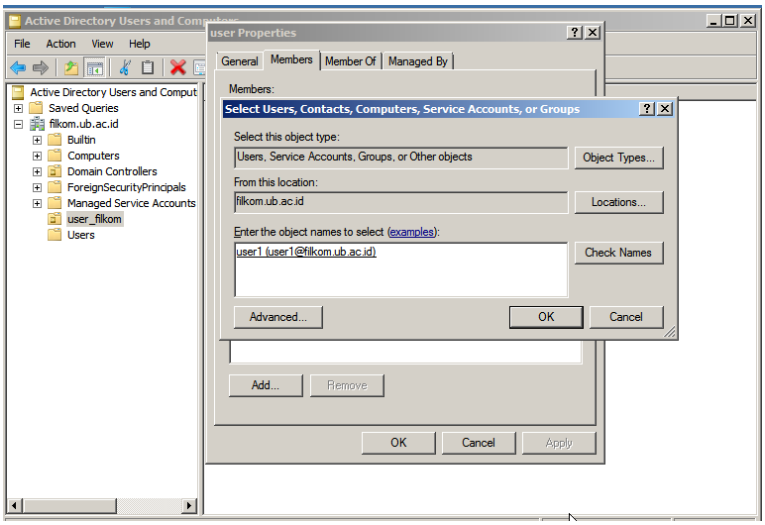
Gambar lampiran 4 Organizational Unit – New Object

16. Setelah folder user dibuat, maka selanjutnya adalah buat user yang nantinya akan digunakan sebagai user autentikasi.
17. Isi data user sesuai dengan kebutuhan, kemudian pilih “Next”.
18. Masukkan kata sandi dan centang hal yang diinginkan, kemudian pilih “Next”.
19. Informasi terkait user yang sudah dibuat. Bila sesuai dengan keinginan pilih “Finish” seperti pada Gambar lampiran 5.



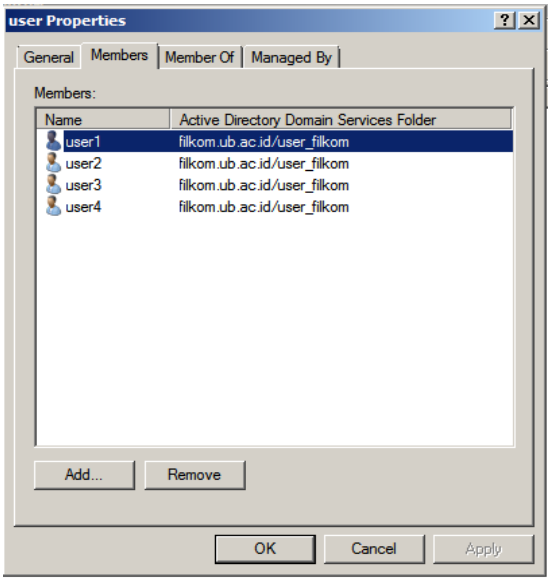
Gambar lampiran 5 buat user – Finish

20. Buat user sebanyak yang diinginkan, disini saya membuat 4 user.
21. Buat grup yang diinginkan, disini saya isi nama grup nya “user”, karena nantinya semua user user, akan di masukkan ke dalam group.
22. Masukkan user yang diinginkan seperti pada Gambar lampiran 6.



Gambar lampiran 6 Pilih Users

23. Lakukan kepada 3 *user* selanjutnya maka semua *user* masuk kedalam grup tersebut di dalam “user Properties”, lalu pilih “Apply” kemudian pilih “Ok” seperti pada Gambar lampiran 7.



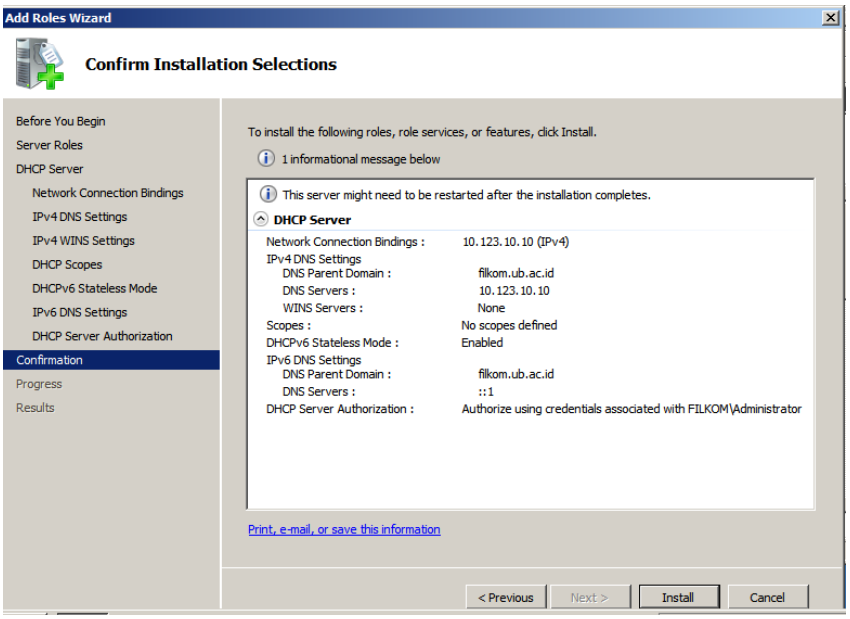
Gambar lampiran 7 user Properties

24. Maka user yang ada di active directory sudah dibuat dan dimasukkan ke grup user.

2.2 Install dan Konfigurasi Dynamic Host Control Protokol (DHCP)

Layanan DHCP pada Windows Server 2008 digunakan untuk memberikan alamat IP kepada *supplicant* atau pengguna jaringan local berbasis kabel. Berikut langkah – langkah untuk menginstal dan mengkonfigurasi layanan DHCP:

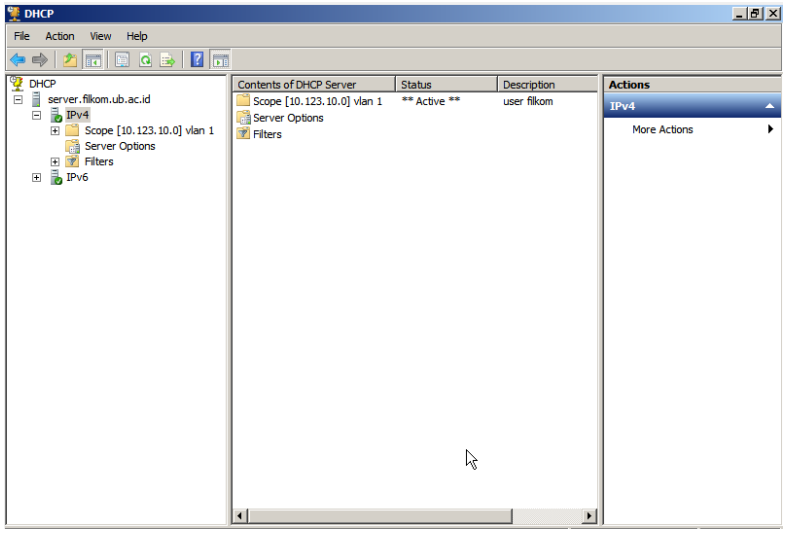
1. Pilih layanan “DHCP Server”, kemudian pilih “Next”.
2. Pilih interface DHCP Server yang digunakan untuk memonitor dan pemberian alamat IP yang diminta, dan kemudian pilih “Next”.
3. Konfigurasi pengaturan *default* DNS DHCP Server yang akan disediakan ke *supplicant* dan kemudian pilih “Next”.
4. Pilih “Add” untuk menggunakan wizard dalam membuat DHCP *Scope* atau pilih “Next” untuk belakangan membuat DHCP *Scope,* kemudian pilih “Next” untuk melanjutkan.
5. Enable atau disable DHCPv6 di server bila dibutuhkan, kemudian pilih “Next”.
6. Sediakan kredensial domain administrator untuk mengotorisasi DHCP Server di Active Directory, dan pilih “Next”.
7. Tinjau kembali konfigurasi yang sudah dibuat kemudian pilih “Install” untuk menyelesaikan instalasi ini seperti pada Gambar lampiran 8.



Gambar lampiran 8 DHCP Server – Confirmation

8. Selanjutnya buat 2 jaringan yang terbagi atas 2 scope alamat IP yang nantinya akan didapatkan oleh *supplicant* ketika selesai melakukan autentikasi. IP yang di dapat di tentukan dari proses autentikasinya.
9. Buka “DHCP Server” Pilih server DHCP contohnya server.filkom.ub.ac.id, lalu klik kanan “IPv4”, kemudian Pilih “New Scope..”.

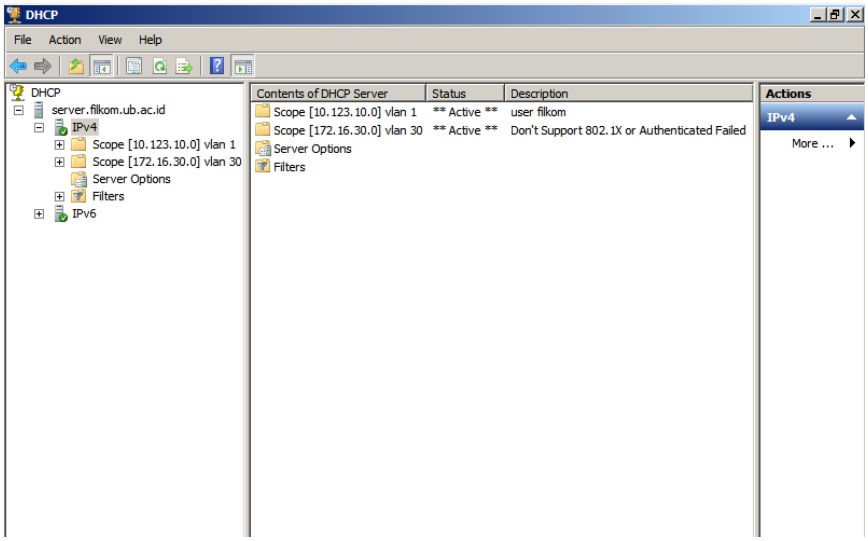
10. Masukkan nama scope yang diinginkan yang nantinya akan digunakan sebagai penanda scope tersebut, lalu masukkan deskripsi dari scope tersebut, untuk deskripsi adalah opsional.
11. Masukkan rentang alamat IP yang ingin didistribusikan sesuai dengan keinginan, dan tentukan subnet mask yang diinginkan juga. Contohnya sebagai berikut. Kemudian pilih “Next”.
12. Selanjutnya adalah rentang alamat IP yang tidak ingin didistribusikan ke *Supplicant*, ini adalah opsional, tergantung dari keinginan sendiri. Disini penulis memilih mengosongkan rentang alamat IP, karena alamat IP akan di pakai semua untuk didistribusikan ke *supplicant*. Kemudian pilih “Next”.
13. Untuk “Lease Duration” dikembalikan ke masing – masing anda, untuk berapa lama *supplicant* dapat menggunakan alamat IP yang sudah didistribusikan dari Scope. Kemudian pilih “Next”.
14. Berikut adalah informasi opsi konfigurasi DHCP supaya *supplicant* dapat menggunakan scope ini. Disini saya kemudian pilih “Yes. I want to configure these option now”. Kemudian pilih “Next”.
15. Isi alamat IP gateway yang nantinya untuk mendistribusikan alamat IP antara server dan *supplicant*. Kemudian pilih “Next” .
16. Akan muncul Domain Name and DNS Servers yang nantinya digunakan oleh *supplicant* untuk proses autentikasi, dan pastikan alamat IP dari server adalah benar. Bila salah nanti akan mempengaruhi dalam distribusi alamat IP.
17. Selanjutnya adalah aktivasi scope yang telah dibuat. Pilih “Yes, I want to activate this scope now”.
18. Kemudian pilih untuk menyelesaikan pembuatan scope.
19. Maka scope VLAN 10 sudah dibuat seperti pada Gambar lampiran 9.



Gambar lampiran 9 Scope VLAN 10

20. Lakukan langkah yang sama untuk membuat scope alamat IP yang lainnya sesuai dengan kebutuhan. Disini penulis membuat 2 scope yang nantinya

akan digunakan untuk penentuan autentikasi berdasarkan "user authentication" yang diinputkan oleh *supplicant* seperti pada Gambar lampiran 10.



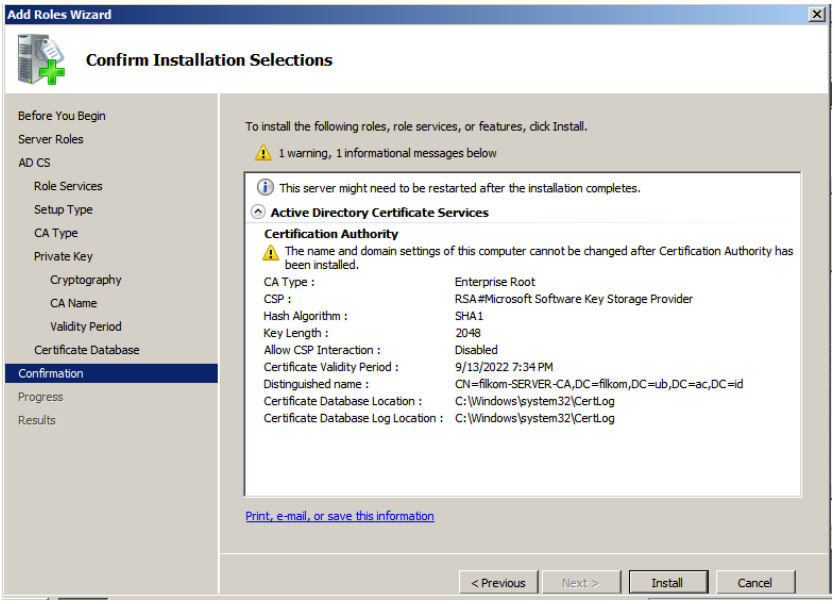
Gambar lampiran 10 Semua Scope VLAN

2.3 Install dan Konfigurasi Certificate Authority (CA)

EAP-PEAP memvalidasi server RADIUS berdasarkan sertifikat yang ada di server. Selain itu, sertifikat server harus dikeluarkan oleh CA publik yang dipercaya oleh komputer *supplicant* (yaitu sertifikat CA publik sudah ada di folder *Trusted Root Certification Authority* di computer *supplicant certificate store*). Berikut langkah-langkah untuk mengkonfigurasi Microsoft Windows server 2008 sebagai server CA yang mengeluarkan sertifikat ke NPS:

1. Pilih layanan "Active Directory Certificate Services" pada "Server Manager" dan pilih "Next".
2. Pilih "Certification Authority" kemudian pilih "Next".
3. Pilih "Enterprise" dan pilih "Next".
4. Pilih "Root CA" dan pilih "Next".
5. Pilih "Create a new private key" dan pilih "Next".
6. Pilih "Next" pada saat konfigurasi Cryptography untuk CA.
7. Pilih "Next" untuk menerima *default common name* untuk CA.
8. Pilih 5 tahun untuk lama waktu validnya sertifikat CA, kemudian pilih "Next".
9. Pilih next untuk lokasi *default Certificate database*.

10. Periksa kembali konfigurasi yang sudah dipilih, dan pilih “install” pada “Confirm Installation Selections” untuk melakukan instalasi Active Directory Certificate Services seperti pada Gambar lampiran 11.

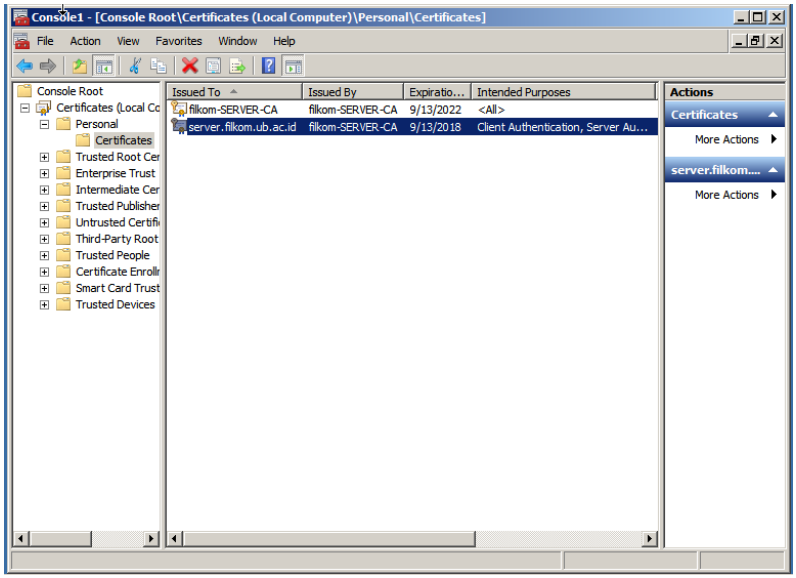


Gambar lampiran 11 Active Directory Certificate Services - Confirmation

11. Instalasi sertifikat CA

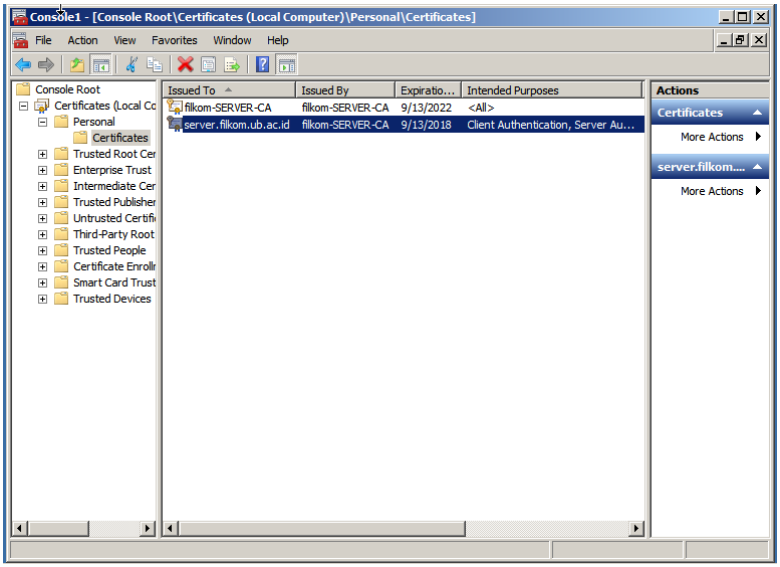
Berikut langkah – langkah untuk instalasi sertifikat computer untuk NPS:

1. Buka program Microsoft Management Console (mmc), pilih “File”, kemudian “Add/Remove Snap-in”.
2. Pilih “Certificates”, dan pilih “Add” kemudian pilih “Computer Account”, dan pilih “Next”.
3. Pilih “Local Computer”, dan pilih “Finish”.
4. Click “OK” untuk kembali ke Microsoft Management Console (mmc).
5. Pilih “Certificates (Local Computer)” selanjutnya pilih “Trusted Root Certification Authorities” folder, kemudian pilih “Certificates”. Temukan “filkom-SERVER-CA” di daftar tersebut. Bila sudah ada maka implementasi sertifikat berhasil seperti pada Gambar lampiran 12.



Gambar lampiran 12 Certificates - filkom-SERVER-CA

6. Kemudian pilih “Certificates (Local Computer)” selanjutnya pilih “Personal” folder, pilih “Certificates”. Klik kanan di kolom putih CA sertifikat, kemudian pilih “All Tasks” kemudian pilih “Request New Certificate”. Pilih “Next” untuk sertifikat *Enrollment*.
7. Pilih “Finish” ketika instalasi berhasil, maka sertifikat NPS sudah terinstall.
8. Pastikan sertifikat membaca autentikasi *supplicant* dan autentikasi server seperti pada Gambar lampiran 13.

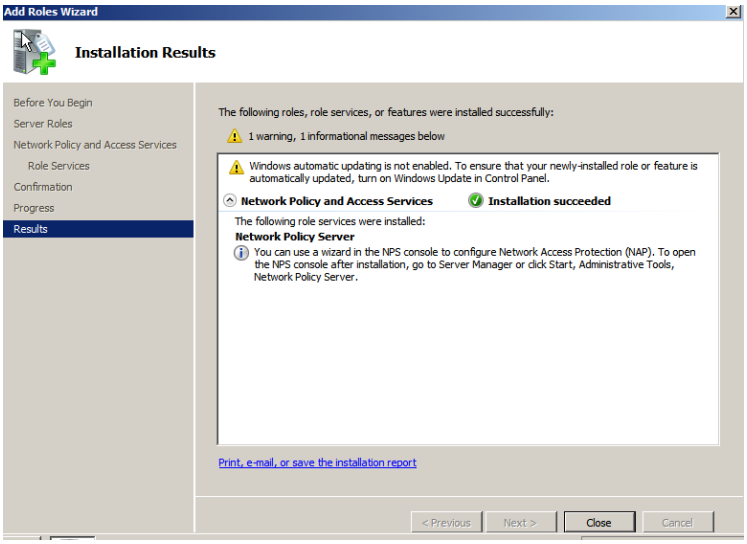


Gambar lampiran 13 Console Root personal certificate

2.4 Install Network Policy Server (NPS)

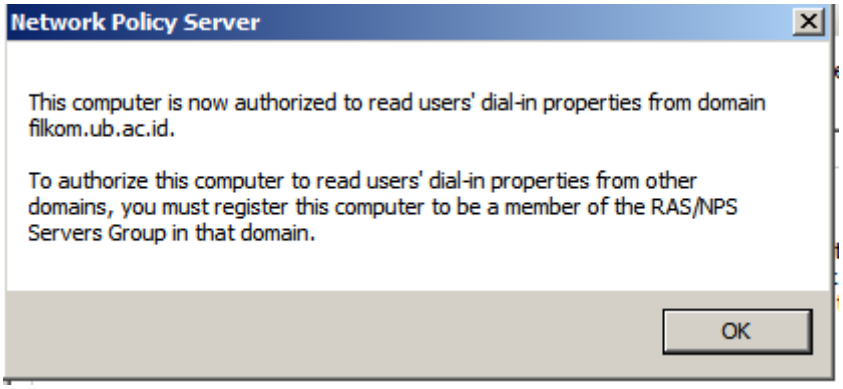
Dalam konfigurasi ini, NPS digunakan sebagai server RADIUS untuk mengautentikasi *supplicant* berbasis kabel dengan autentikasi PEAP. Berikut langkah-langkah untuk menginstal dan mengkonfigurasi NPS di Windows server 2008:

1. Pilih “Start” kemudian “Server Manager”, pilih “Roles” kemudian “Add Roles”, pilih “Network Policy and Access Services” dan pilih “Next”.
2. Pilih “Network Policy Server”, kemudian pilih “Next”.
3. Sebelum instalasi periksa kembali konfimasi pemilihan instalasi dan kemudian pilih “Install”.
4. Setelah instalasi selesai, maka akan muncul pemberitahuan keberhasilan instalasi “Network Policy Server” seperti berikut, kemudian pilih “Close” untuk menutup instalasi seperti pada Gambar lampiran 14.



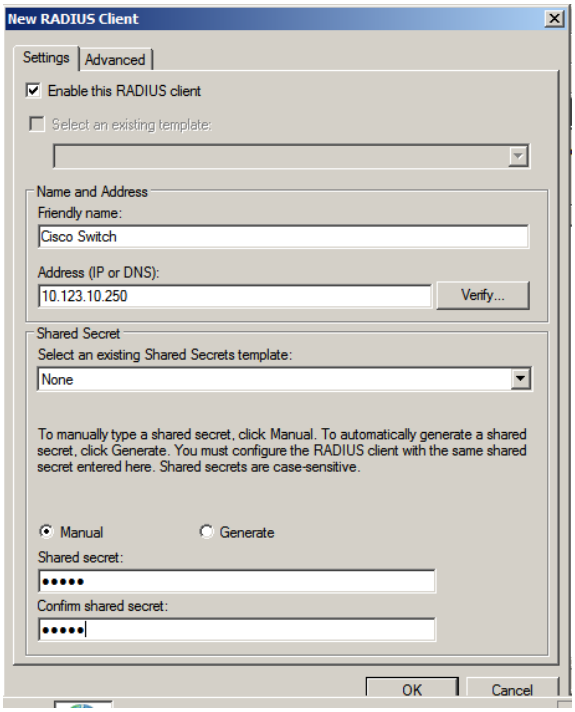
Gambar lampiran 14 Instalasi Network Policy Server

5. Kemudian buka Network Policy Server. Lakukan registrasi Network Policy Server dengan Active Directory yang sudah dibuat, supaya proses autentikasi menggunakan *username* dan kata sandi *user* yang ada di Active directory. Klik kanan “NPS (Local)” lalu pilih “Register Server in Active Directory”.
6. Kemudian muncul pemberitahuan untuk meregister NPS dengan Active Directory yang ada di domain controller seperti pada Gambar lampiran 15.



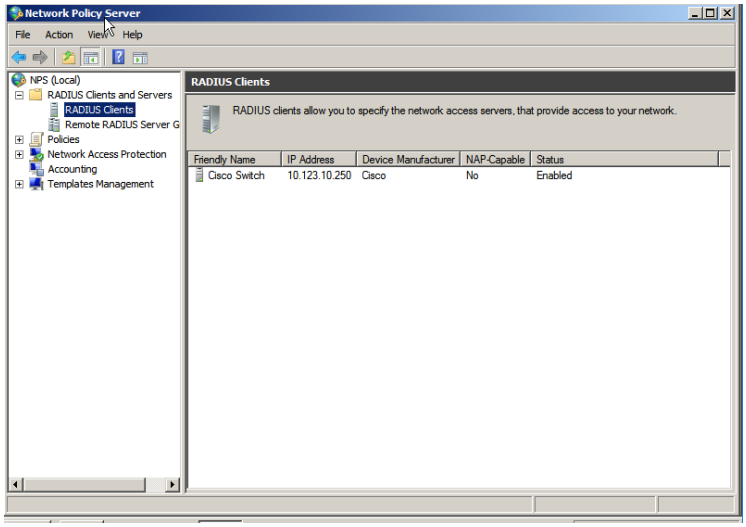
Gambar lampiran 15 Network Policy Server – Register NPS dengan Active Directory

7. Setelah diregistrasi, buat radius *client* dimana berfungsi sebagai penghubung antara *supplicant* dan server yang nantinya akan dipasang atau dikonfigurasi di switch. Pilih "RADIUS Clients and Servers".
8. Isi sesuai dengan keinginan, pastikan "Address (IP or DNS)" sesuai dengan gateway dari server, lalu lakukan "verify" untuk mengetahui valid atau tidaknya IP tersebut. Kemudian isi "shared secret" yang nantinya berfungsi sebagai passwork untuk koneksi antara switch dan radius *supplicant* seperti pada Gambar lampiran 16.



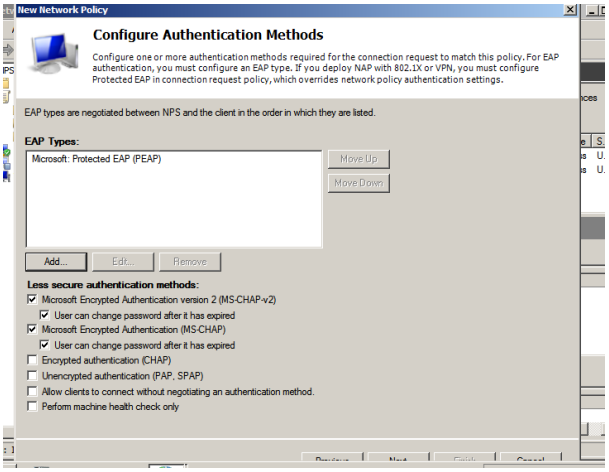
Gambar lampiran 16 Radius Client

9. Setelah diisi, lalu pilih “OK” maka radius *client* sudah terbuat seperti pada Gambar lampiran 17.



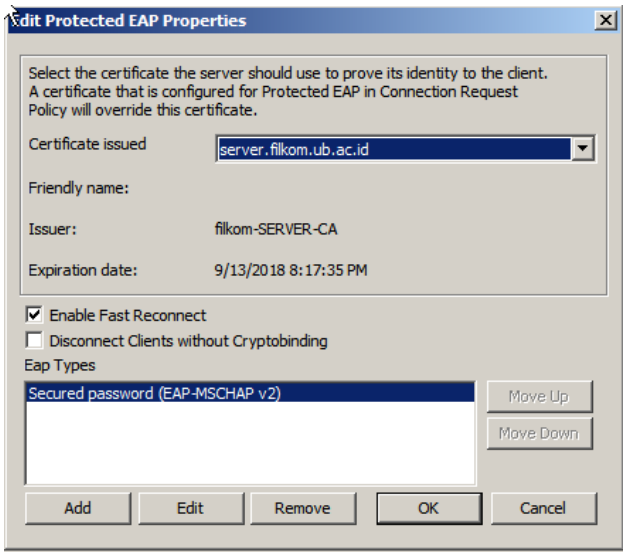
Gambar lampiran 17 Radius Client

10. Sekarang saatnya konfigurasi “Network Policies” yang nantinya digunakan sebagai autentikasi user akan diarahkan ke posisi VLAN yang diotorisasi oleh kredensial user. Pilih “Policies”, kemudian klik kanan “Network Policies”, pilih “New”.
11. Isi policy name sesuai dengan keinginan anda, pastikan bila kita ingin mengakses jaringan server menggunakan 802.1X pastikan, “Type of network access server adalah Unspecified”.
12. Kemudian kita membutuhkan kondisi apa yang diinginkan untuk melakukan permintaan koneksi. Dengan kata lain kita harus memasukkan kondisi user group apa yang bisa mengakses VLAN 10 dan menggunakan Ethernet secara fisik untuk melakukan koneksi. Pilih “add”.
13. Pilih “Access Granted” bila koneksi cocok dengan kondisi kebijakan yang telah diterapkan. Kemudian pilih “Next”.
14. Konfigurasi metode autentikasi EAP yang diinginkan, pilih “Add”, kemudian pilih “Microsoft: Protected EAP (PEAP)”, pilih “OK”. Maka metode autentikasi sudah terpilih seperti pada Gambar lampiran 18.



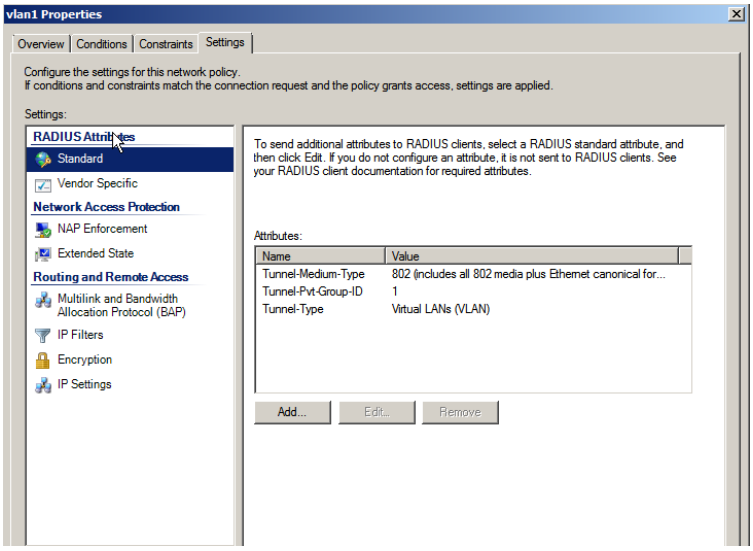
Gambar lampiran 18 EAP Types

15. Lalu pilih “Edit”, untuk melakukan pengecekan sertifikat autentikasi yang sudah dibuat sebelumnya sudah dapat digunakan. Kemudian pilih “OK” seperti pada Gambar lampiran 19.



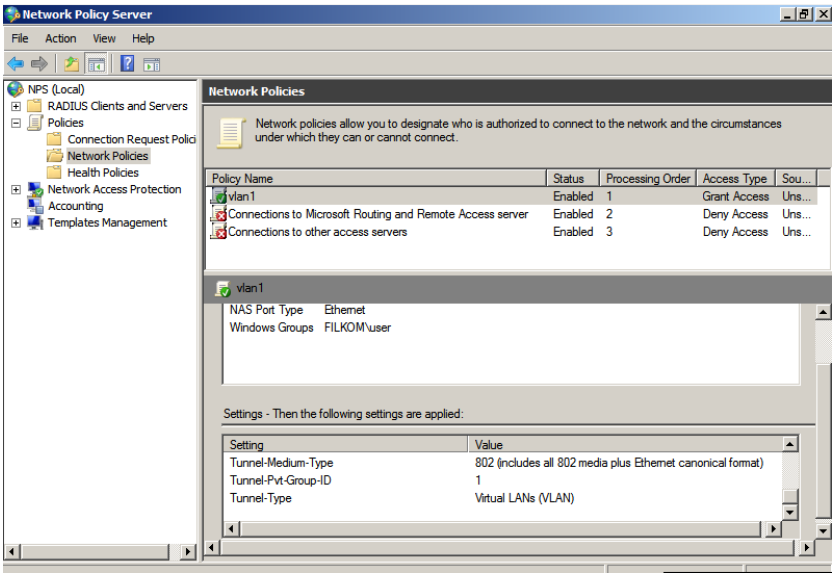
Gambar lampiran 19 Edit Protected EAP Properties

16. Pastikan pengaturan konfigurasi dalam “RADIUS Attributes” standard seperti gambar dibawah. Dimana kita menggunakan VLAN, dan protokol 802, serta VLAN 10 yang digunakan bila user grup tersebut melakukan autentikasi. Kemudian pilih “Next” dan konfigurasi NPS untuk user grup user sudah selesai seperti pada Gambar lampiran 20.



Gambar lampiran 20 RADIUS Attributes Standard

17. Konfigurasi NPS untuk grup user sudah selesai. Berikut Network Policy yang telah dibuat pada Gambar lampiran 21.



Gambar lampiran 21 Network Policy

3. Konfigurasi Switch untuk mengaktifkan protokol IEEE 802.1X

Mengkonfigurasi Cisco Switch, membuat VLAN 1 sebagai gateway, VLAN 10 untuk *user authorized* dan 30 untuk Guess. Pada antarmuka VLAN 10 dan 30 kita perlu mengkonfigurasi DHCP relay. Aktifkan autentikasi 802.1X pada switch dan port switch. Bila *supplicant* terhubung ke port, switch akan meminta pengguna untuk melakukan autentikasi.

1. Mengaktifkan AAA (Authentication, Authorization, *Accounting*) dan 802.1X pada Switch dan dialihkan ke radius server.
2. Buat VLAN seperti pada Gambar lampiran 22.

```
Switch(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/3, Gi0/4, Gi0/5
                                                Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                                Gi0/10, Gi0/11, Gi0/12
10   UserAuthenticated                active    Gi0/2
30   dontsupport                      active
```

Gambar lampiran 22 buat VLAN

3. Tetapkan alamat IP *interface* VLAN 10 untuk *supplicant* dalam mengakses gateway server dan atur alamat IP *interface* VLAN 10 sebagai gateway di server seperti pada Gambar lampiran 23.

```
interface Vlan10
 ip address 172.16.10.250 255.255.255.0
 ip helper-address 10.123.10.10
```

Gambar lampiran 23 VLAN 10

4. Atur alamat IP *interface* VLAN 30 untuk grup "Guest" dan konfigurasikan DHCP Relay pada VLAN 30 seperti pada Gambar lampiran 24.

```
interface Vlan30
 ip address 172.16.30.250 255.255.255.0
 ip helper-address 10.123.10.10
```

Gambar lampiran 24 VLAN 30

5. Aktifkan AAA di switch, seperti pada Gambar lampiran 25:

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
```

Gambar lampiran 25 Aktifkan AAA

- aaa new-model merupakan mengaktifkan AAA pada switch. Perintah ini adalah untuk memberitahu kepada switch bahwa kita memakai AAA server untuk urusan *username* dan kata sandi.
- aaa authentication dot1x default group radius merupakan perintah ini membuat sesuatu yang disebut daftar metode untuk autentikasi 802.1X. Daftar metode tidak lebih dari daftar user yang ingin diautentikasi. Kata kunci default menentukan bahwa ini adalah daftar

yang digunakan untuk semua situasi yang tidak disebutkan secara spesifik.

- aaa authorization network default group radius merupakan perintah untuk *supplicant* yang terkonfirmasi dengan *username* dan kata sandi yang ada di grup "user" di Active Directory akan diberikan VLAN sesuai dengan kebijakan yang telah di konfigurasi di server NPS.
- aaa *accounting* dot1x default start-stop group radius – untuk mengaktifkan *accounting* secara langsung tanpa harus menunggu perintah untuk dijalankan.

6. Aktifkan 802.1X pada Switch seperti pada Gambar lampiran 26.

```
dot1x system-auth-control
```

```
radius server host
 address ipv4 10.123.10.10 auth-port 1812 acct-port 1813
 key 12345
!
```

Gambar lampiran 26 Aktifkan 802.1X

- dot1x system-auth-control merupakan perintah untuk mengaktifkan 802.1X di switch secara global.
- radius server host address ipv4 10.123.10.10 auth port 1812 acct-port 1813 key 12345 merupakan perintah inilah yang mengarahkan switch ke radius server. Alamat IP merupakan alamat dari radius server, port auth adalah port UDP 1812, yang merupakan default untuk RADIUS. Port 1813 adalah port standar *accounting*. Key merupakan secret key yang diberikan switch kepada radius server. Key ini adalah secret key yang sama disaat radius server membuat radius *supplicant* di servernya.

7. Konfigurasi port berbasis autentikasi pada port GigabitEthernet 0/3 seperti pada Gambar lampiran 27.

```
interface GigabitEthernet0/5
 switchport mode access
 authentication event fail action authorize vlan 30
 authentication event no-response action authorize vlan 30
 authentication host-mode multi-auth
 authentication port-control auto
 dot1x pae authenticator
!
```

Gambar lampiran 27 konfigurasi port GigabitEthernet0/3

- Switchport mode access merupakan perintah untuk menjalankan port akses yang bekerja menggunakan protokol IEEE 802.1X yang ditujukan kepada *supplicant* untuk mengakses jaringan.

- authentication event fail action authorize VLAN 30 merupakan perintah untuk memberikan akses VLAN 30 ketika *supplicant* salah dalam memasukkan *username* atau kata sandi.
- authentication event no-respon action authorize VLAN 30 merupakan perintah untuk memberikan akses VLAN 30 ketika *supplicant* tidak mengirim atau memasukkan *username* atau kata sandi dan bisa juga *supplicant* tidak mengaktifkan protokol IEEE 802.1X-nya.
- authentication host-mode *multi-auth* merupakan perintah untuk menjalankan mode *multi-auth*
- authentication port control auto merupakan perintah untuk mengaktifkan 802.1X di interface GigabitEthernet 0/3.
- dot1x pae authenticator merupakan perintah port yang dikendalikan oleh PAE 802.1X (Port Access Entity) untuk memungkinkan (dalam status *authorized*) atau mencegah lalu lintas jaringan yang tidak diotorisasi dan masuk ke atau dari port yang dikontrol. Port yang tidak terkontrol digunakan oleh PAE 802.1X untuk mengirim dan menerima frame EAPOL.

8. Konfigurasi port berbasis autentikasi pada port GigabitEthernet 0/1 seperti pada Gambar lampiran 28.

```
interface GigabitEthernet0/1
 switchport mode access
!
```

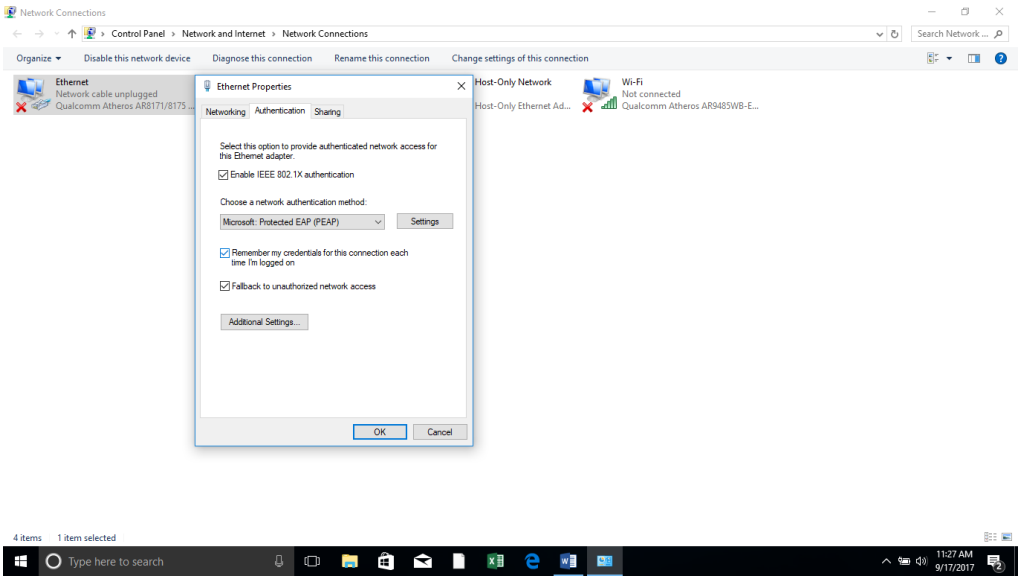
Gambar lampiran 28 konfigurasi port GigabitEthernet0/1

- Switchport mode access merupakan perintah untuk menjalankan port akses yang bekerja menggunakan protokol IEEE 802.1X yang ditujukan kepada *supplicant* untuk mengakses jaringan.

4. Mengaktifkan Protokol IEEE 802.1X di Supplicant

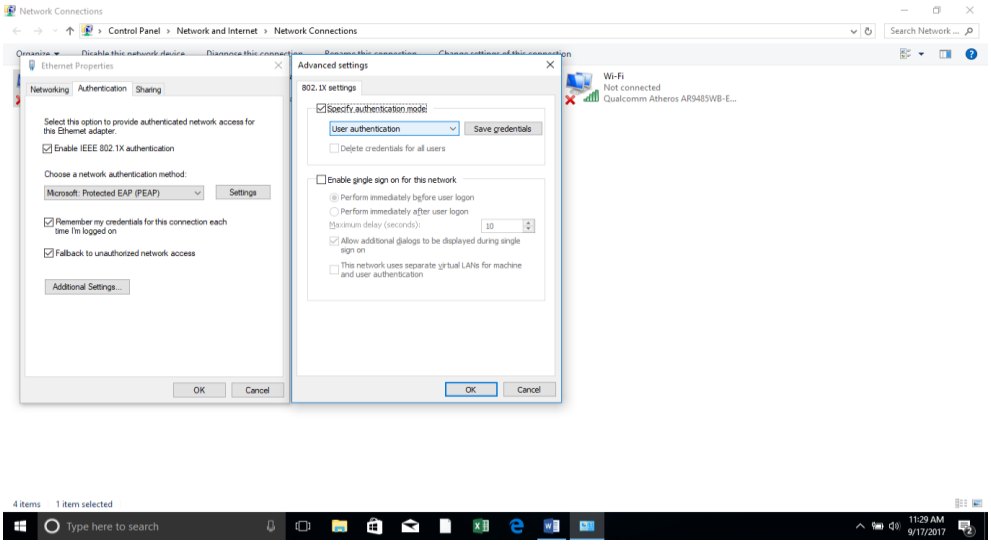
Adapun langkah – langkah untuk mengaktifkan protokol IEEE 802.1X adalah sebagai berikut:

1. Aktifkan “Wired AutoConfig”, pada “Services (Local)” secara otomatis.
2. Aktifkan IEEE 802.1X pada Ethernet “Local Area Connection”.
3. Pilih Bar “Authentication”, centang “Enable IEEE 802.1X authentication”, pastikan metode autentikasi adalah PEAP seperti pada Gambar lampiran 29.



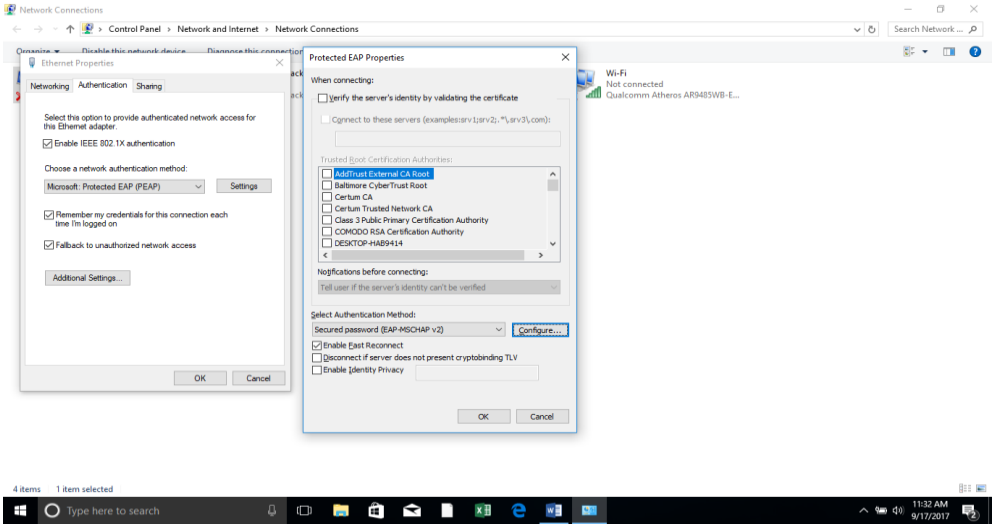
Gambar lampiran 29 Ethernet - Aktifkan IEEE 802.1X

4. Kemudian pilih "Additional Settings…", centang "Specify authentication mode", pilih "User authentication", lalu pilih "OK" seperti pada Gambar lampiran 124.



Gambar lampiran 30 User authentication

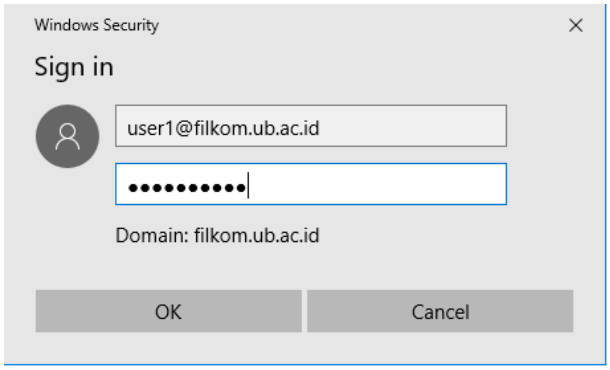
5. Lalu pilih "Settings" yang berada di samping metode autentikasi, pastikan "select authentication method" merupakan EAP-MSCHAP V2. Lalu pilih "OK" seperti pada Gambar lampiran 31.



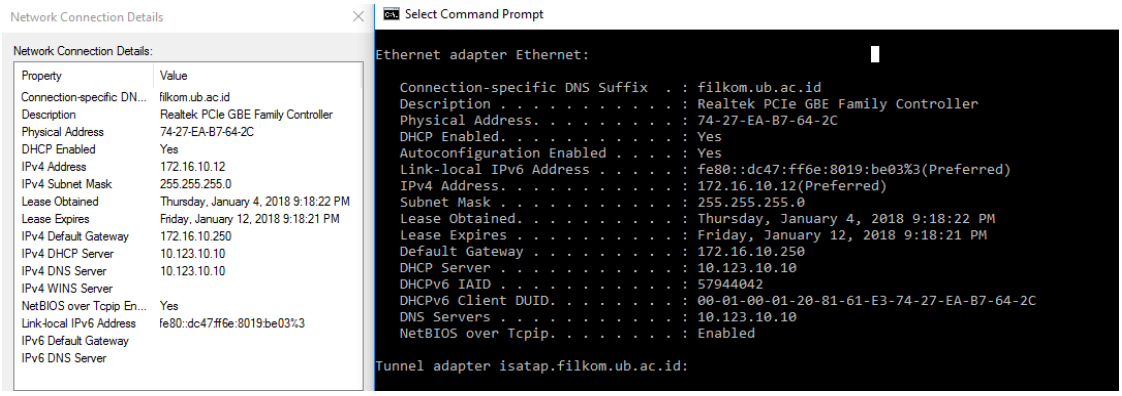
Gambar lampiran 31 Protected EAP Properties – EAP-MSCHAP V2

6. Maka konfigurasi *supplicant* sudah siap untuk melakukan proses autentikasi dengan server menggunakan protokol IEEE 802.1X

5. Proses Autentikasi 802.1X



Gambar lampiran 32 Logon Autentikasi



Gambar lampiran 33 Pengalokasian Alamat IP