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.

y Object - User		×
Create in: filkom.ub.a	ic.id/Users	
When you click Finish, the following	g object will be created:	
Copy from: Administrator		A
Full name: user1		
User logon name: user1@filkom.ub	b.ac.id	
The password never expires.		
		-
	< Back Finish	Cancel

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.

Active Directory Users and Com	user Properties	? ×	<u>_ </u>
File Action View Help	General Members Member Of Managed By		
🗇 🔿 📶 🔏 🛄 🗶 🖸	General Member of Managed by		
Active Directory Users and Comput	Members:		
Saved Queries	Select Users, Contacts, Computers, Service Accounts, or Grou	ups <u>?</u> ×	
H Builtin	Select this object type:		
Computers	Users, Service Accounts, Groups, or Other objects	Object Types	
Domain Controllers	From this location:		
ForeignSecurityPrincipals Managed Service Accounts	filkom.ub.ac.id	Locations	
i user_fikom			
Contract Users	Enter the object names to select (examples):	-	
	user1 (user1@hilkom.ub.ac.id)	Check Names	
	Advanced OK	Cancel	
	Add Remove		
	OK Cancel App	y .	
	· · · · · · · · · · · · · · · · · · ·	N	

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.

use	r Prop	erties		? ×
G	eneral	Members	Member Of Managed By	
	Membe	ne.		
	Name		Active Directory Domain Services Folder	
	👗 us	er1	filkom.ub.ac.id/user_filkom	
	👗 us	er2	filkom.ub.ac.id/user_filkom	
	👗 us	er3	filkom.ub.ac.id/user_filkom	
T	👗 us	er4	filkom.ub.ac.id/user_filkom	
	Ad	d	Remove	
T				
_				
			OK Cancel	Apply

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".
- 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.

Add Roles Wizard		×
Confirm Installat	ion Selections	
Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings IPv4 WINS Settings DHCP Scopes DHCPv6 Stateless Mode IPv6 DNS Settings DHCPserver Authorization Confirmation Progress Results	To install the following roles, role serv	vices, or features, dick Install. estarted after the installation completes. 10.123.10.10 (IPv4) filkom.ub.ac.id 10.123.10.10 None No scopes defined Enabled filkom.ub.ac.id ::1 Authorize using credentials associated with FILKOM\Administrator
	Print, e-mail, or save this information	
		< Previous Next > Install Cancel

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.

DHCP				
File Action View Help				
🗢 🔿 🙍 🗊 🖾 😣 🛛 🗖				
Yet Implement Implement Implement Implement	Contents of DHCP Server	Status ** Active ** ** Active **	Description user filkom Don't Support 802. 1X or Authenticated Failed	Actions IPv4 A More >

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:

- 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.
- 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.

Add Roles Wizard			×
Confirm Installat	tion Selections		
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Crybtography CA Name Validity Period Certificate Database Confirmation Progress Results	To install the following roles, role servic	es, or features, dick Install. ges below tarted after the installation completes. ervices of this computer cannot be changed after Certification Authority has Enterprise Root RSA#Microsoft Software Key Storage Provider SHA1 2048 Disabled 9/13/2022.7:34 PM CN=filkomSPURPCA,DC=filkom,DC=ub,DC=ac,DC=id C:\Windows\system32\CertLog C:\Windows\system32\CertLog	
		<previous next=""> Install Cancel</previous>	

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).
- 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:

- 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".
- 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.

w RADI	US Client					>
ettings	Advanced					
🗸 Enab	le this RADIUS cl	ient				
🗖 Sela	ect an existing tem	plate:				
	2				-	
-Name	and Address					_
Friend	y name:					
Cisco	Switch					
Addres	ss (IP or DNS):					
10.12	3.10.250				Verify	
Shared Select	I Secret an existing Share	d Secrets template	e:			
None					•	
To ma secret secret	nually type a share , click Generate, Y entered here. Sha anual d secret:	ed secret, click Ma You must configure red secrets are ca C Generate	anual. To auto the RADIUS sse-sensitive.	matically ge client with t	merate a shared he same shared	
••••	•					
Confirm	n shared secret:					
••••	•					
				ОК	Cancel	

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.

Select the certificate t A certificate that is co Policy will override this	he server should use to prove its identii nfigured for Protected EAP in Connectio certificate.	ty to the dient. n Request	
Certificate issued	ertificate issued server.filkom.ub.ac.id		
Friendly name:			
Issuer:	filkom-SERVER-CA		
Expiration date:	9/13/2018 8:17:35 PM		
 Enable Fast Reconnect Clients Types 	nect without Cryptobinding		
Secured password (EA	P-MSCHAP ∨2)	Move Up Move Down	

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.

vlan1 Properties Overview Conditions Constraints Settings	js	×
Configure the settings for this network policy. If conditions and constraints match the conne Settings:	ection request and the policy grants access, settings are applied.	
Kandard Standard Vendor Specific Network Access Protection NAP Enforcement	To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.	
	Attributes:	
Extended State	Name Value	
Routing and Remote Access	Tunnel-Medium-Type 802 (includes all 802 media plus Ethemet canonical for	
Multilink and Bandwidth Allocation Protocol (BAP)	Tunnel-Type Virtual LANs (VLAN)	
TP Filters		
Generation		
A IP Settings		
🦓 ir Settings	Add Edit Fiemove	

Gambar lampiran 20 RADIUS Attributes Standard

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

🛸 Network Policy Server			le ×
File Action View Help			
🗢 🔿 🔰 🖬 🚺 🖬			
NPS (Local) RADIUS Clients and Servers If Policies Connection Request Polici Network Policies	Network Policies Network Policies Image: Network policies allow you to designate who is a under which they can or cannot connect.	uthorized to connect to the network and the circumstances	
Health Policies Network Access Protection	Policy Name	Status Processing Order Access Type So	ou
Accounting	vian1	Enabled 1 Grant Access U	ns
🕀 🌉 Templates Management	Connections to Microsoft Routing and Remote Access	server Enabled 2 Deny Access U	ns
	vian1 NAS Port Type Ethernet Windows Groups FILKOM/user		
	Settings - Then the following settings are applied:		
	Setting Valu	Je 🔺]
	Tunnel-Medium-Type 802	(includes all 802 media plus Ethemet canonical format)	
	Tunnel-Pvt-Group-ID 1 Tunnel-Type Virtu	ual LANs (VLAN)	-
	•		
• • •			Þ

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.

Swit	ch(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 30	UserAuthenticated dontsupport	active active	Gi0/2

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.

inte	erface 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	5.0
ip	helper-a	ddress	10.123.	10.10	

Gambar lampiran 24 VLAN 30

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



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.



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.



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.

Disable this network device Disappose this conner Ethernet Properties X	Protected EAP Properties ×		8F • 0	1 ()
Networking Authentication Sharing	ack When connecting: ackyerify the server's identity by validating the certificate	Wi-Fi Not connected Qualcomm Atheros AR9485WB-E		
Select this option to provide authenticated network access for this Ethernet adapter.	Connect to these servers (examples:srv1;srv2;, *srv3com):			
Enable IEEE 802.1X authentication				
Choose a network authentication method:	Trusted Root Certification Authonities: AddTrust External CA Root			
Microsoft: Protected EAP (PEAP) V Settings	Baltimore CyberTrust Root Certum CA			
Remember my credentials for this connection each time I'm logged on	Certum Trusted Network CA Class 3 Public Primary Certification Authority			
Fallback to unauthorized network access	DESKTOP-HAB9414			
Additional Settings	Notifications before connecting: Tell user if the server's identity can't be verified			
	Select Authentication Method:			
	Secured password (EAP-MSCHAP v2) Configure			
	Disconnect if server does not present cryptobinding TLV			
OK Cancel				
	OK Cancel			
	ι			
ms 1 item selected				8:: 6

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

Windows S	ecurity		×
Sign ir	1		
8	user1@filkom.ub.ac.	id	
	•••••		
	Domain: filkom.ub.ac.	id	
	OK	Cancel	

Gambar lampiran 32 Logon Autentikasi

Network Connection Deta	ils	X Select Command Prompt
Network Connection Details:		Ethernet adapter Ethernet:
Property Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Epitres IPv4 Default Gateway IPv4 DHCP Server IPv4 WINS Server IPv4 WINS Server IPv4 WINS Server IPv4 WINS Server IPv5 Default Gateway IPv5 Default Gateway IPv5 Default Gateway	Value filkom.ub.ac.id Reatek PCIe GBE Family Controller 74:27-EA-87-64-2C Yes 172:16:10.12 255:255:256.0 Thursday, January 4, 2018 9:18:22 PM fiday, January 12, 2018 9:18:21 PM 172:16:10.250 10:123:10.10 10:123:10.10 Yes fe80::dc47#f6e:8019.be03%3	Connection-specific DNS Suffix . : filkom.ub.ac.id Description : Realtek PCTe GBE Family Controller Physical Address : 74-27-EA-B7-64-2C DHCP Enabled : Yes Autoconfiguration Enabled : Yes Link-local IPv6 Address : fe80::dc47:ff6e:8019:be03%3(Preferred) IPv4 Address : 172.16.10.12(Preferred) Subnet Mask : 255.255.0 Lease Obtained : ITursday, January 4, 2018 9:18:22 PM Lease Expires : 172.16.10.250 DHCPv6 IAID : 57944042 DHCPv6 Client DUID : 00-091-08-01-20-81-61-E3-74-27-EA-B7-64-2C DNS Servers : 10.123.10.10 Tunnel adapter isatap.filkom.ub.ac.id:

Gambar lampiran 33 Pengalokasian Alamat IP