BAB III

PEMBAHASAN

3.1 Analisis Jaringan

Analisis terbagi kedalam beberapa pokok bahasan diantaranya seperti yang akan dijelaskan dibawah ini :

3.1.1 Analisis Masalah

Dari tahap analisis dapat diketahui dengan jelas masalah-masalah apa saja yang sering muncul, bagaimana cara menyelesaikan masalah atau kendala pada pengaturan dan pembagian bandwidth sampai solusi yang dapat diajukan untuk memecahkan masalah tersebut. Untuk mengurangi dampak ketidak stabilan koneksi internet perlu adanya *router* dalam jaringan, yang bertugas melakukan pengaturan pemakaian *bandwidth* dan pembagian *bandwidth* seefektif mungkin ke seluruh *client*, jadi setiap *user* akan mendapatkan jumlah *bandwidth* yang sama banyak dalam proses *browsing* ataupun men-*download* data dari internet, dengan ini di harapkan tidak akan ada lagi *user* yang mengeluh atas lambatnya koneksi internet bila ada *user* lain yang sedang men-*dowload.* Atas dasar tersebut, mengaplikasikan Mikrotik OS sebagai *router* jaringan yang memiliki *feature* dan *tools* yang cukup lengkap baik untuk jaringan kabel maupun jaringan *wireless. Bandwidth* adalah besar *byte* penggunaan pada transfer data dalam jaringan. Oleh karena itu diperlukan program yang dapat mengatur alur *Bandwidth* dari masing-masing komputer yang melewati *router* tersebut.

3.1.2 Analisis Kebutuhan Non Fungsional

Analisis kebutuhan non-fungsional merupakn analisis yang dibutuhkan untuk menentukan spesifikasi sistem**.** Spesifikasi ini juga meliputi elemen-elemen atau komponen-komponen apa saja yang dibutuhkan. Kebutuhan non-fungsioanal terbagi mejadi dua analisis, yaitu analisis perangkat keras, perangkat lunak.

3.1.3 Analisis *Hardware* (Perangkat Keras)

Spesifikasi perangkat keras pada komputer yang digunakan di PT Pembangkitan Jawa Bali Unit Pembangkitan Cirata *client* adalah :

1. Prosesor : Intel Core 2 Duo 2.4 GHz
2. RAM : 1 GB
3. Hard Disk : 160 GB
4. VGA : On Board (di set 64 MB)
5. Ethernet Card : RTL8139 PCI 10/100 Mbps
6. Monitor : 15 Inci dengan resolusi 1024x768 *color* 32bit

Spesifikasi perangkat keras pada komputer *server* :

1. Prosesor : Intel Core 2 Duo 2.8 GHz
2. RAM : 4 GB
3. Hard Disk : 500 GB
4. VGA : NVDIA G-FORCE 9500GT 128 Mb
5. Ethernet Card : RTL8139 PCI 10/100 Mbps
6. Monitor : LCD 17” dengan resolusi 1024x768 *color* 32bit

3.1.4 Analisis *Software* (Perangkat Lunak)

Perangkat lunak yang digunakan pada setiap komputer *client* :

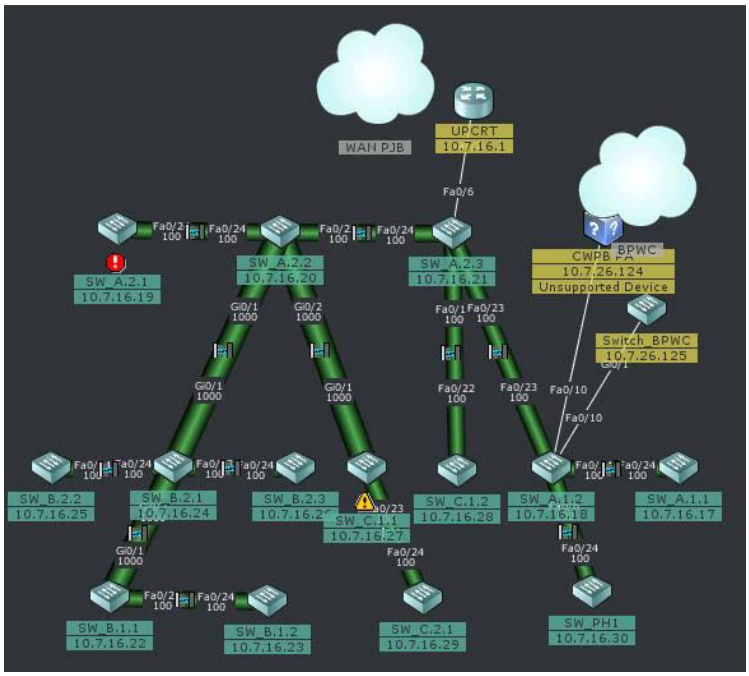
1. Sistem Operasi : Microsoft Windows XP Profesional
2. Proteksi : Antivirus Kaspersky 7 dan Deep Freeze
3. Browser : Internet Explorer, Mozilla Firefox dan Opera

Perangkat lunak yang digunakan pada komputer *server* :

1. Sistem Operasi : Microsoft Windows Server 2003
2. Pengaturan Bandwith : Microtic for Windows
3. Proteksi :
    - Kaspersky 7 (Antivirus)
    - R admin (aplikasi untuk memantau / memonitor komputer *client*)
    - IP Angry Scanner (aplikasi untuk mengecek komputer *client* yang sedang aktif pada jaringan / *workgroup*)
4. Browser : Internet Explorer, Mozilla Firefox dan Opera

3.1.5 Topologi Jaringan

Topologi jaringan yang digunakan pada PT Pembangkitan Jawa Bali Unit Pembangkitan Cirata adalah topologi STAR. Topologi star tidak langsung terhubung satu sama lain, tetapi melalui perangkat pusat pengendali (*central controller*) yang biasa disebut dengan switch. Pada topologi star, switch berfungsi layaknya seperti pengatur lalu lintas. Jika satu komputer ingin mengirimkan data ke komputer lainnya maka data tersebut dikirimkan ke switch terlebih dahulu, yang kemudian meneruskannya ke komputer tujuan. Arsitektur jaringan secara global yang terdapat di PT. Pembangkitan Jawa Bali Unit Pembangkitan Cirata adalah sebagai berikut :



Gambar 3. 1 Topologi Jaringan PT PJB UP Cirata

3.1.6 Kondisi Ruangan di Gedung B PT Pembangkitan Jawa Bali Unit Pembangkitan Cirata

PT. Pembangkitan Jawa Bali Unit Pembangkitan Cirata memiliki 4 gedung yaitu :

- Gedung A (2 lantai)
- Gedung B (2 lantai)
- Gedung C (2 lantai)
- Gedung Sarana Olahraga

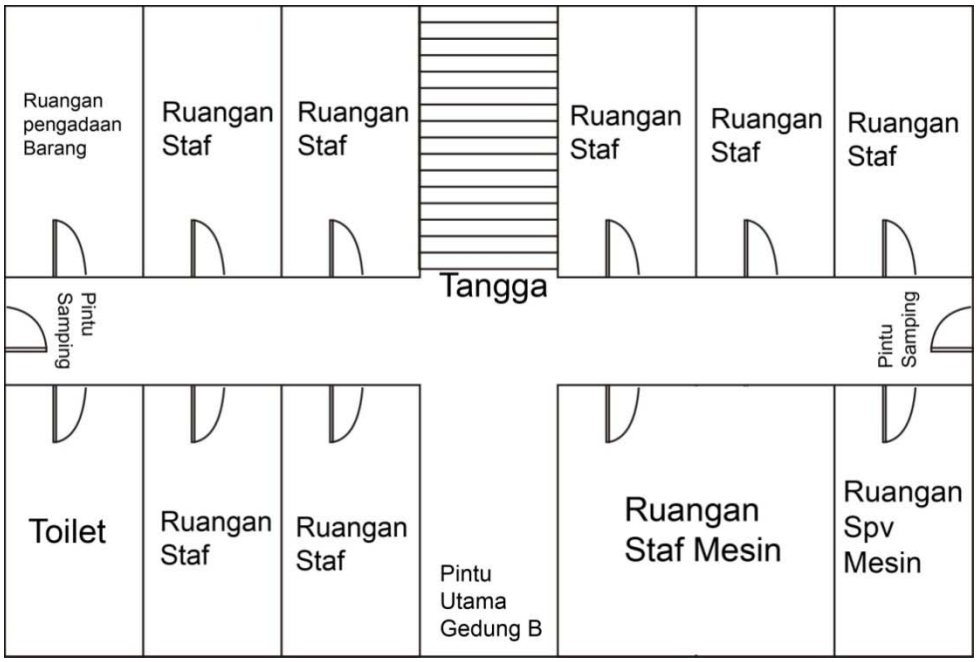
Berikut adalah denah gedung B yang menjadi fokus penerapan port based authentication 802.1x. Disetiap gedung kecuali gedung olahraga terdapat masing – masing sebuah server untuk mengelola jaringan yang dihubungkan dengan *fiber optic* sehingga memungkinkan untuk melakukan konfigurasi maupun perawatan jaringan di salah satu gedung untuk keseluruhan gedung.



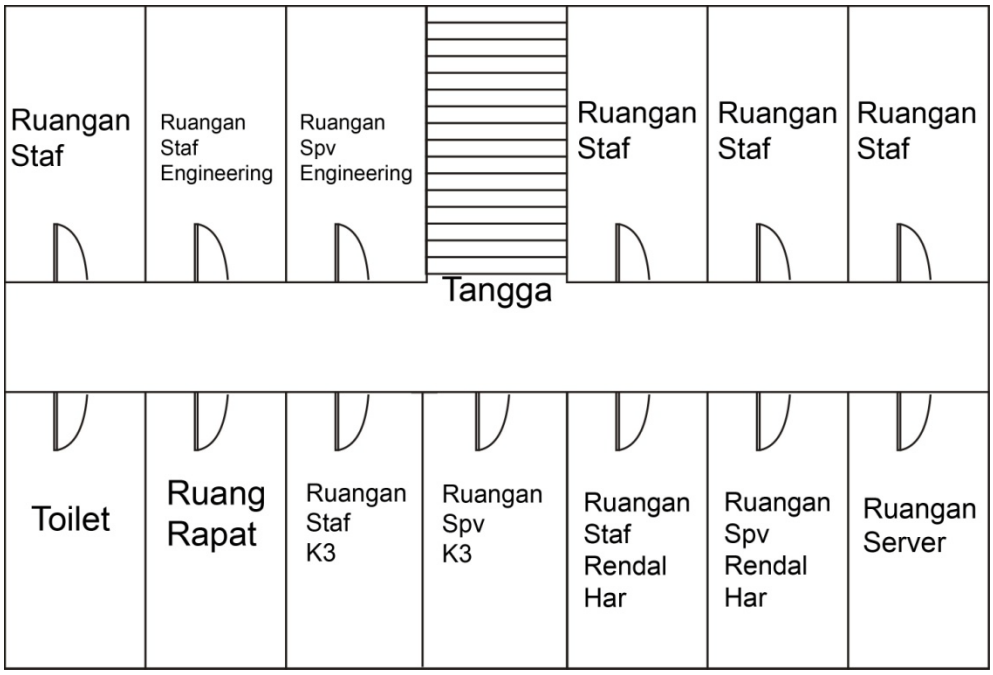
Gambar 3. 2 Gedung B PT PJB UP Cirata

3.1.7 Denah Ruangan dan Kondisi di Dalam Gedung

Dalam gedung B PT Pembangkitan Jawa Bali Unit Pembangkitan Cirata terdapat 2 lantai yang masing – masing lantai terbagi menjadi ruangan – ruangan untuk staf dan ruangan *server.*



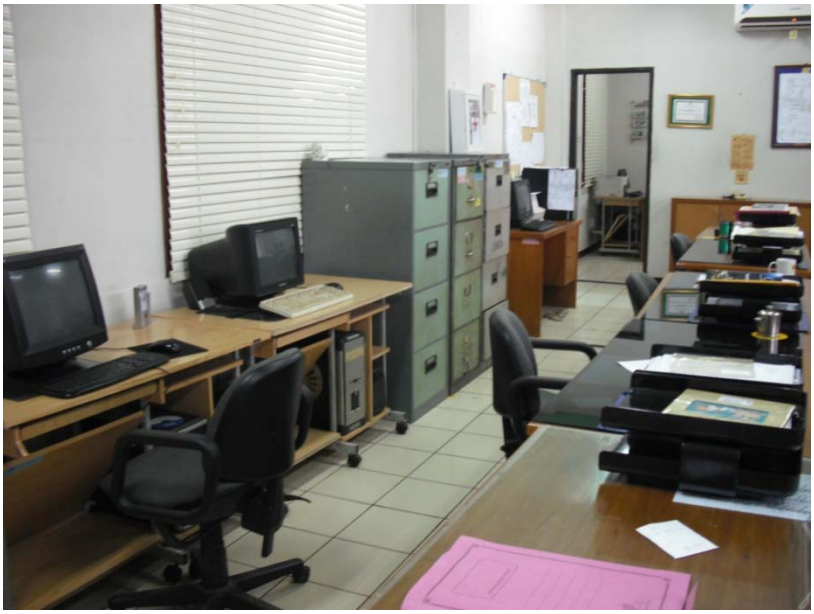
Gambar 3. 3 Denah Lantai 1



Gambar 3. 4 Denah Lantai 2



Gambar 3. 5 Server



Gambar 3. 6 Salah satu Ruangan di Gedung B

3.2 Konfiguasi Protokol 802.1x Port Based Authentication

3.2.1 Cisco Secure ACS

Cisco Secure Access Control Server (ACS) Solusi Engine merupakan alat yang berfungsi untuk kontrol akses jaringan. Ini bertujuan untuk mematuhi persyaratan peraturan dan perusahaan berkembang, meningkatkan produktivitas, dan mengandung biaya. Mendukung skenario secara bersamaan, termasuk:

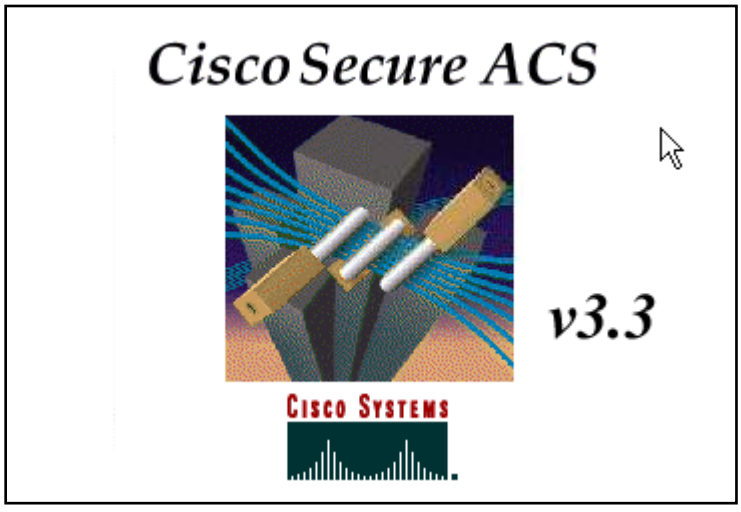
1. Perangkat administrasi: mengotentikasi administrator, mengotorisasi perintah, dan menyediakan jejak audit.
2. Remote Access: Bekerja dengan VPN dan perangkat jaringan lainnya remote akses untuk menegakkan kebijakan akses.
3. Wireless: mengotentikasi dan mengotorisasi pengguna nirkabel dan host dan melaksanakan kebijakan nirkabel spesifik.
4. Jaringan masuk kontrol: Berkomunikasi dengan server dan audit untuk menegakkan kebijakan masuk kontrol.

Cisco Secure ACS Solution Engine memungkinkan untuk mengatur akses ke sumber daya jaringan untuk berbagai tumbuh jenis akses, perangkat, dan kelompok pengguna. Fitur-fitur kunci alamat kompleksitas saat kontrol jaringan akses:

1. Dukungan untuk berbagai protokol termasuk Protokol Otentikasi yang Diperluas (EAP) dan non-protokol EAP memberikan fleksibilitas untuk memenuhi semua kebutuhan otentikasi.
2. Integrasi dengan produk Cisco untuk mengontrol perangkat administrasi akses memungkinkan kontrol terpusat dan audit tindakan administratif
3. Dukungan untuk database eksternal dan server audit centralizes kontrol akses kebijakan dan memungkinkan untuk mengintegrasikan sistem akses dan kontrol identitas

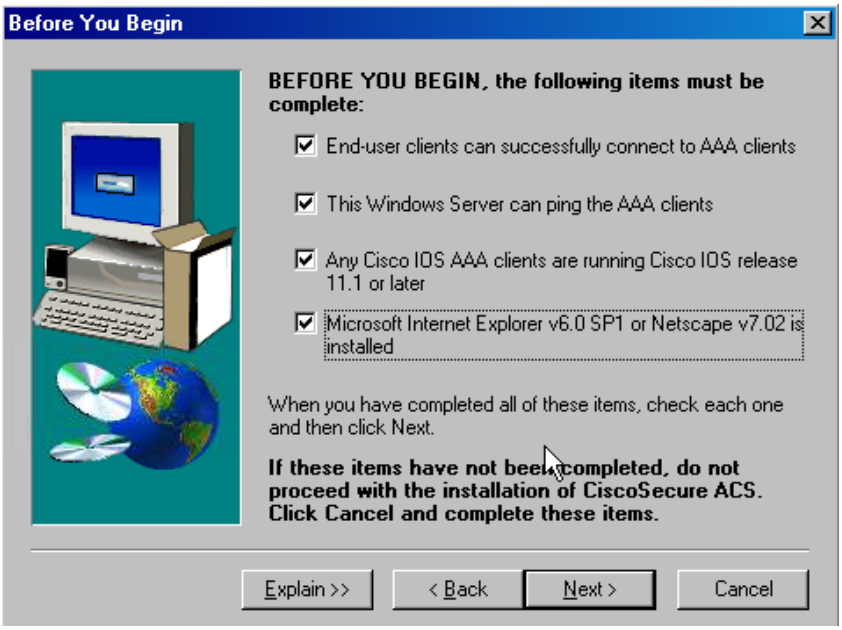
3.2.2 Installasi Cisco Secure ACS v3.3

Langkah pertama untuk mengkonfigurasi 802.1x Port Based Authentication memerlukan software pendukung seperti Cisco Secure ACS v3.3. Berikut adalah cara installasi Cisco Secure ACS v3.3



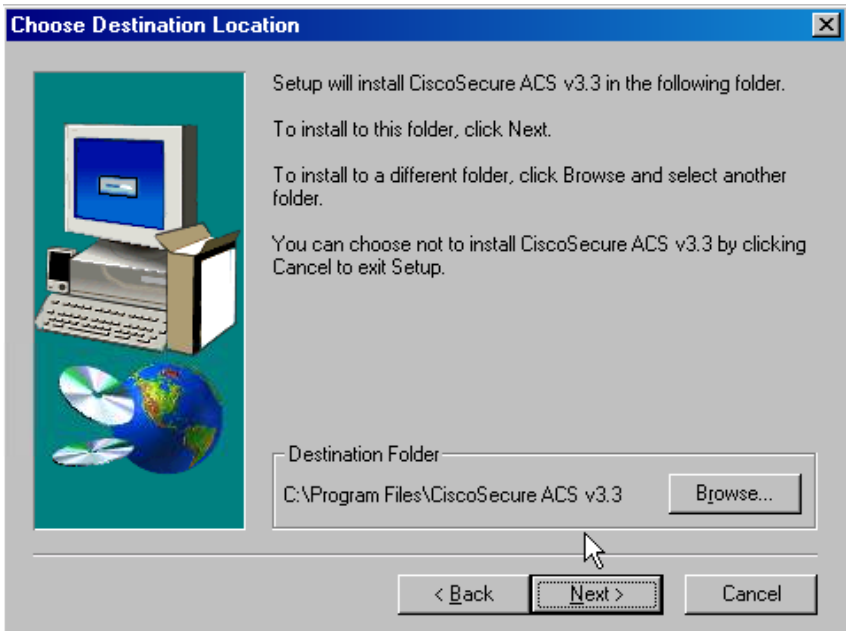
Gambar 3. 7 Tampilan awal Cisco Secure ACS v3.3

Setelah menunggu beberapa saat setelah tampilan awal, maka akan muncul jendela installasi. Centang semua kotak yang kosong kemudian klik next, lihat gambar berikut.



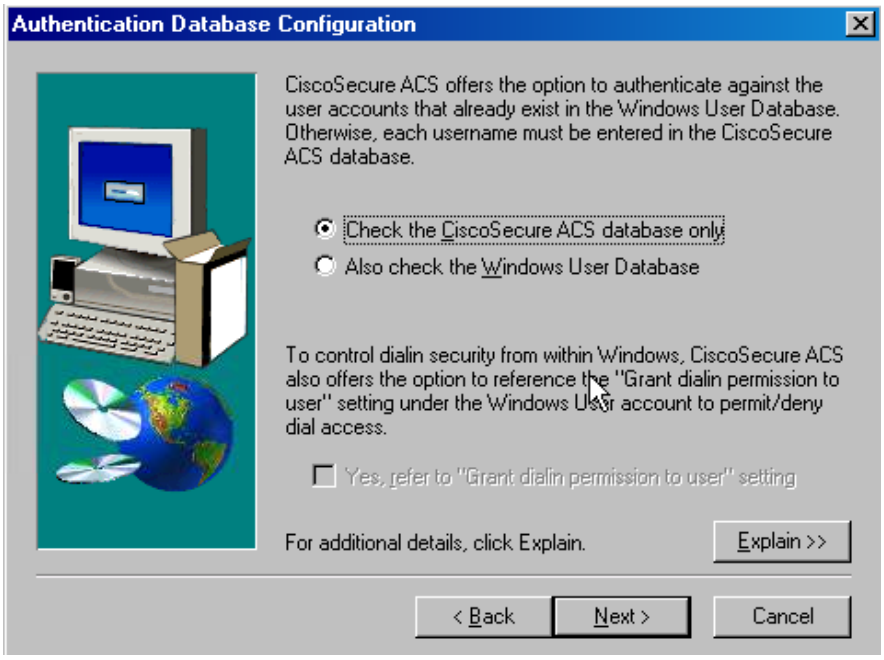
Gambar 3. 8 Tandai semua pilihan pada kotak dialog

Kemudian tentukan dimana file akan disimpan.



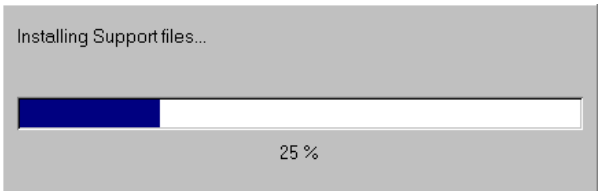
Gambar 3. 9 Tentukan folder installasi

Pada jendela Authentication Database Configuration pilih pilihan pertama agar mempermudah untuk melakukan pengaturan user.



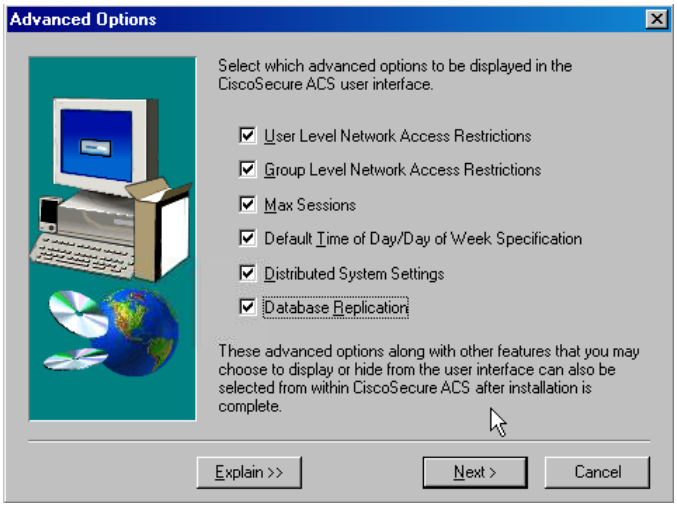
Gambar 3. 10 Pilih option pertama agar lebih mempermudah pengaturan user

Proses installasi akan berlangsung dan memerlukan waktu beberapa saat.



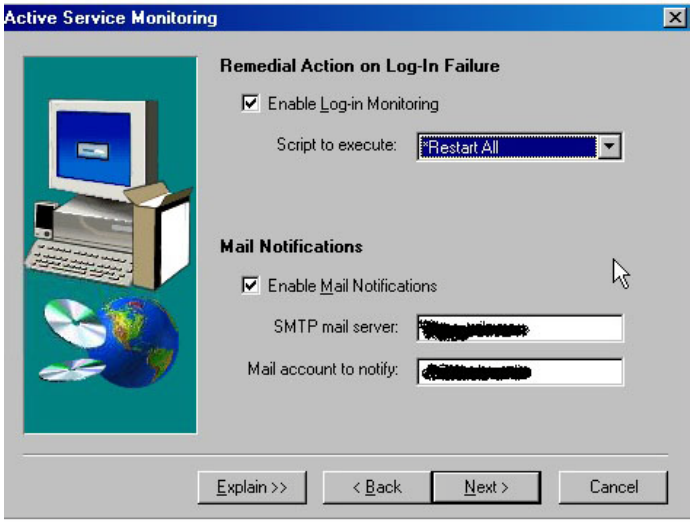
Gambar 3. 11 Proses Installasi sedang berlangsung

Pada jendela option centang kotak yang kosong sesuai dengan kebutuhan, fungsi ini bertujuan untuk menampilkan pilihan pada saat menjalankan aplikasi. Tetapi disarankan untuk mencentang semua pilihan agar penggunaan lebih mudah untuk dijalankan. Lihat gambar berikut.



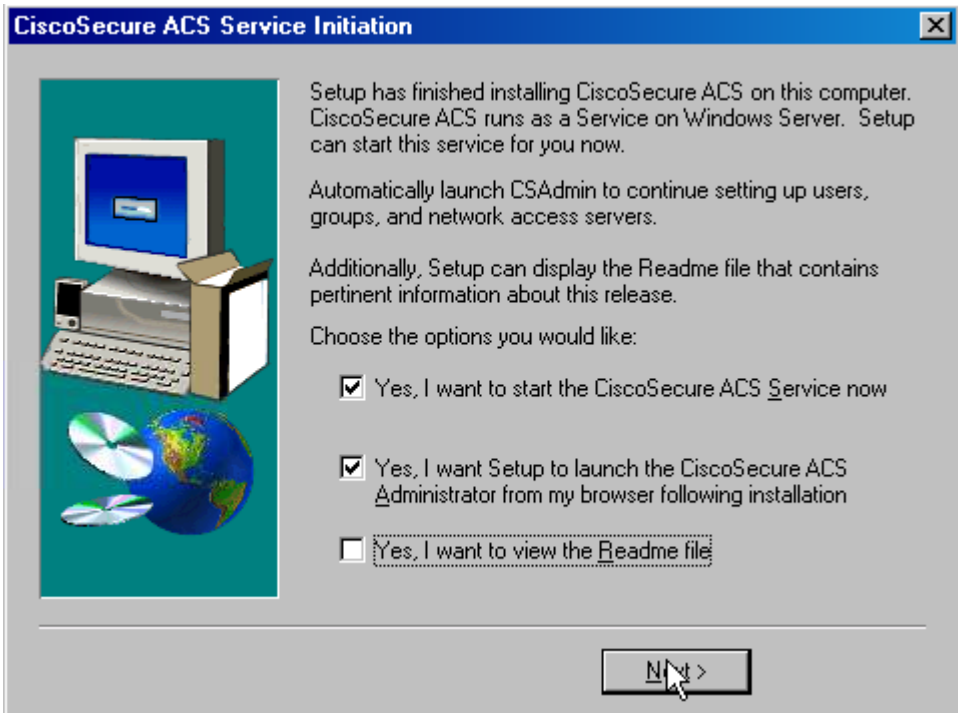
Gambar 3. 12 Centang semua pilihan

Kemudian masukan notifikasi SMTP mail server dan notifikasi accounr email.



Gambar 3. 13 Isikan Email Notifikasi

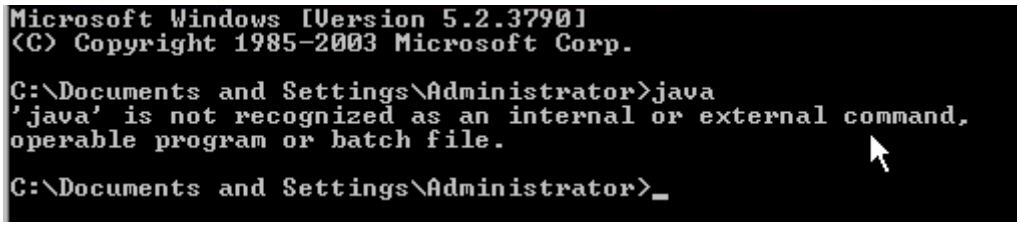
Inisialisasikan Cisco Secure ACS Service dan centang kotak yang tersedia sesuai dengan kebutuhan dan proses installasi selesai. Dan Cisco Secure ACS siap untuk dijalankan.



Gambar 3. 14 Finishing Installasi

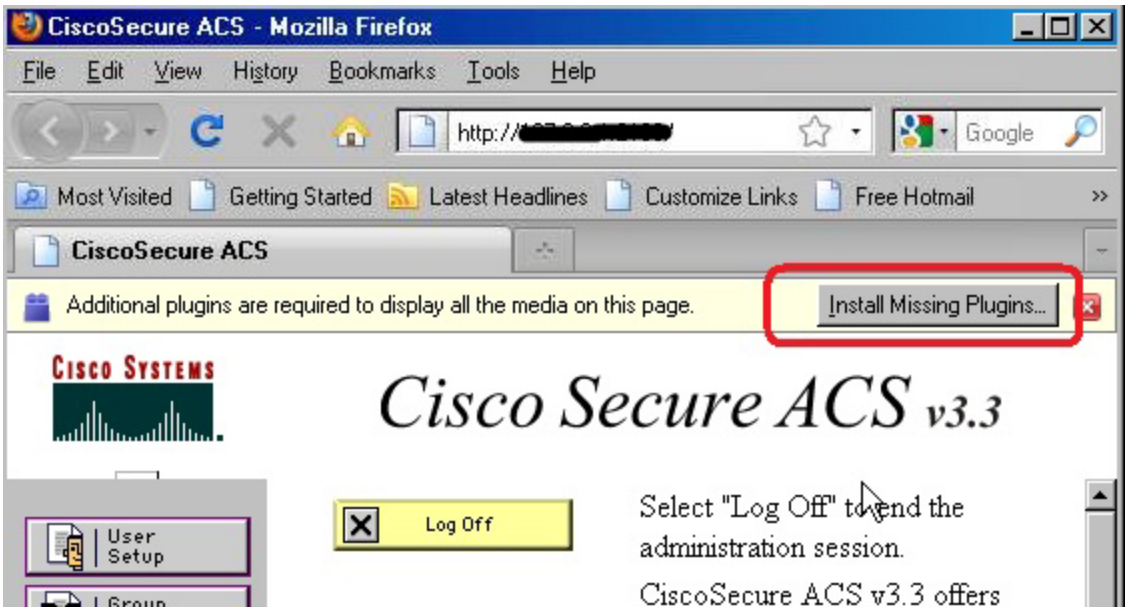
3.2.3 Konfigurasi Cisco Secure ACS

Konfigurasi Cisco secure ACS sebagian besar dilakukan melalui web GUI. Sebelum membuka web GUI, pastikan di komputer telah terinstall *java runtime environment*. Sebab, web GUI mnggunakan *applet* dalam sebagian menu-nya. Untuk mengecek keberadaan java, cukup ketikan perintah "*java*" di DOS Console.



Gambar 3. 15 Java belum terinstall

Jika java belum terpasang web browser dan ketikkan ip address dengan format http:/xxx.xx.xxx.xx kemudian tekan Install missing Plugins



Gambar 3. 16 Install plugin Java

Jika telah selesai cek kembali dengan mengetikkan perintah java di DOS Console

```
C:\Documents and Settings\Administrator>java
Usage: java [-options] class [args...]
           (to execute a class)
   or  java [-options] -jar jarfile [args...]
           (to execute a jar file)

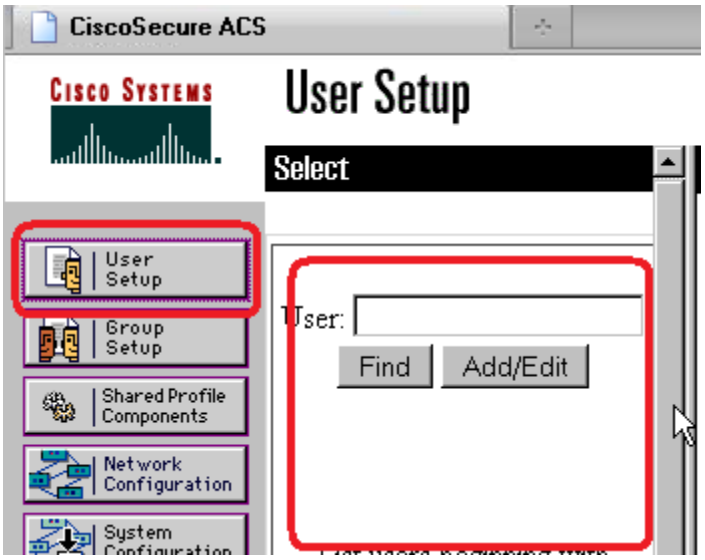
where options include:
    -client       to select the "client" VM
    -server       to select the "server" VM
    -hotspot      is a synonym for the "client" VM  [deprecated]
                  The default VM is client.
```

Gambar 3. 17 Java sudah terinstall

Konfigurasi yang perlu dilakukan di dalam web GUI Cisco ACS 3.3 antara lain adalah :

– Pendaftaran User

User adalah pengguna yang nantinya akan meminta autentifikasi ke server Cisco ACS. Proses penambahan user bisa dilakukan secara *one by one*, atau *batch*. Penambahan secara one by one dilakukan langsung di menu *User Setup*

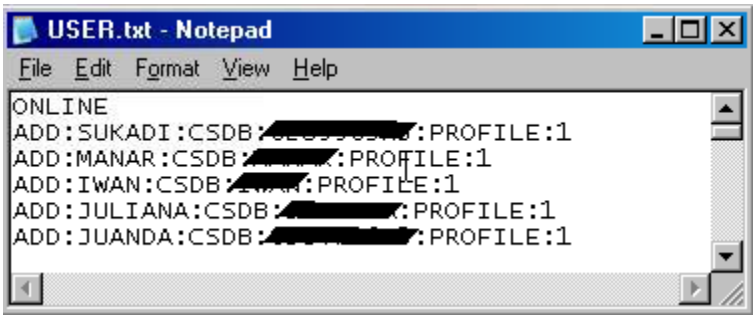


Gambar 3. 18 User Setup Cisco ACS 3.3

Penambahan user one by one melalui menu ini kurang efektif apabila network administrator ingin mengambahkan user yang berjumlah relatif banyak. Oleh karena itu, Cisco menyediakan fitur untuk menambahkan user melalui batch proses. Yaitu melalui CLI (Command Line Interface). Adapun langkah-langkah menggunakan fitur ini adalah sebagai berikut:

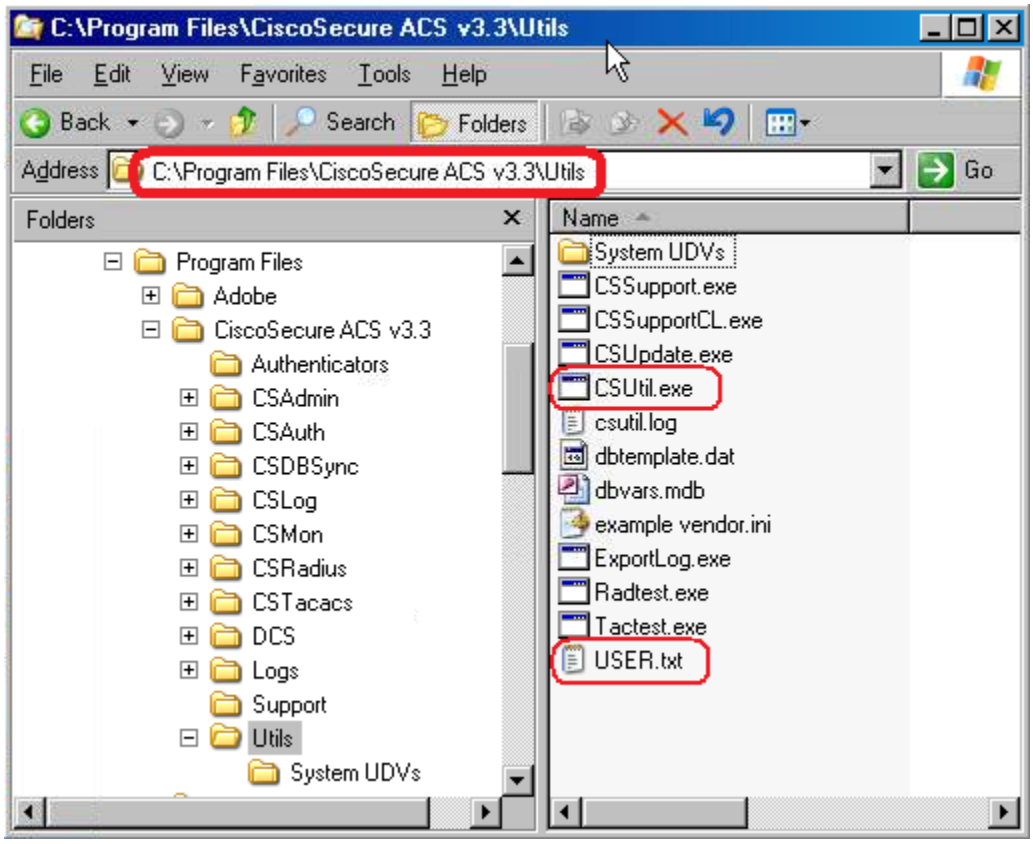
a. Membuat file text berisi daftar user yang akan diupload ke Cisco server ACS dengan format

ADD:<USERNAME>**:CSDB:**<PASSWORD>**:PROFILE:**<PROFILE_NUMBER>



Gambar 3. 19 Contoh file text

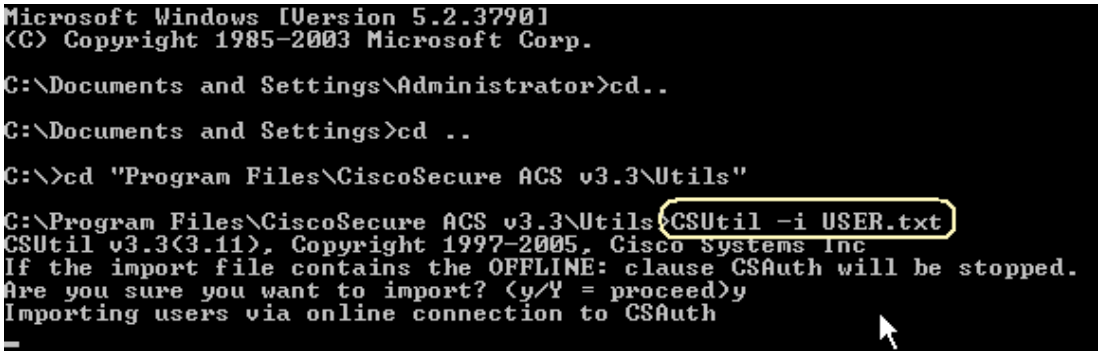
b. Mencari lokasi *CSUtil.exe* kemudian mengkopikan file user.txt di atas ke folder yang sama dengan *CSUtil.exe*



Gambar 3. 20 Letak CSUntil.exe dan user.txt

c. Menjalkan CSUtil.exe dengan Perintah

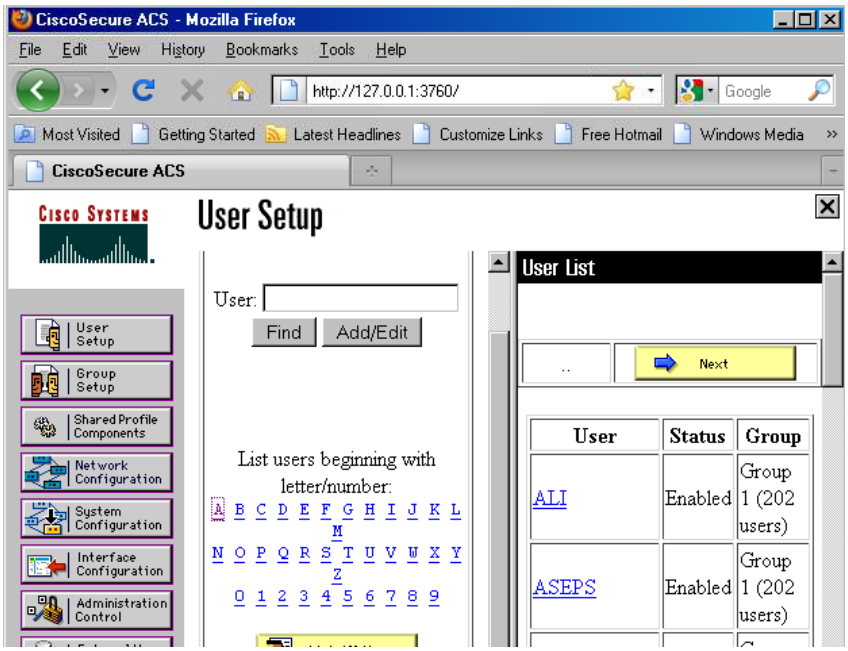
CSUtil - i USER.txt



Gambar 3. 21 CSUntil

d. Apabila terjadi error saat proses sedang berlangsung, *command* di atas bisa dieksekusi lagi untuk memastikan bahwa *USER.txt* berhasil diload seluruhnya ke database User Cisco ACS

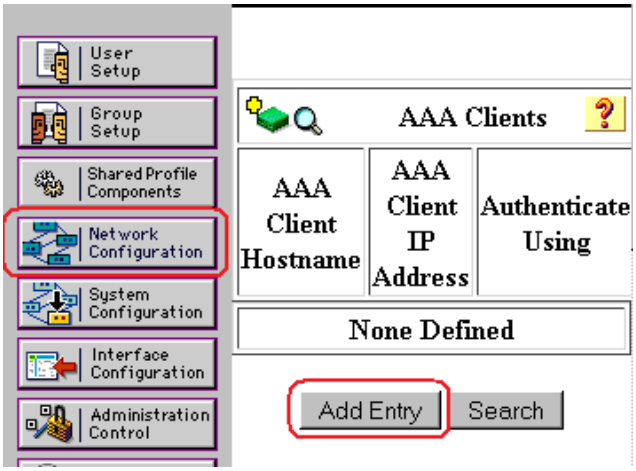
e. Untuk mengkonfirmasi bahwa data user telah berhasil di load, bisa dicek di web GUI Cisco ACS, menu User Setup



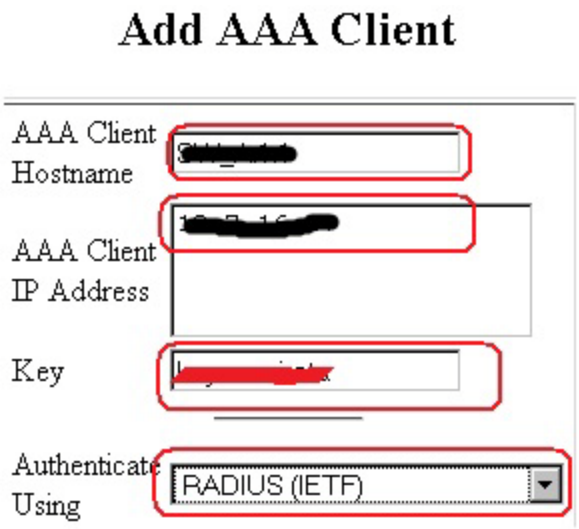
Gambar 3. 22 Daftar User

– **Pendaftaran Switch**

Tahap berikutnya adalah mendaftarkan switch-switch yang bertidak sebagai Client ke dalam Cisco Secure ACS. Cara pendaftarannya adalah sebagai berikut:

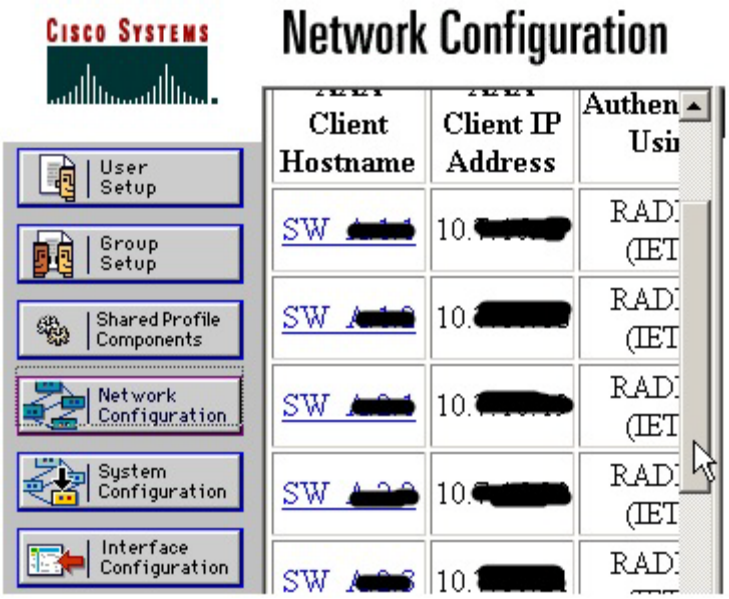


Gambar 3. 23 Mendaftarkan switch ke Cisco Secure ACS 3.3



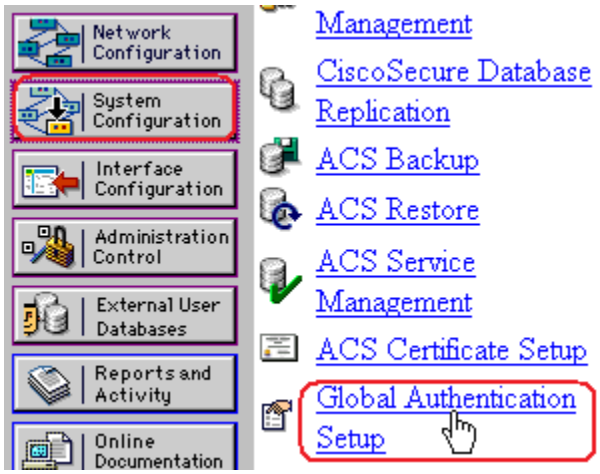
Gambar 3. 24 Mengisi data-data yang berkaitan dengan switch tersebut

Yang perlu diperhatikan pada tahap ini adalah, KEY harus sama antara yang didaftarkan disini dengan yang nanti dikonfigurasikan ke switch. Apabila key tidak sama, maka proses autentikasi akan gagal

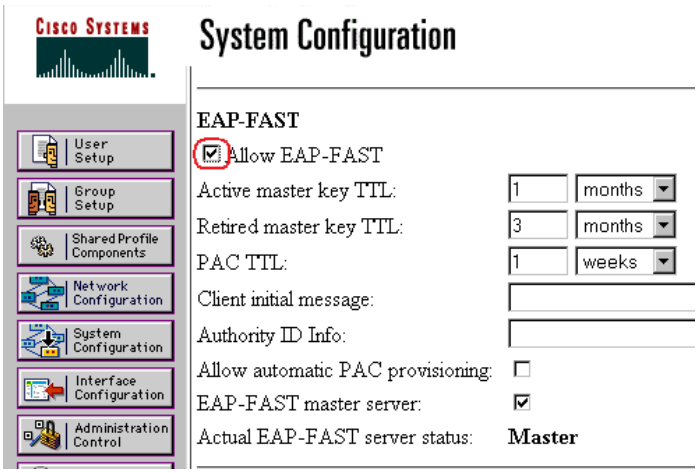


Gambar 3. 25 Switch yang telah dimasukkan ke dalam Cisco ACS

3.2.4 Mengaktifkan EAP-FAST



Gambar 3.20 Buka menu Global Authentication Setup di System Configuration



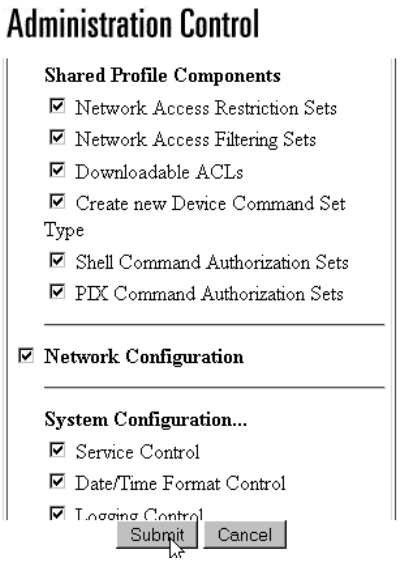
Gambar 3.21 Lalu aktfkan EAP-FAST

3.2.5 Menambakan user Administrator

User administrator dipakai ketika mengakses web GUI Cisco ACS dari komputer lain melalui web browser.



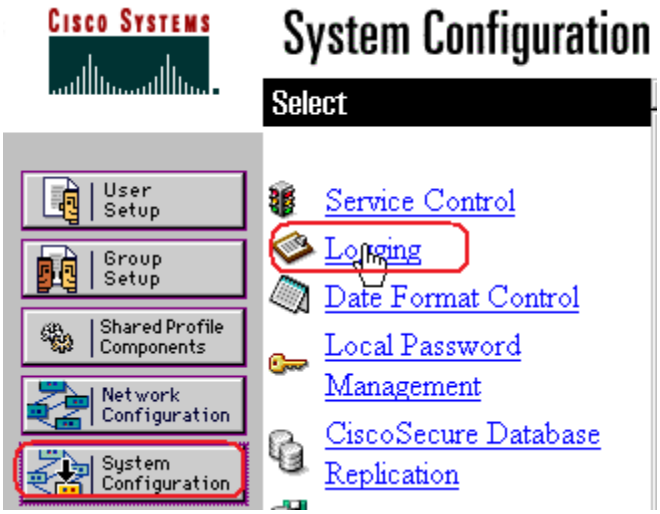
Gambar 3.22 Buka menu Administration Control & klik Add Administrator



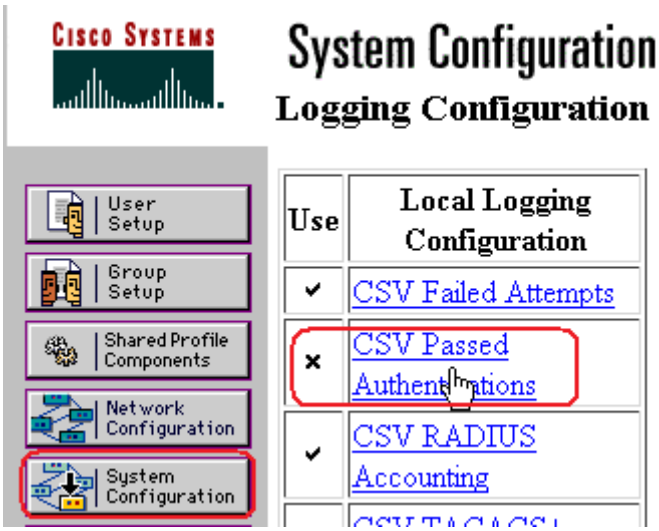
Gambar 3.23 Berikan semua akses, tekan tombol submit

3.2.6 Mengaktifkan Proses *Logging*

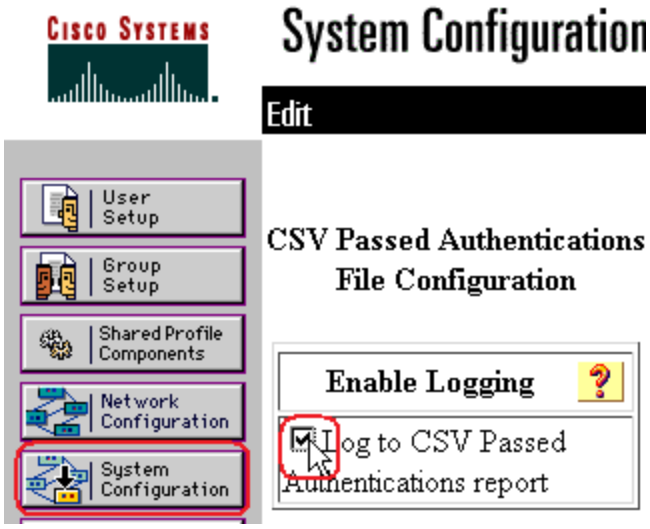
Agar aktifitas-aktifitas yang terjadi di Cisco Secue ACS bisa termonitor dengan baik, *log* hendaknya diaktifkan. Yaitu dengan jalan sebagai berikut:



Gambar 3.24 *Mengkses menu logging*



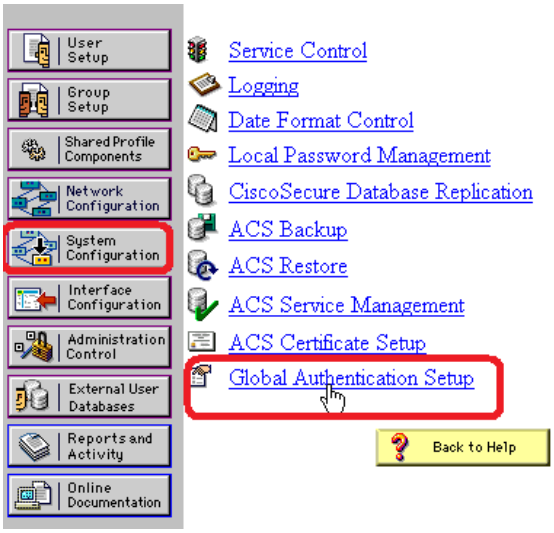
Gambar 3.25 Memilih log yang akan diaktifkan



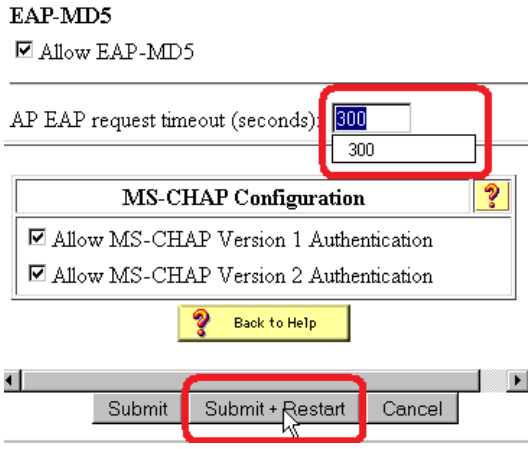
Gambar 3.26 Mengaktifkan Log ke dalam file CSV

3.2.7 Menambah waktu EAP Request timeout

Default dari cisco ACS 3.3, end user diberi waktu duapulu (20) detik untuk meresponse permintaan autentikasi pada saat pertama kali mengakses jaringan. Alokasi waktu ini hendaknya ditambah guna meningkatkan kenyamanan end user. Sebab seringkali alokasi waktu ini habis sebelum end user sempat mengetikkan username dan password. Cara menambah alokasi waktu ini adalah sebagai berikut:



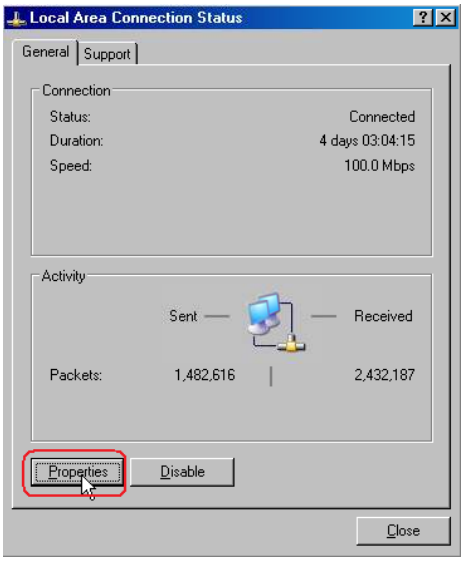
Gambar 3.27 Buka Global Authentication Setup



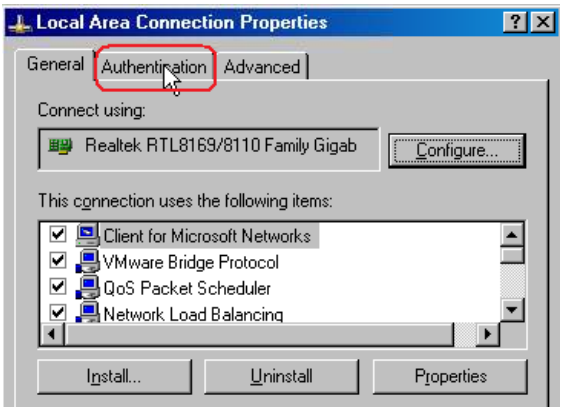
Gambar 3.28 Ganti request timeout menjadi 300 seconds Submit + Restart

3.3 Konfigurasi Network Adapter Client

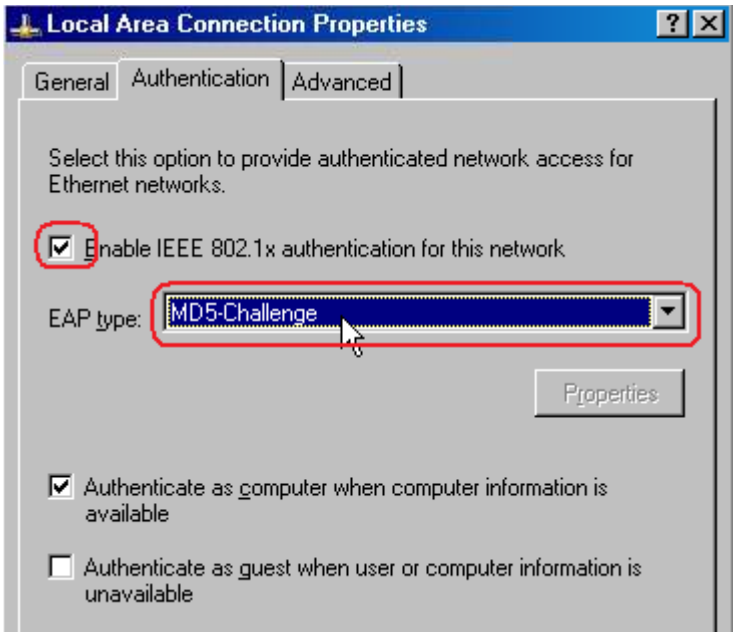
Agar Network adapter di sisi end user bisa mengirimkan sinyal autentikasi, maka network adapter tersebut harus disetting terlebih dahulu. Caranya adalah sebagai berikut:



Gambar 3.29 Buka network adapter properties



Gambar 3.30 Masuk ke tab Authentication
(Apabila belum ada tab ini, jalankan service Wired Autoconfigatau Wireless zero configuration di Administratif tools)



Gambar 3.31 Masukkan settingan sebagaimana screenshot di atas Tekan Apply

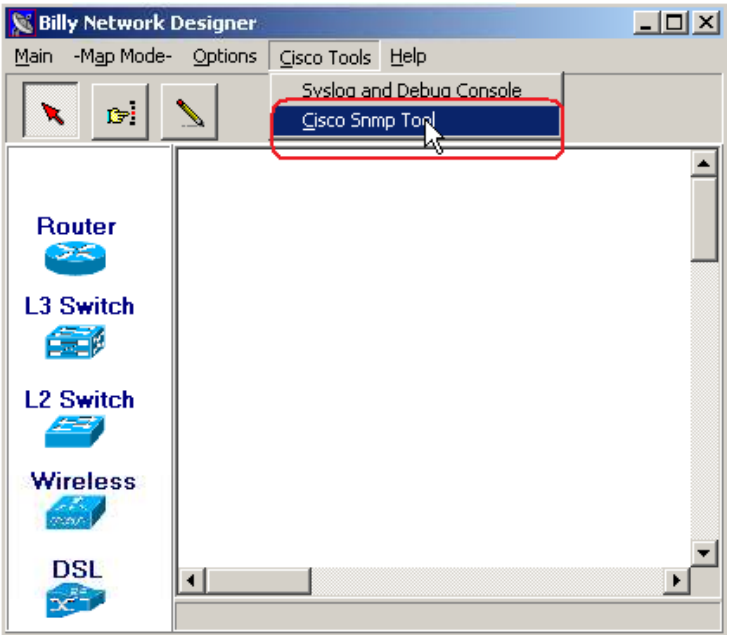
Dengan demikian, end client siap menerima permintaan request autentikasi dari switch

3.3.1 Konfigurasi Switch

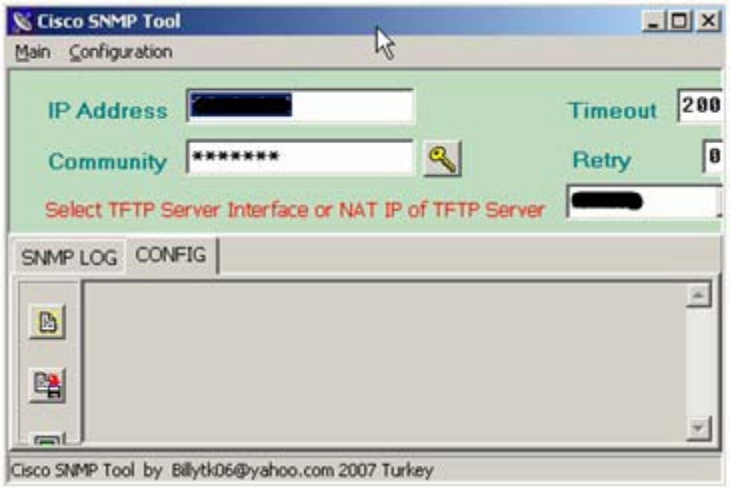
Tahap berikutnya adalah menkonfigurasi switch agar bisa meneruskan komunikasi request dan autentikasi dari client ke Cisco ACS dan sebaliknya. Agar lebih mempermudah, proses konfigurasi ini dilakukan dengan menggunakan software *Cisco SNMP tools*

3.3.1.1 Mendownload Running Config dari switch

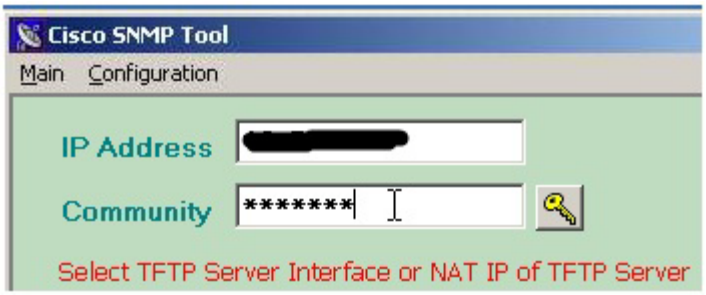
Agar konfigurasi tidak dilakukan dari nol, running config yang sudah ada pada switch didownload terlebih dahulu untuk kemudian di edit. Cara mendownload *running config* tersebut dengan menggunakan *Cisco SNMP Tool* adalah sebagai berikut:



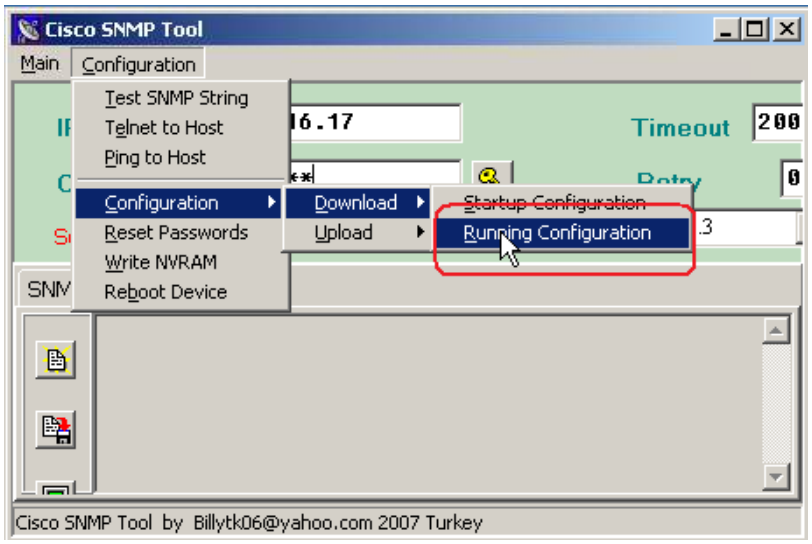
Gambar 3.32 Menjalankan Cisco SNMP Tool



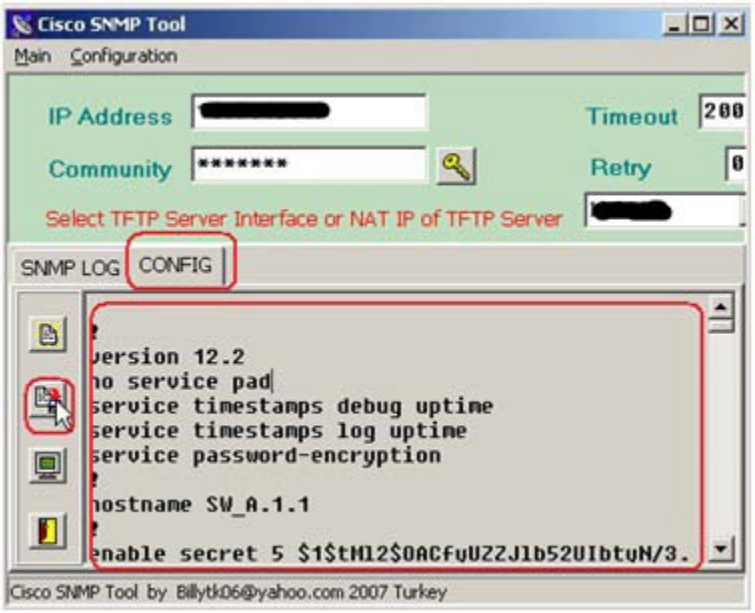
Gambar 3.33 Tampilan Cisco SNMP Tool



Gambar 3.34 Isi dengan IP Address switch yang akan dikonfigurasi



Gambar 3.35 Mendownload Running Config agar bisa dimodifikasi



Gambar 3.36 Script Configuration hasil download, selanjutnya disave dan diedit dengan menggunakan text editor

3.3.1.2 Menambahkan configurasi untuk mengaktifkan Autentikasi pada switch secara global

Mengaktifkan 802.1x adalah dengan menambahkan script berikut pada file Configuration yang telah didownload pada nomer 1 di atas.

Script berikut ditambahkan pada *scopeglobal configuration* :

a. Cisco 2950:

aaa new-model

aaa authentication login default local

aaa authentication dot1x default group radius

aaa authorization network default group radius

radius-server host <ip-addr-ACS> auth-port 1812 acct-port 1813 key <key-ACS>

radius-server retransmit 3

radius-server deadtime 1

b. Cisco 2960:

aaa new-model

aaa authentication login default local

aaa authentication dot1x default group radius

aaa authorization network default group radius

dot1x system-auth-control

radius-server host <ip-addr-ACS> auth-port 1812 acct-port 1813 key <key-ACS>

radius-server retransmit 3

radius-server deadtime 1

3.3.1.3 Mengaktifkan autentikasi 802.1x per port

Setelah 802.1x aktif di skala global, tahap berikutnya adalah mengaktifkan security 802.1x per port. Scriptnya adalah sebagai berikut:

a. Cisco 2950:

```
interface FastEthernet0/1
switchport mode access
dot1x port-control auto
dot1x host-mode single-host
dot1x timeout tx-period 5
dot1x timeout reauth-period 30000
dot1x guest-vlan 2
dot1x reauthentication
spanning-tree portfast
```

b. Cisco 2960:

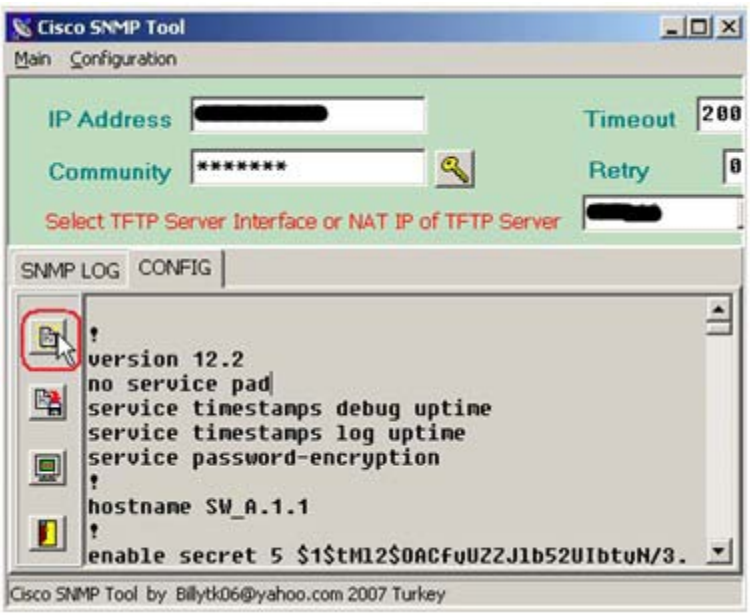
```
interface FastEthernet0/1
    dot1x pae authenticator
    switchport mode access
    dot1x port-control auto
    dot1x host-mode single-host
    dot1x timeout tx-period 5
    dot1x timeout reauth-period 30000
    dot1x guest-vlan 2
    dot1x reauthentication
    spanning-tree portfast
```

Keterangan :

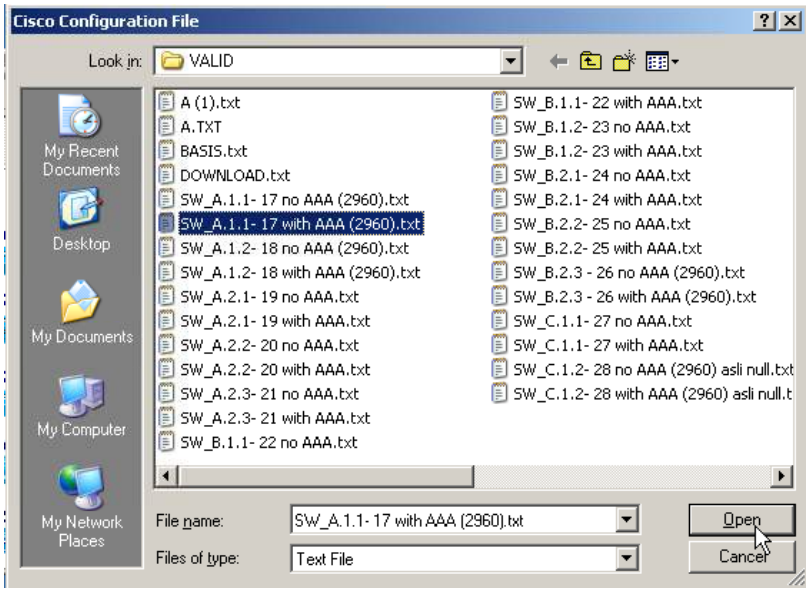
Script di atas hanya ditambahkan pada port yang diaktifkan saja.

3.3.1.5 Mengupload Script yang telah diedit

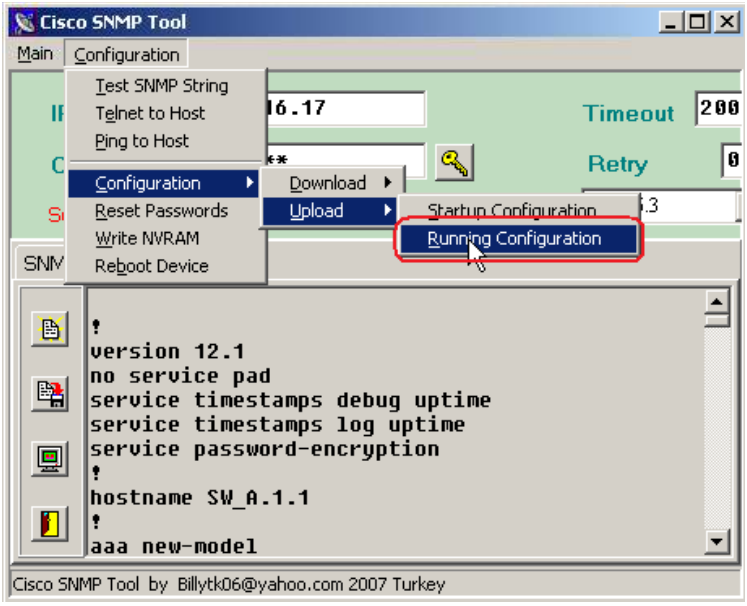
Caranya adalah sebagai berikut:



Gambar 3.37 Klik tombol load configuration fromfile



Gambar 3.38 Pilih file configurasi yang etlah diedit sebelumnya



Gambar 3.39 Upload Ke Running configuration ataupun Startup Configuration

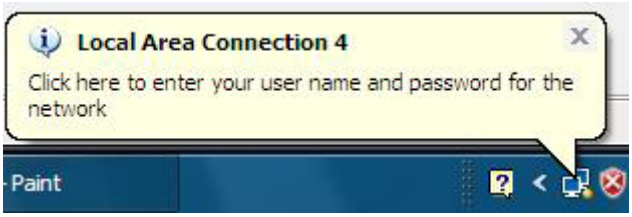
Dengan demikian, autentikasi 802.1x di sisi switch & port telah aktif

Keterangan :

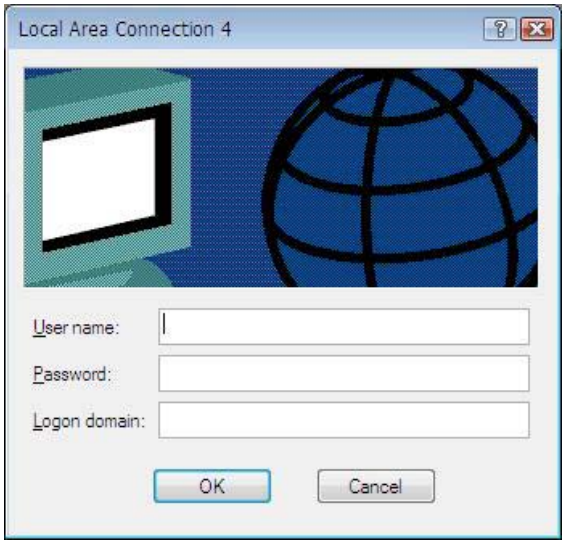
Untuk mengupload ke switch, dibutuhkan SNMP String dengan hak *Write.*

3.4 Pengetesan

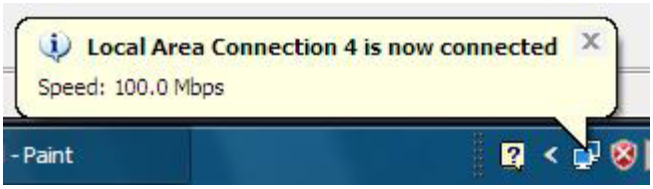
Untuk mengetahui apakah konfigurasi radius telah berfungsi, cara melakukan pengetesannya adalah sebagai berikut:



Gambar 3.40 Pasang kabel LAN, tunggu beberapa saat hingga muncul balon notifikasi di task bar



Gambar 3.41 Ketika balon notifikasi di klik, akan muncul dialog seperti di atas Masukkan Username & password saja, LOGON DOMAIN dikosongkan



Gambar 3.42 Apabila autentikasi berhasil, maka jaringan akan terkoneksi

3.5 Tips dan Troubleshooting

Adakalanya dalam proses pengerjaan setting switch maupun penerapan autentikasi dot1x berbasis RADIUS mengalami berbagai kendala. Berikut ini adalah error maupun *issue* yang sering muncul dalam proses penyettingan switch maupun server ACS.

3.5.1 Gagal mengakses telnet ke seitch karena lupa username atau password

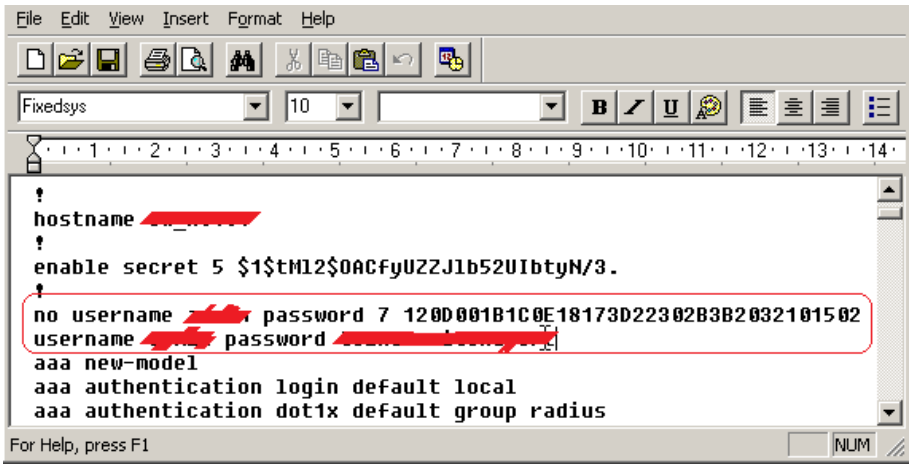
Permasalahan di atas bisa diatasi dengan cara yang cukup mudah tanpa harus me-*resetswitch* secara langsung. Yaitu dengan jalan meng-*uploadconfiguration script* yang baru

berisi pembatalan *username&password* lama sekaligus pengesetan *username & password* yang baru via *Cisco SNMP Tools*.

Syntax:

no username <username> password <password>

Username <username> password <password>



Gambar 3.43 Configuration script yang baru

3.5.1 Prompt Sudah Muncul Namun End User Gagal Authentukasi

Permasalahan di atas kemungkinan besar disebabkan adanya masalah di sisi *switch* maupun di sisi Server Cisco ACS.



Gambar 3.44 Gagal autentikasi

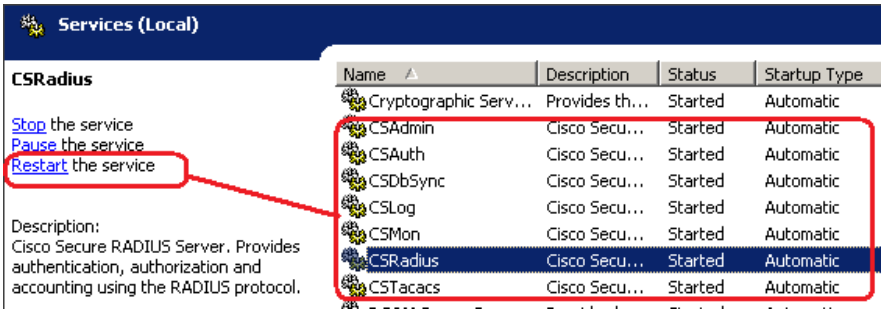
Pemecahannya adalah sebagai berikut (sesuai dengan penyebab permasalahannya):

- **Koneksi fisik dari *switch* ke *Cisco ACS* Server terputus**

Bisa dilacak dengan jalan melakukan tes ping dari Server ACS ke switch yang end usernya mengalami gagal autentikasi.

– **Service *Cisco ACS* Tidak berjalan sebagaimana mestinya**

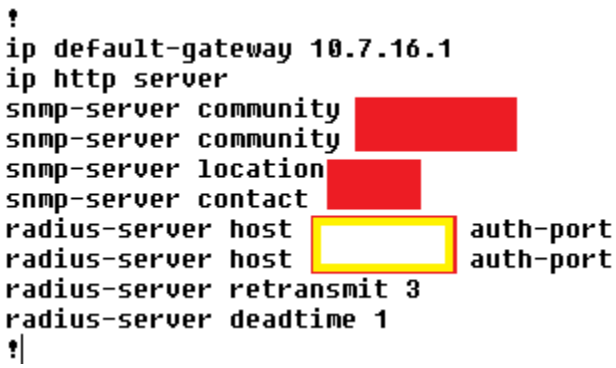
Masalah ini bisa terjadi ketika windows mengalami hard shutdown, misalnya ketika terjadi mati listrik. Untuk memperbaikinya, jalankan/restart semua service yang berhubungan dengan Cisco Secure ACS



Gambar 3.45 Restart service yang berhubungan dengan Cisco Secure ACS

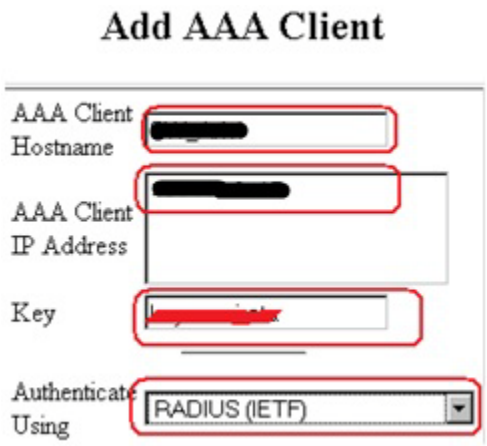
– **IP Address di switch configuration salah**

Bisa terjadi karena kesalahan pengetikan, atau keteledoran. Perbaikan bisa dilakukan secara online langsung via *telnet*, atau via *offline* kemudian diupload melalui *Cisco SNMP Tools*.



Gambar 3.46 Letak IP address di configuration script (kotak kuning)

– **Key antara di switch dengan di Cisco ACS tidak sesuai**



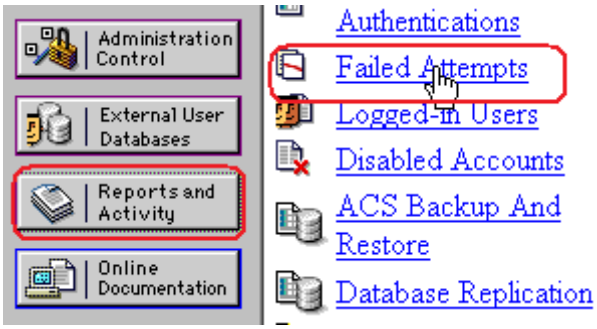
Gambar 3.47 Letak key di Cisco Secure ACS



Gambar 3.48 Letak key di configuration script

– **Username / Password salah**

Adakalanya autentikasi gagal karena end user lupa akan username & passwordnya. Untuk melacak hal ini, bisa dilihat di log yang terdapat di Cisco Secure ACS, yaitu di bagian *Failed Attempts*



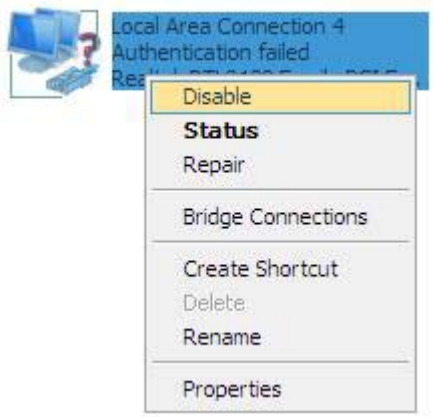
Gambar 3.49 Letak log Failed Attempts

Failed Attempts active.csv

Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	NAS-Port
09:06:28	Authen failed	HARTONO	Group 1	00-24-21-5C-F1-F9	CS CHAP password invalid	50003
09:02:43	Authen failed	HARY	..	00-24-21-5F-59-7A	CS user unknown	50003
08:42:44	Authen failed	00-0C-61-00-00-00	..	00-0C-61-00-00-00	CS user unknown	50006
08:13:31	Authen failed	00-11-D8-08-CE-98	..	00-11-D8-08-CE-98	CS user unknown	50020

Gambar 3.50 Daftar user yang gagal autentikasi & sebab kegagalannya

Apabila semua permasalahan-permasalahan telah diketahui & diperbaiki, tahap selanjutnya adalah mengulangi proses autentikasi dengan jalan merestart network adapter (*disable – enable*).



Gambar 3.51 Restart network adapter