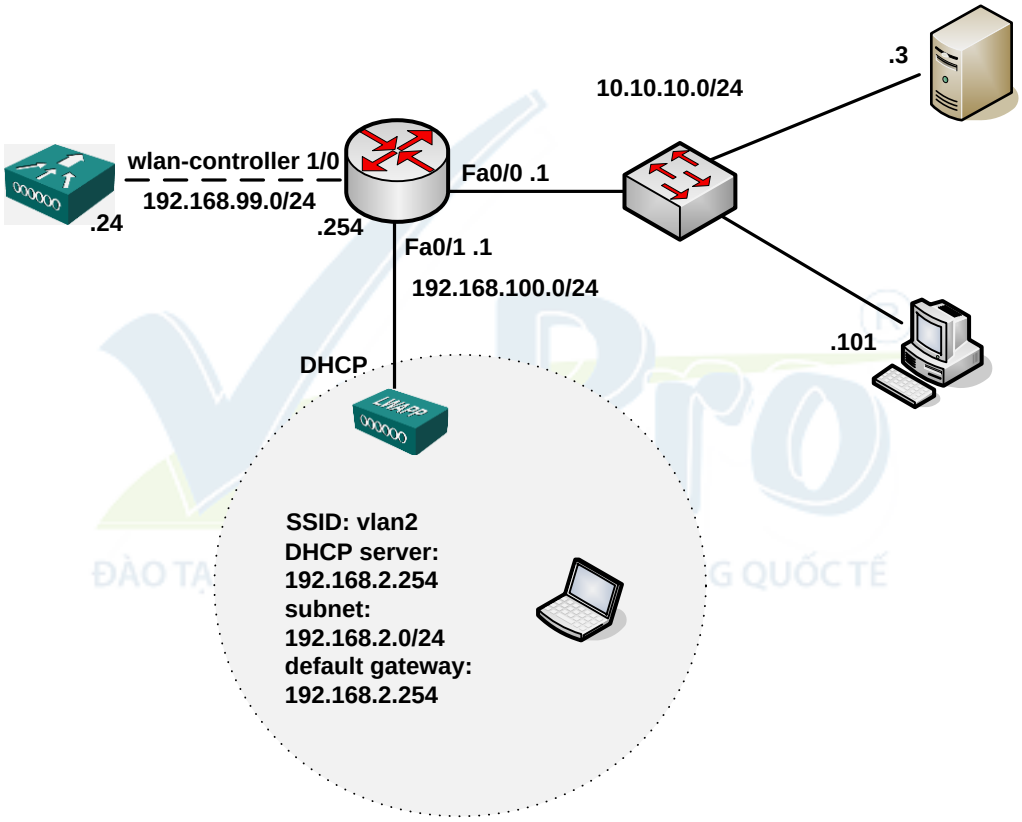
LAB 7: Dùng cơ chế bảo mật WPA cùng cơ chế xác thực dot1x dùng kiểu PEAP

Mô tả

Bài lab này mô tả cách sử dụng WPA trong bảo mật mạng wireless cùng cơ chế xác thực dot1x dùng cơ chế PEAP, các thiết bị dùng trong bài bao gồm ACS của Cisco, wireless client adapter chạy trên hệ điều hành WINXP service pack 3, WLAN Controller và Lightweight Access Point.

Sơ đồ



Hình 142

Thực hiện

Cấu hình cơ bản trên router:

```
C2811#sh run
Building configuration...

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c2811
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
enable secret 5 $1$QgGG$mjteEFA5x1onr2X3kuDp50
!
aaa session-id common
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.100.1
ip dhcp excluded-address 10.10.10.1 10.10.10.100
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.2.254
!
ip dhcp pool 192.168.100.0
  network 192.168.100.0 255.255.255.0
  default-router 192.168.100.1
  option 43 ip 192.168.99.24
!
ip dhcp pool 10
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.1
!
ip dhcp pool vlan2
  network 192.168.2.0 255.255.255.0
  default-router 192.168.2.254
!
```

```
multilink bundle-name authenticated
!
username admin password 0 admin
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.0
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface wlan-controller1/0
no ip addresss
shutdown
!
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 4
!
!
scheduler allocate 20000 1000
```

Trước khi thực hiện bài lab này yêu cầu cài đặt thành công phần mềm ACS trên server làm vai trò máy chủ xác thực.

Bước 1: Cấu hình cơ bản router 2811 và WLC module.

Cấu hình địa chỉ IP trên interface W1/0 của Router 2811.

```
c2811#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c2811(config)#
c2811(config)#interface wlan-controller 1/0
c2811(config-if)#ip address 192.168.99.254 255.255.255.0
c2811(config-if)#no shut
```

Truy cập vào WLC module từ Router 2811:

```
c2811#service-module wlan-controller 1/0 session
Trying 192.168.99.254, 2066 ... Open
```

Cấu hình WLC từ chế độ SETUP MODE như hình 143.

Sau khi khởi động lại WLC, tiến hành các bước như sau:

a. Sau khi WLC khởi động xong, truy cập vào WLC từ Router 2811, nhập username: cisco và password: cisco để vào WLC.
b. Để quay trở lại router 2811, nhấn tổ hợp phím **ctrl+shift+6** thả ra và nhấn tiếp phím **x.**
c. Kiểm tra đảm bảo Router có thể ping thấy WLC module.


```
c2811#ping 192.168.99.24
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.24, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4
ms
c2811#service-module wlan-controller 1/0 session
Trying 192.168.99.254, 2066 ... Open
```

d. Ping kiểm tra kết nối IP đến WLC.

Ghi chú: cần đồng bộ thời gian giữa WLC module và router 2811, trong trường hợp này router 2811 sẽ được cấu hình trở thành bộ đồng bộ thời gian chính (source clock).

```
C2811#conf t
C2811(config)#ntp master 2
```

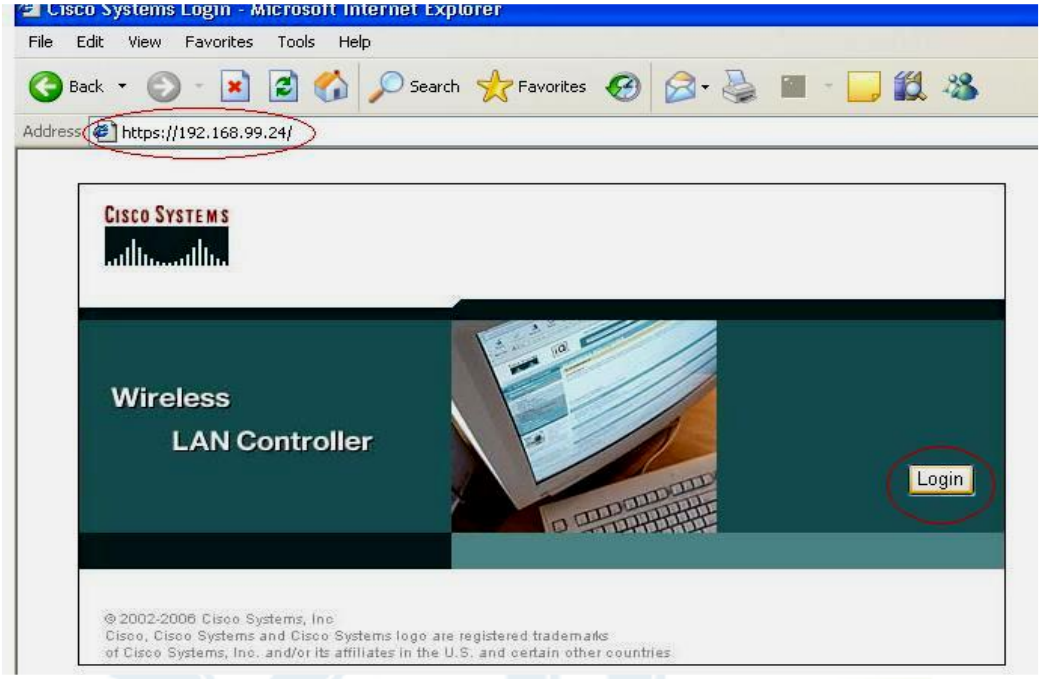
Cisco Controller

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_ff:f6:a0]: NMWLC
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (24 characters max): cisco

Management Interface IP Address: 192.168.99.24
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.99.254
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1]: 1
Management Interface DHCP Server IP Address: 192.168.99.24

AP Manager Interface IP Address: 192.168.99.25

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.99.24): 192.168.99.24

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mg1

Network Name (SSID): wl15
Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: YES
Enable 802.11a Network [YES][no]: YES
Enable 802.11g Network [YES][no]: YES
Enable Auto-RF [YES][no]: no
Configuration saved!
Resetting system with new configuration...
```

Hình 143

Bước 2: Dùng PC cấu hình WLC bằng https.

Truy cập vào WLC bằng web, dùng firefox hoặc IE nhập vào https://192.168.99.24 (hình 144).

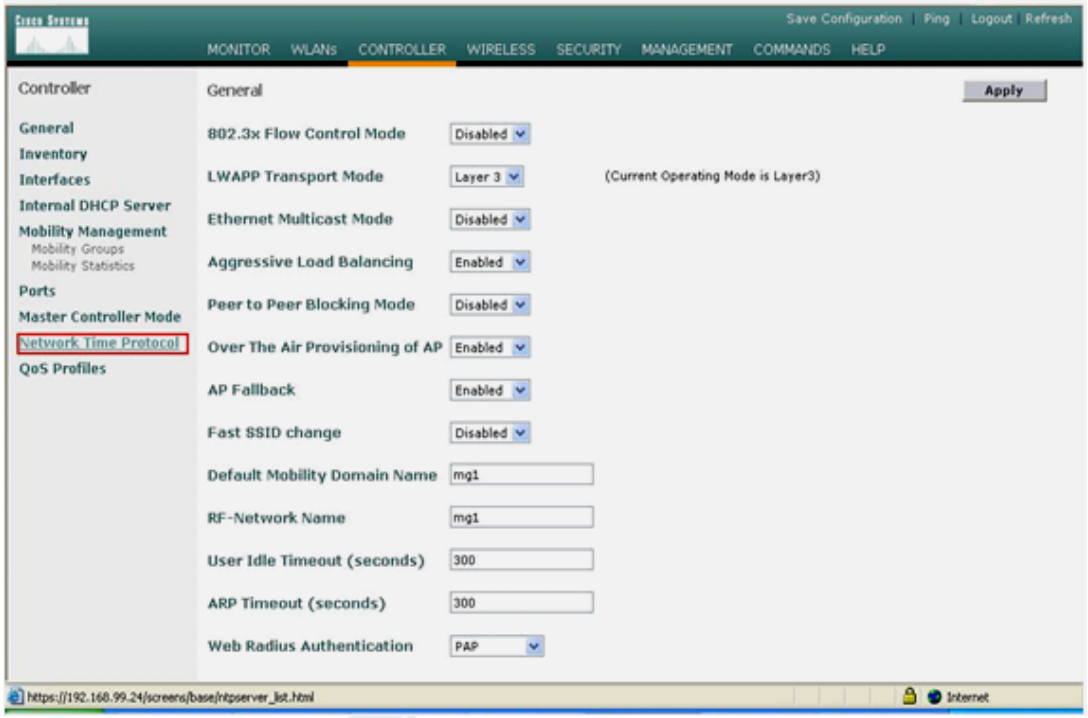


Hình 144

Chọn Login, nhập username: cisco, password: cisco (username và password cấu hình trong bước 1) - hình 145.

Hình 145

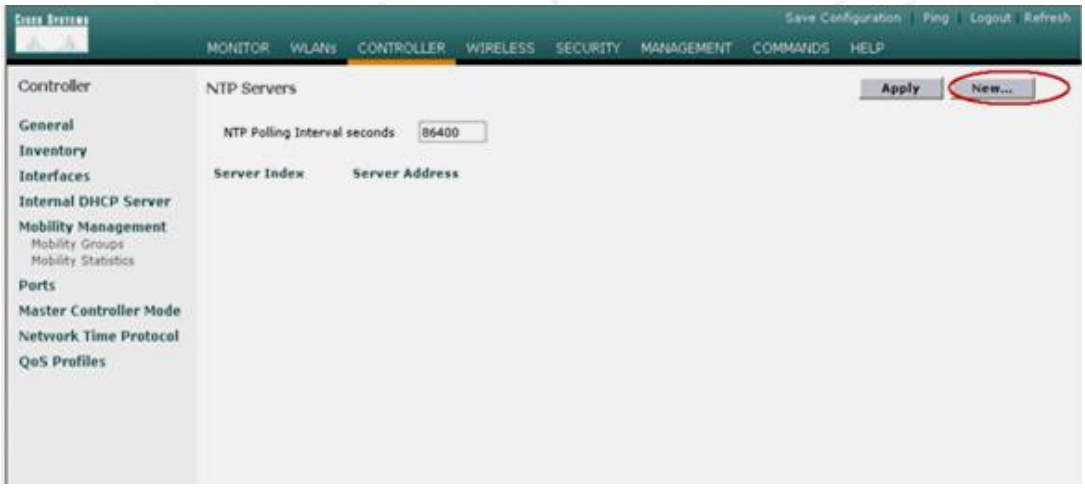
Cấu hình đồng bộ thời gian cho WLC với R2811 (hình 146).



Hình 146

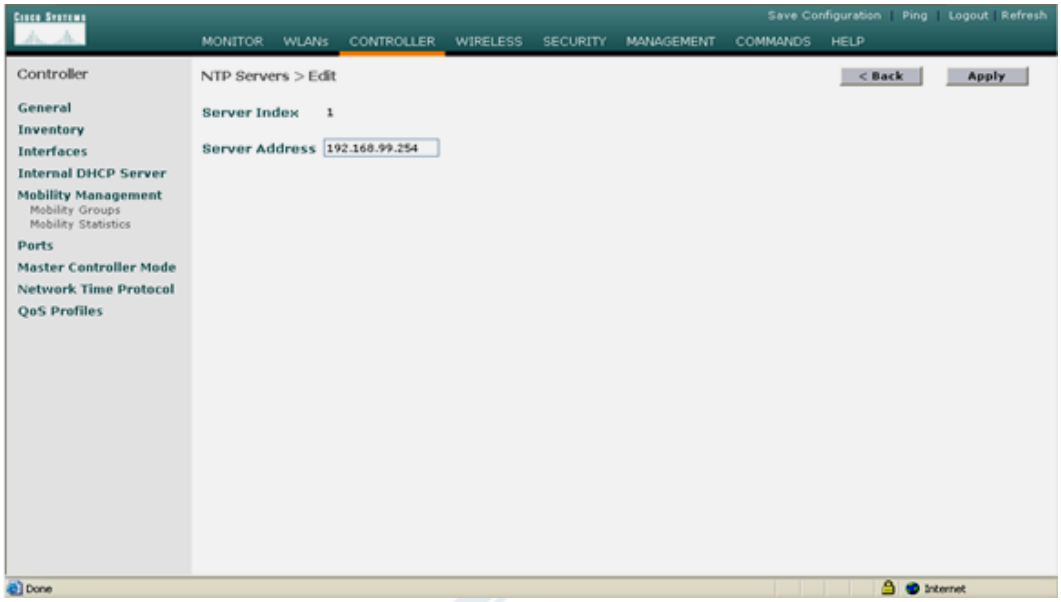
Chọn New để khai báo thời gian mới cho server (hình 147), cần cấu hình trên router 2811 là thiết bị cấp thời gian clock chủ đạo dùng câu lệnh:

```
R2811(config)#ntp master 2.
```



Hình 147

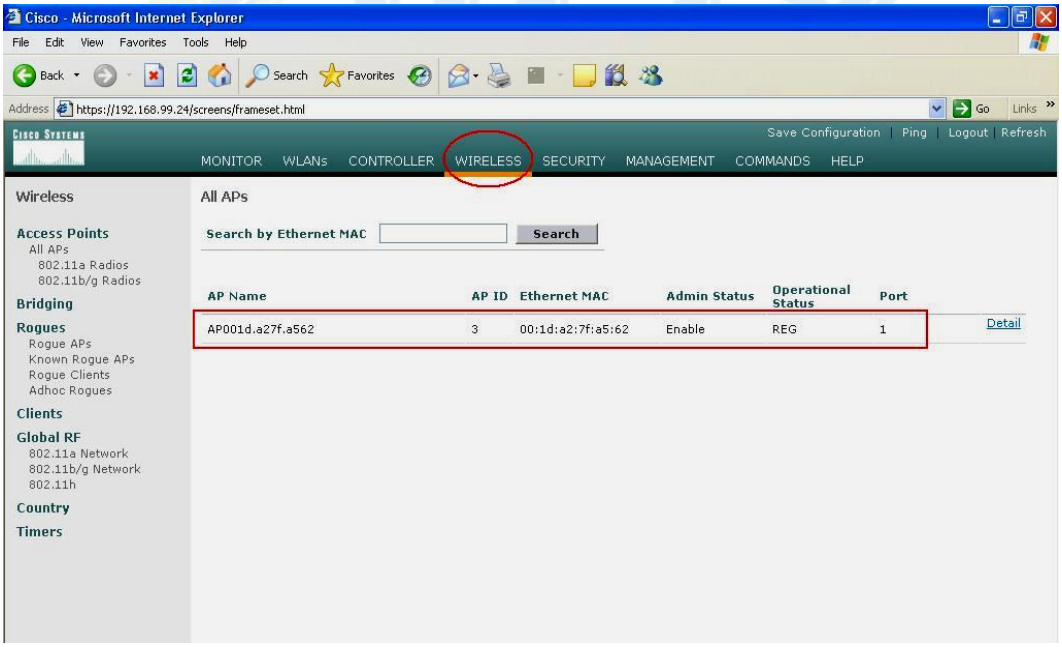
Chọn Apply (hình 148).



Hình 148

Khi LWAP bật lên sẽ được nhận địa chỉ IP từ Router 2811 cùng với option 43 chỉ sự tồn tại của WLAN Controller, quá trình đăng ký sẽ tự động thực hiện.

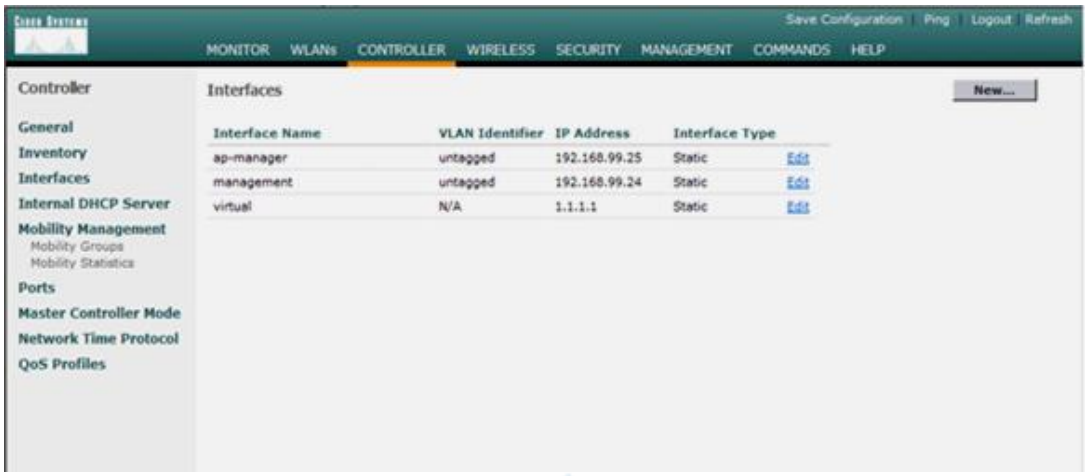
Khi quá trình đăng ký thành công thì trên WLC sẽ có kết quả như sau, chú ý cột Operational Status có trạng thái REG (registered – đã đăng ký) – hình 149.



Hình 149

Cấu hình các thông số cho Wireless Client (hình 150).

- Chọn **Controller > Interfaces > New**.

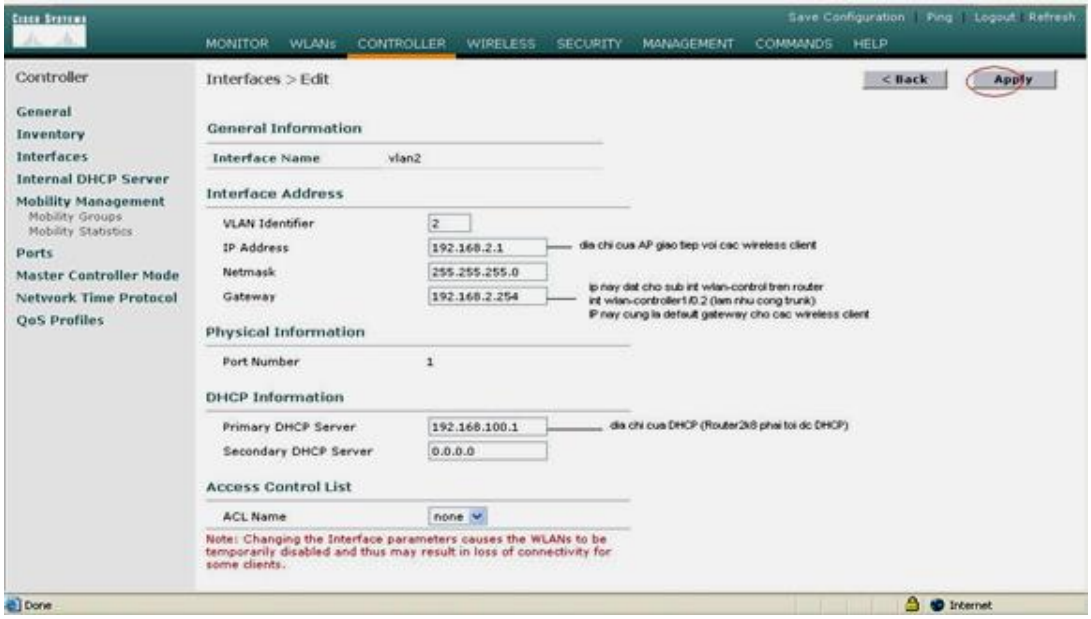


Hình 150

Nhập tên Interface và VLAN (trong trường hợp này giả định wireless client dùng vlan2 có địa chỉ mạng 192.168.2.0/24) sau đó click **Apply.**

Cửa sổ sau sẽ xuất hiện sau khi đã nhập vào tên Interface và VLAN.

Nhập địa chỉ IP (địa chỉ này đại diện một giao tiếp trên thiết bị WLC), Netmask, Gateway và địa chỉ IP của DHCP Server, click **Apply** (hình 151).



Hình 151

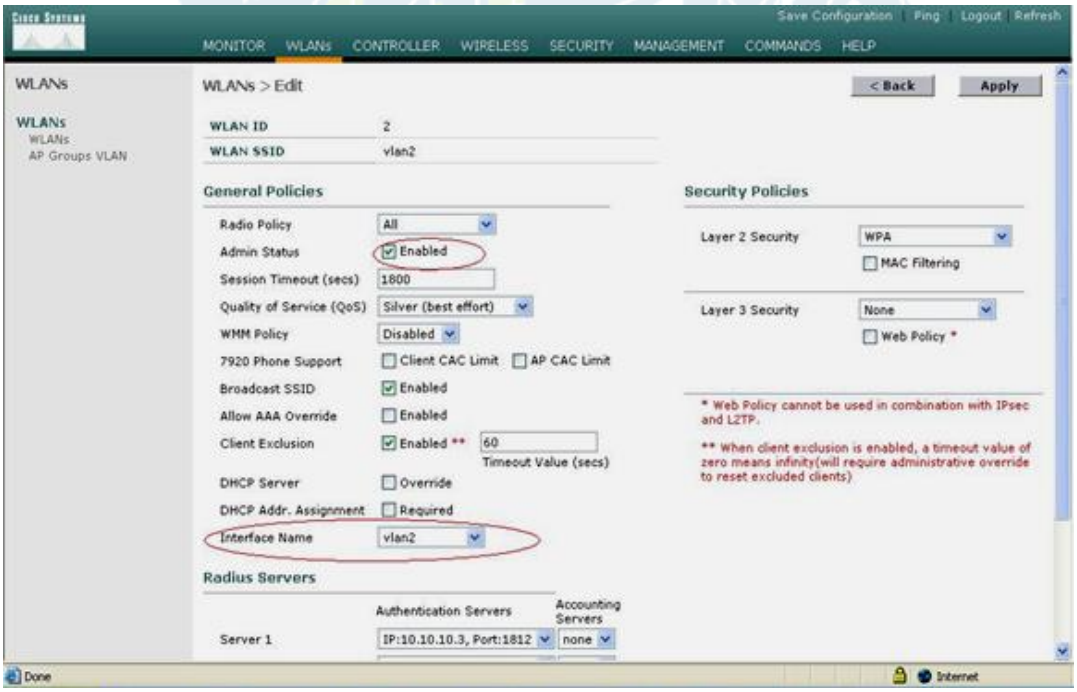
Kiểm tra lại cấu hình.

Kết quả thu được (hình 152).

Hình 152

- Chọn tab **WLANs** trên thanh menu ở góc trên cửa sổ, và click **New…**
- Nhập vào service set identifier (SSID) là **vlan2** và click **Apply**.
- Chọn **vlan2** từ thanh thực đơn **Interface Name** ở cuối cửa sổ, và click **Apply** (hình 153).

  Trong trường hợp này, SSID vlan2 được kết hợp với **Interface Name vlan2**.



Hình 153

Trên router 2811, cấu hình thêm cổng phục vụ cho lớp mạng 192.168.2.0/24 qua vlan 2 đồng thời cấu hình DHCP server cho lớp mạng này.

```
R1(config)# interface wlan-controller1/0.2
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip address 192.168.2.254 255.255.255.0
```

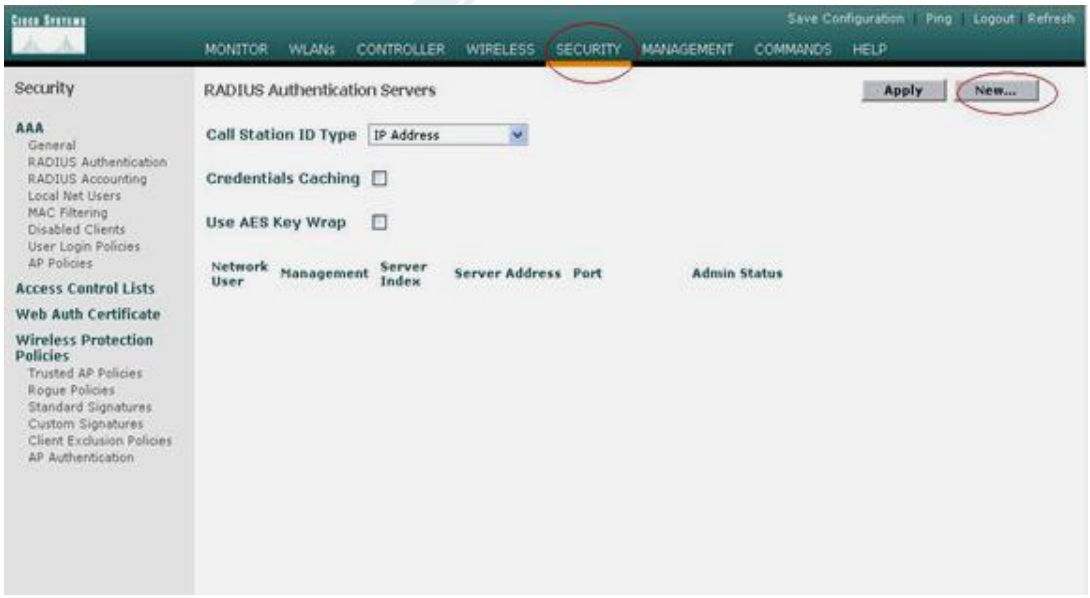
Cấu hình DHCP server trên router cấp địa chỉ động cho lớp mạng 192.168.2.0/24.

```
C2811#conf t
C2811(config)#ip dhcp pool vlan2
C2811(config-dhcp)# network 192.168.2.0 255.255.255.0
C2811(config-dhcp)# default-router 192.168.2.254
```

Bước 3: Cấu hình các tham số xác thực dot1x trên WLC.

Cấu hình khai báo sự tồn tại của Server Radius.

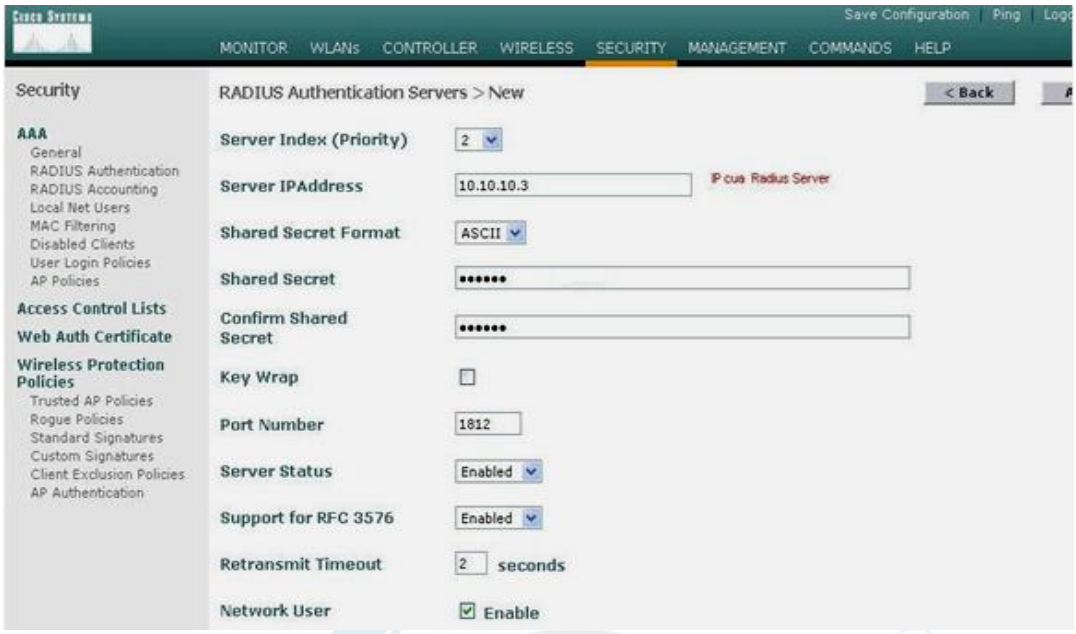
Chọn Security → New (hình 154).



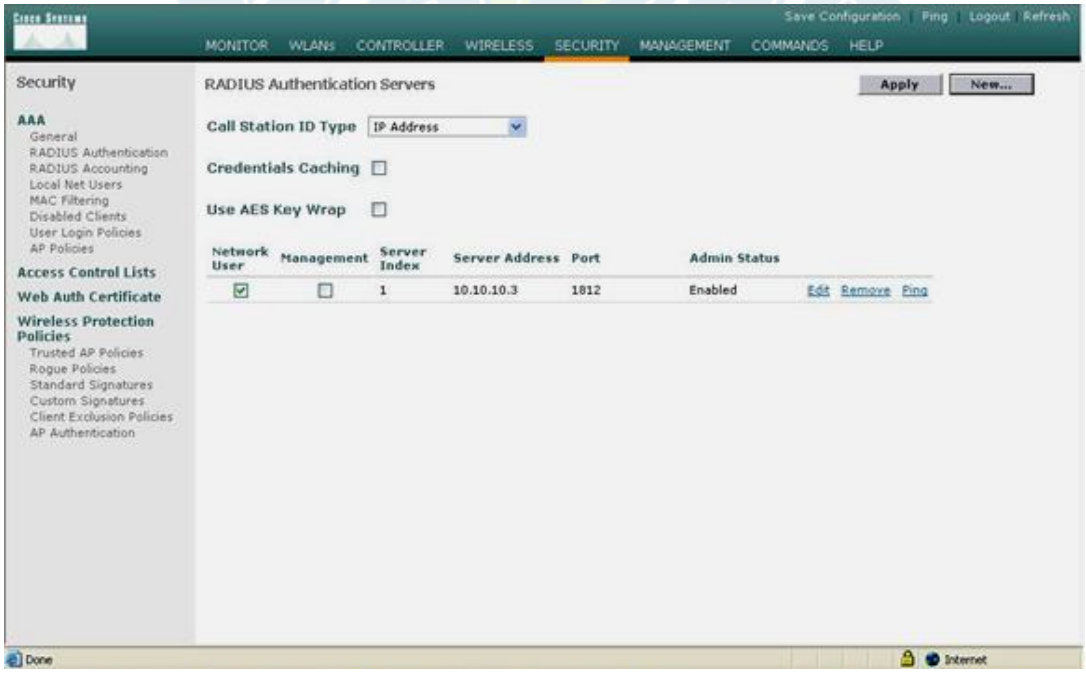
Hình 154

Khai báo sự tồn tại của ACS server (đóng vai trò máy chủ xác thực Radius) – hình 155.

Chọn Apply (hình 156).



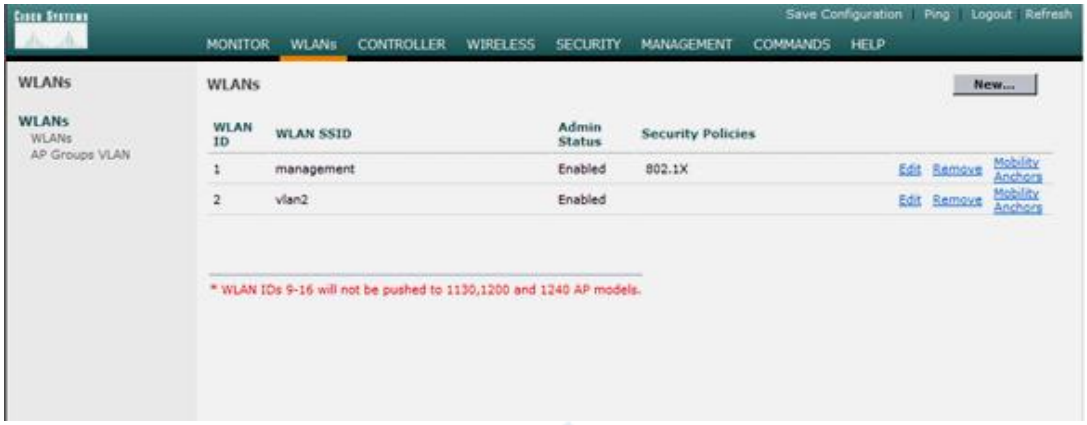
Hình 155



Hình 156

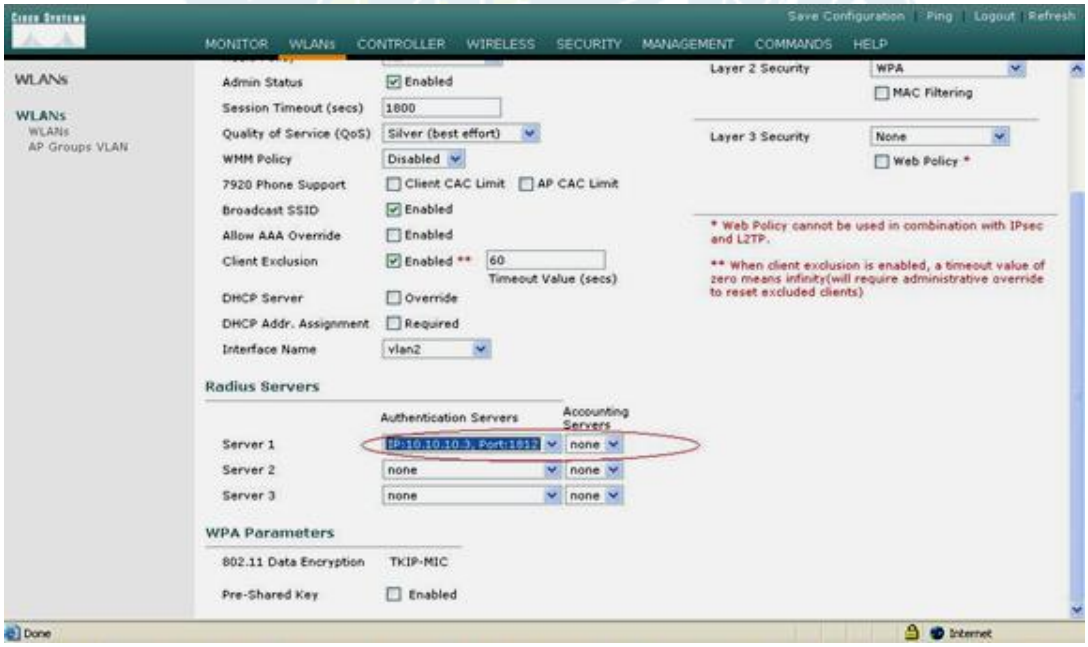
Cấu hình mô hình bảo mật WPA kết hợp cơ chế xác thực Dot1x dùng PEAP.

Vào WLAN để chọn kiểu xác thực, dùng edit để chỉnh sửa thông tin tương ứng (hình 157).



Hình 157

Chọn Layer 2 security dùng WPA, mặc định nếu không cấu hình xác thực preshare-key, cơ chế xác thực 802.1x sẽ được áp dụng. Khai báo thông tin của Radius server. Nhấn apply để hoàn tất cấu hình (hình 158). Nếu có câu hiển thị thông báo các client đang kết nối sẽ bị đứt kết nối chọn OK.



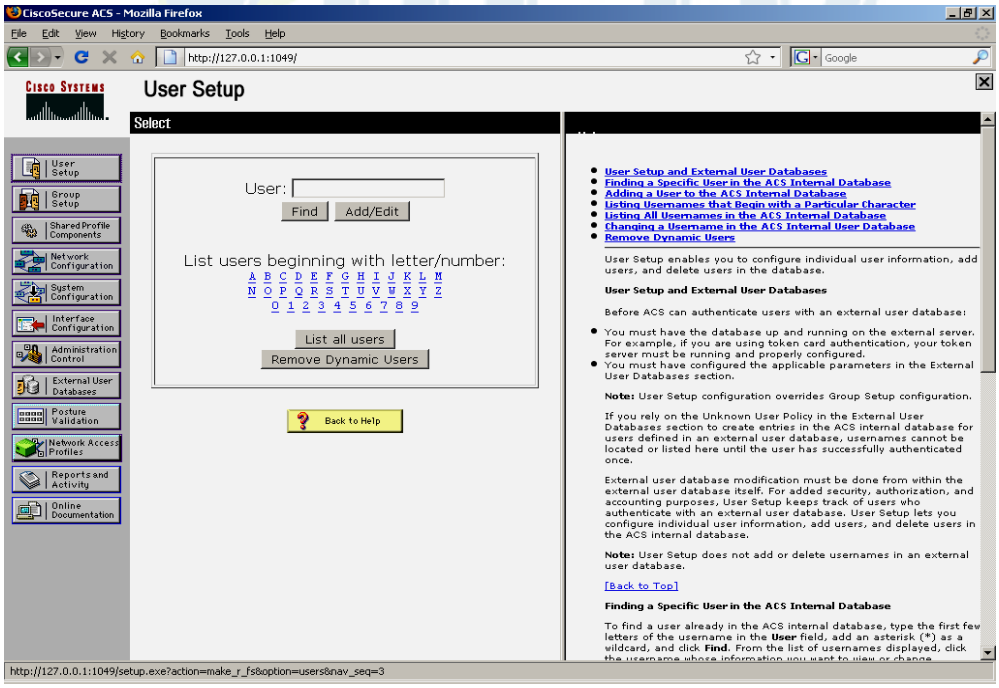
Hình 158

Cấu hình trên ACS hỗ trợ xác thực bằng PEAP.

Truy nhập vào đường liên kết cấu hình ACS (hình 159).

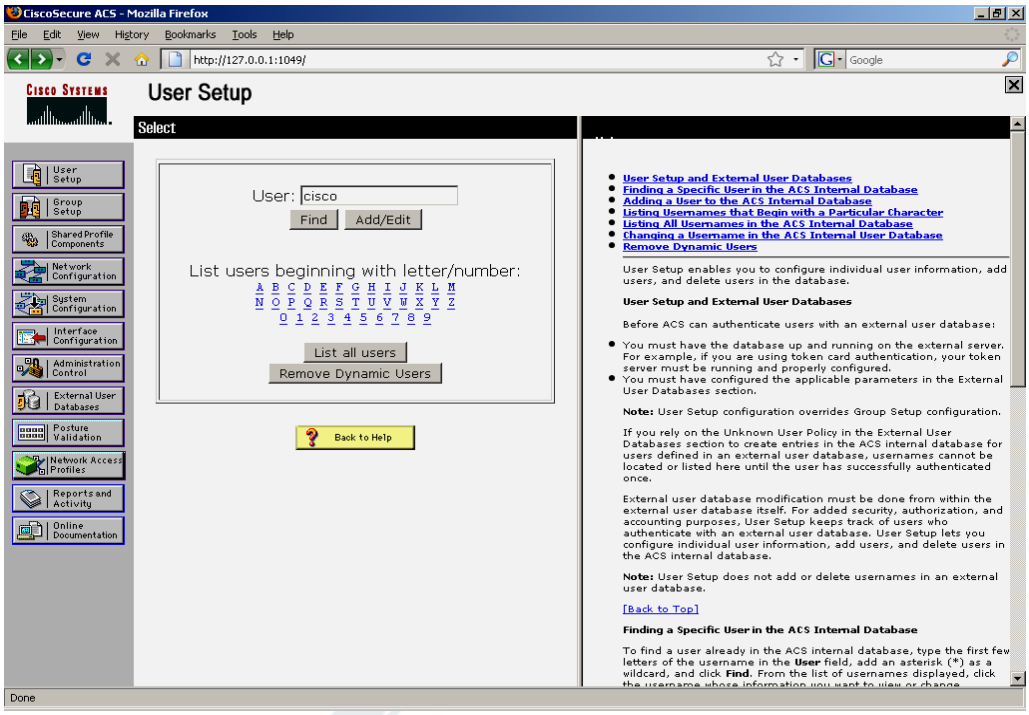
Hình 159

Tạo thêm tài khoản người dùng mới (hình 160).



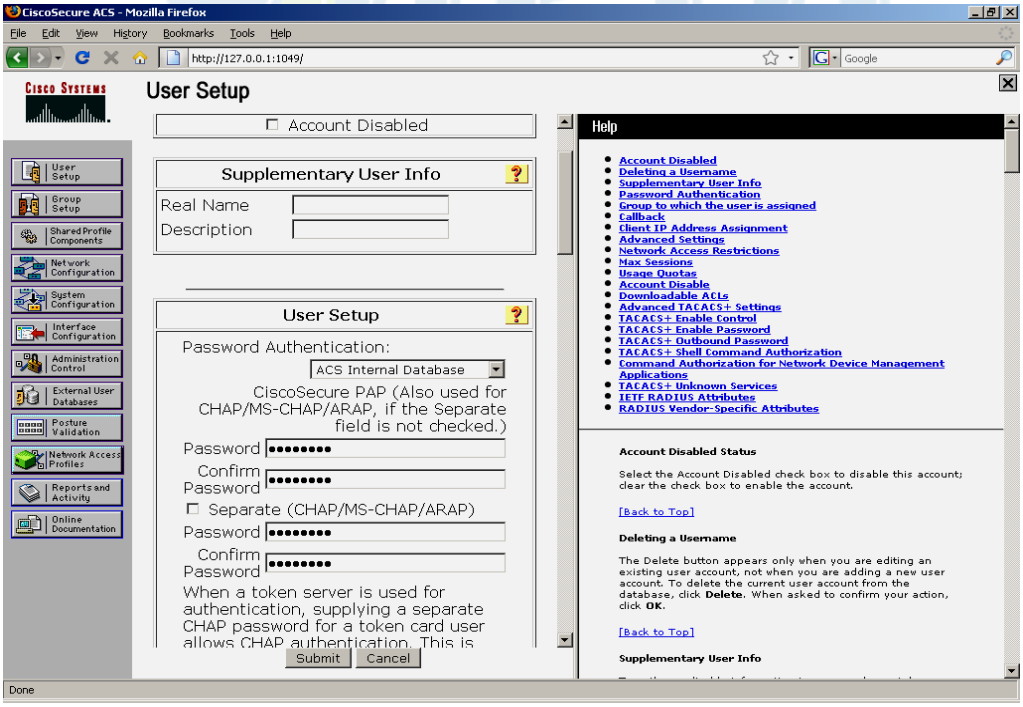
Hình 160

Nhập Username: cisco (hình 161).



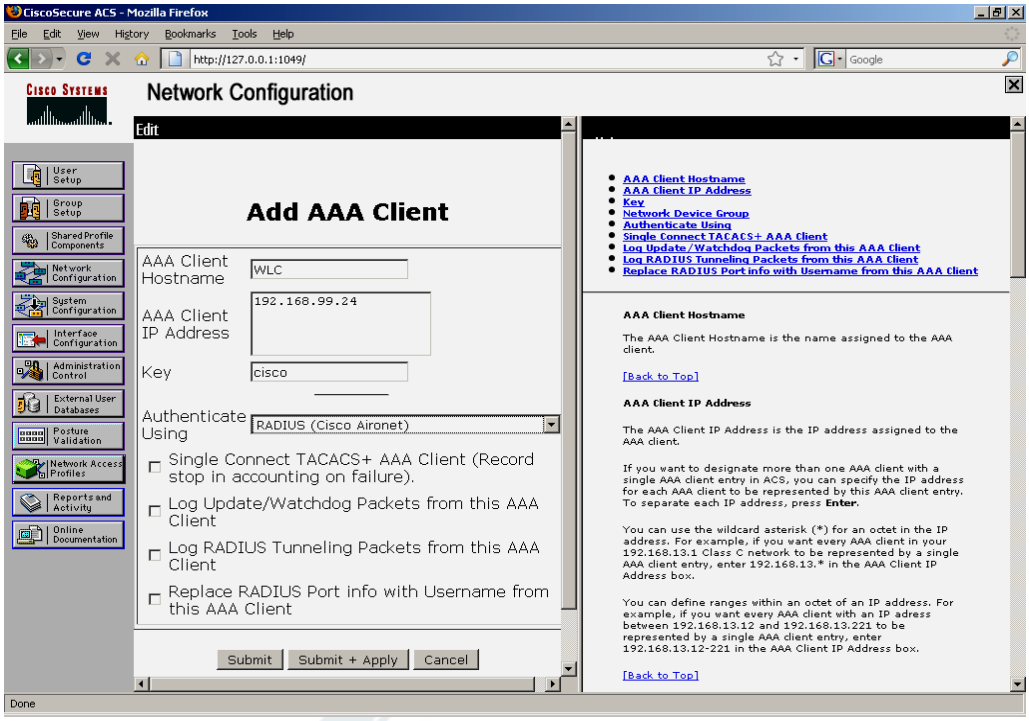
Hình 161

Nhập Password: cisco123 → chọn submit (hình 162).



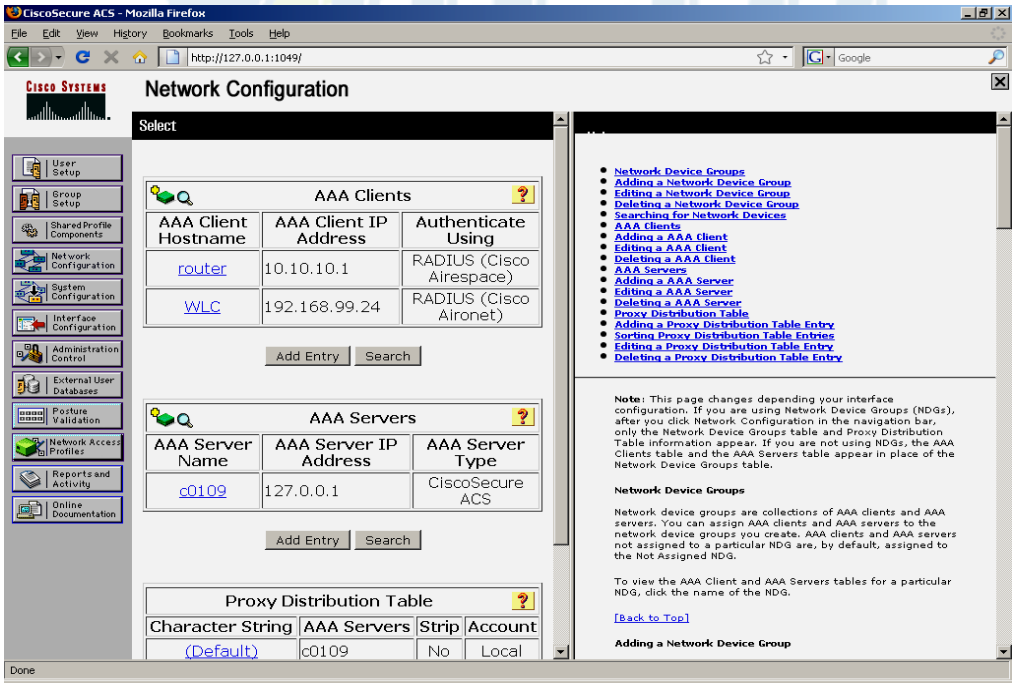
Hình 162

Khai báo sự tồn tại của WLC trên ACS (hình 163).



Hình 163

Chọn Submit + Apply và xem kết quả (hình 164).

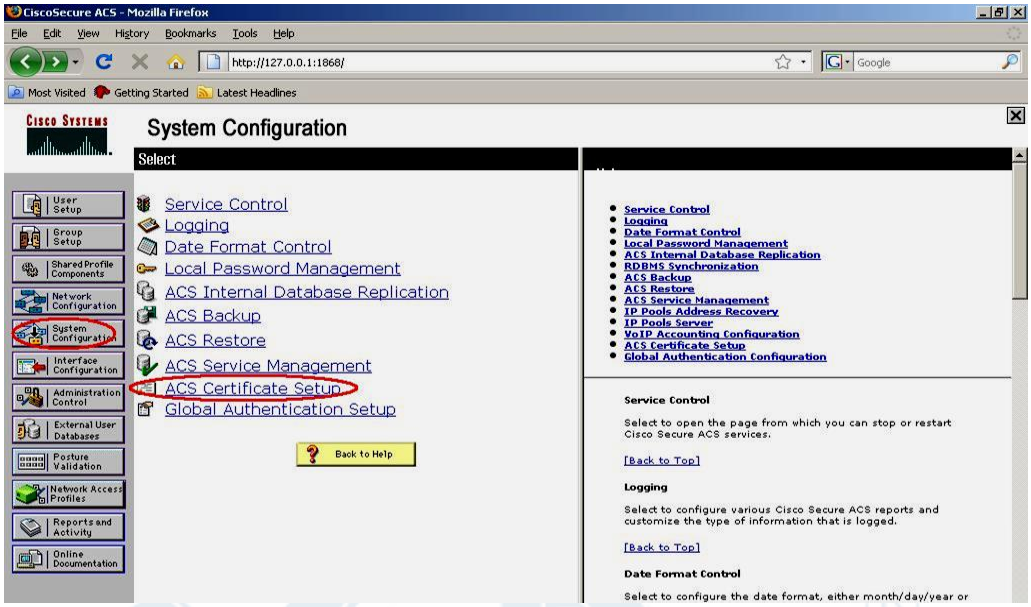


Hình 164

Khai báo kiểu xác thực PEAP trên ACS.

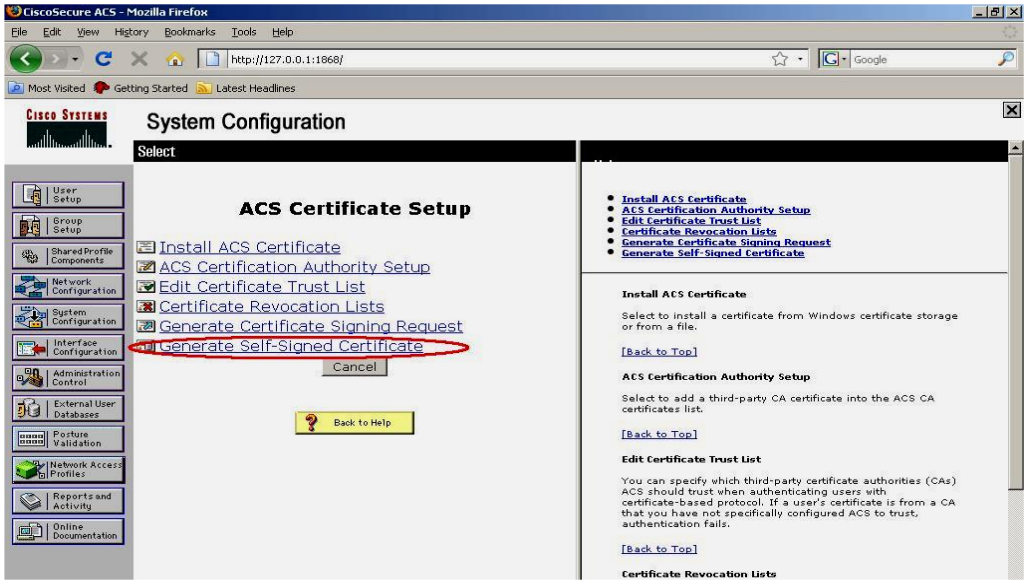
Để xác thực kiểu PEAP, ACS server phải có chứng thực điện tử, thực hiện thao tác tự tạo chứng thực điện tử trên server ACS.

Vào System configuration --> ACS Certificate Setup (hình 165).



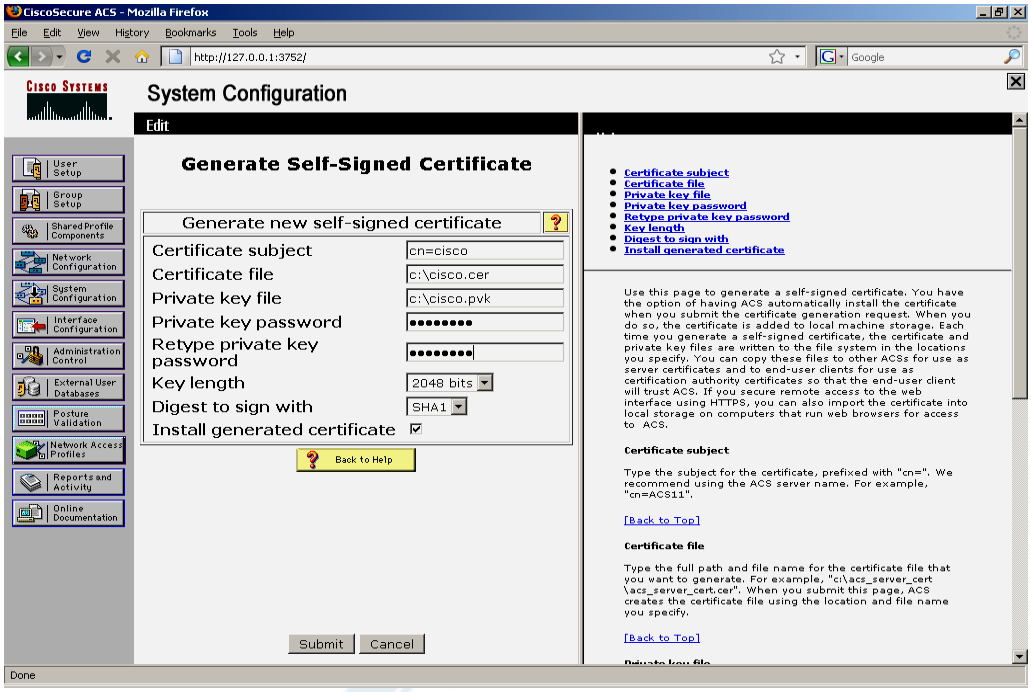
Hình 165

Chọn Generate Self-Signed Certificate, ACS sẽ tự tạo ra một chứng thực điện tử riêng cho mình (hình 166).



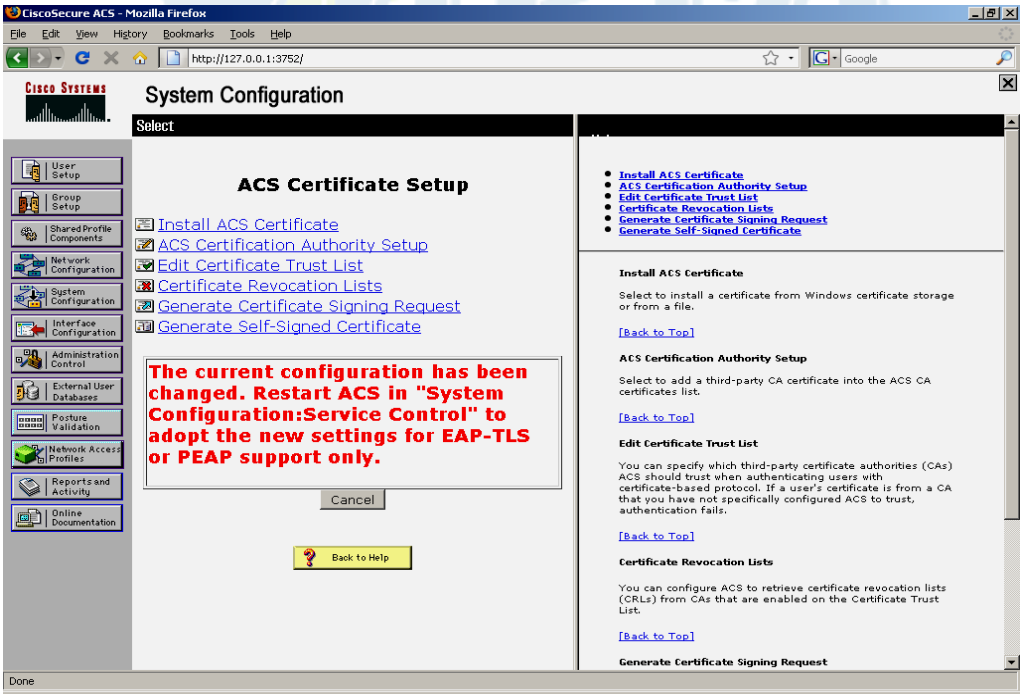
Hình 166

Nhập các thông tin cần thiết, sau đó chọn submit (hình 167).



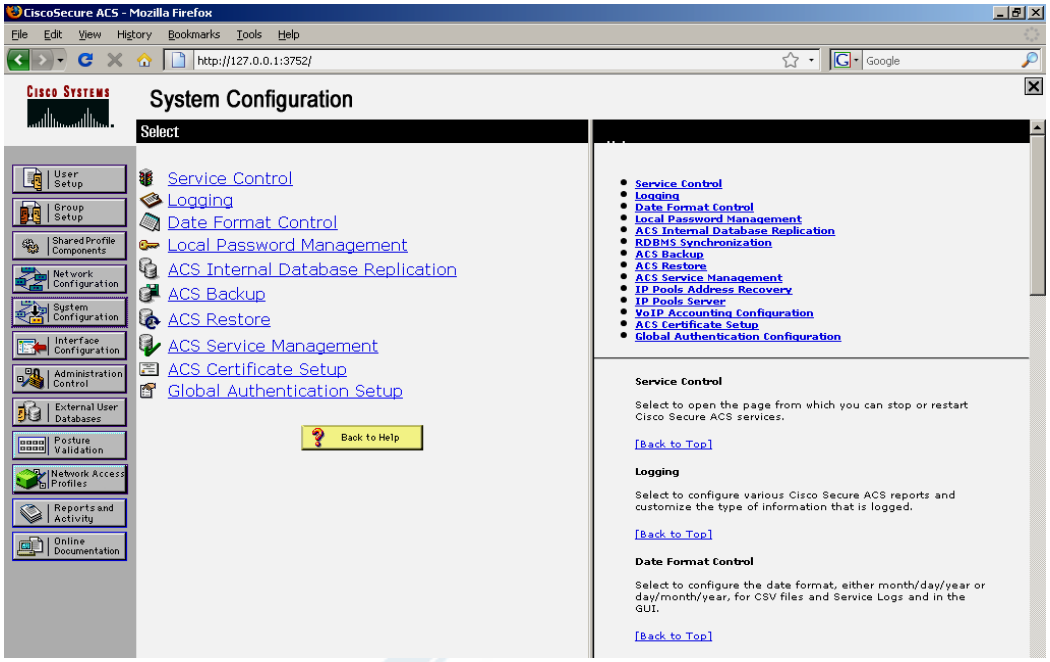
Hình 167

Xuất hiện thông báo sau (hình 168)



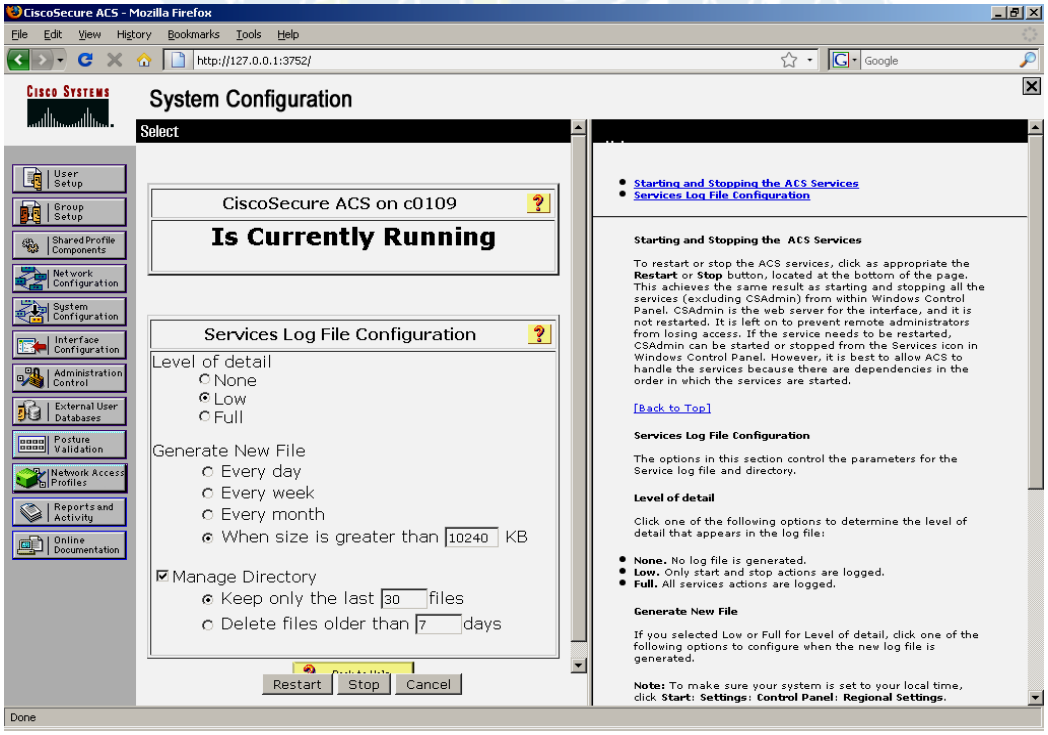
Hình 168

Vào system configuration --> Service Control (hình 169).



Hình 169

Chọn Restart, dịch vụ ACS sẽ được khởi tạo lại (hình 170).

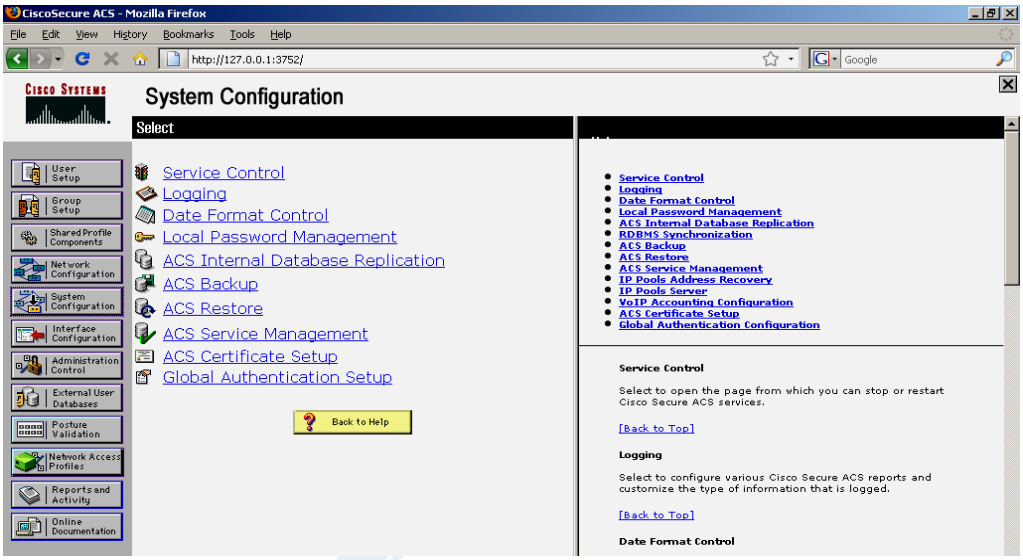


Hình 170

Có thể tiến hành kiểm tra lại trên thư mục C:/ trên server sẽ thấy có 2 file là cisco.cer và cisco.pvk trong thư mục này

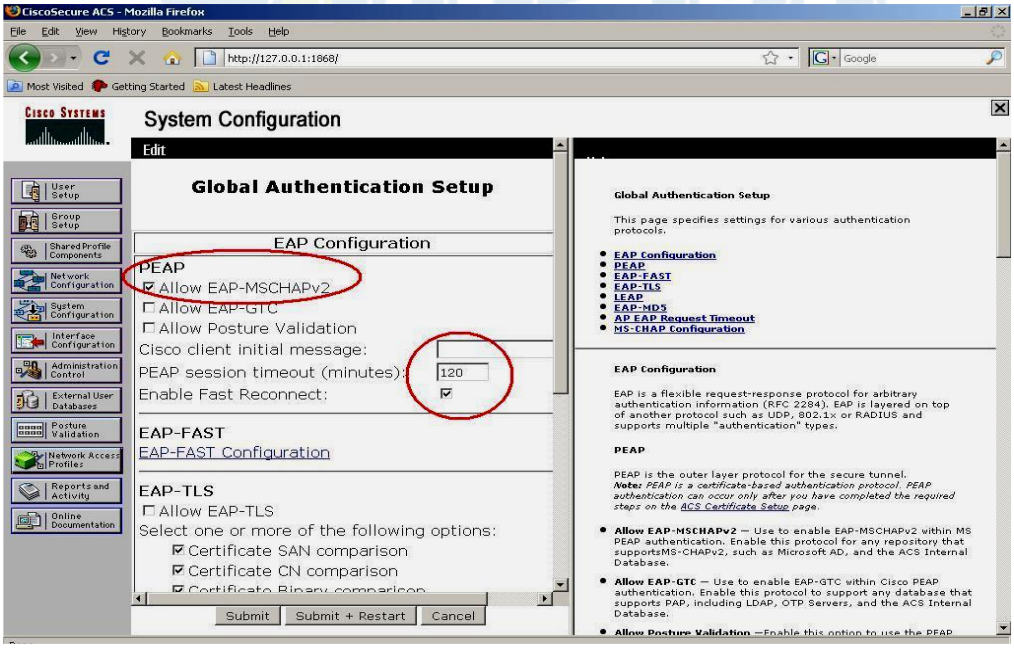
Cấu hình hỗ trợ cơ chế xác thực theo FAST.

Vào System Configuration --> Global Authentication Setup (hình 171).



Hình 171

Chọn liên kết cấu hình PEAP, chọn kiểu xác thực dùng EAP-MSCHAP v2 (hình 172).



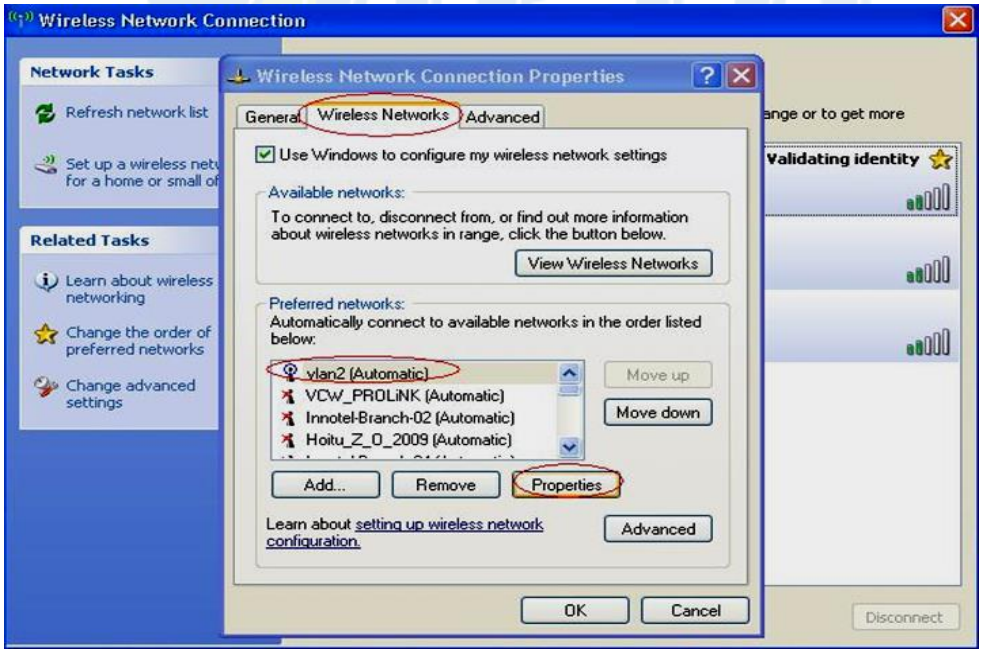
Hình 172

Cấu hình các bước cuối cùng trên PC.

Chép file cisco.cer qua PC rồi import vào PC (hình 173).

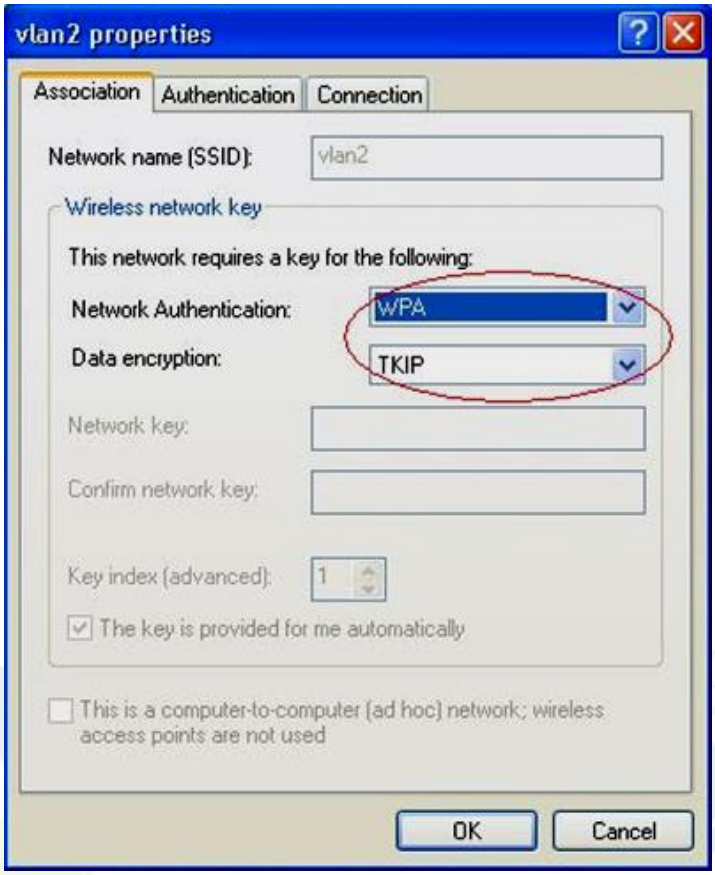
Hình 173

Xem thông tin của mạng wireless có SSID là vlan2, chọn Properties (hình 174).



Hình 174

Chọn phần xác thực Network Authentication là WPA, phần Data Encryption dùng TKIP (có thể dùng WPA2 nhưng phải cấu hình WPA2 trên Wireless Lan Controller) – hình 175.



Hình 175

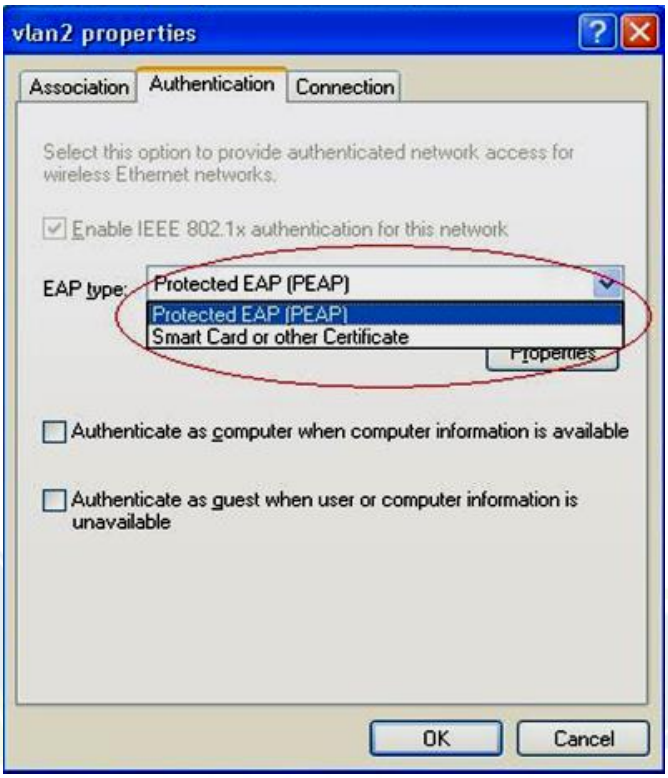
Chỉnh kiểu xác thực theo kiểu PEAP, chọn properties (hình 176).

Có thể tiến hành yêu cầu client xác thực Radius server, nếu chọn tùy chọn này, phải import certificate như đã hướng dẫn ở trên. Trong trường hợp không muốn client xác thực Radius Server, tức là chỉ xác thực 1 chiều, Radius Server xác thực client thì không cần chọn

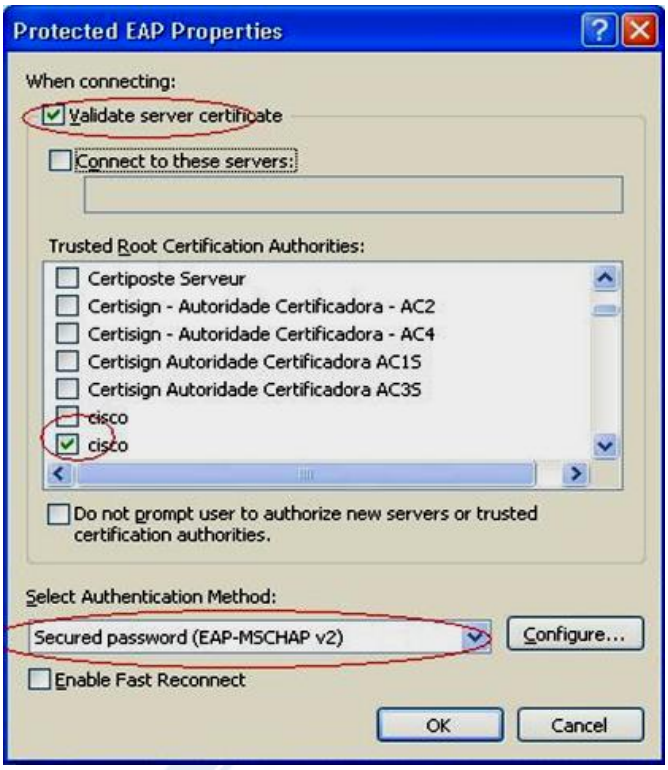
tùy chọn này cũng không cần import certificate. Chọn phần xác thực phía bên Client dùng là secured password. Nhấn OK (hình 177).

Khung thoại yêu cầu nhập thông tin tài khoản xác thực người dùng sẽ hiện ra, nhập thông tin tài khoản (hình 178). Quá trình xác thực sẽ diễn ra sau đó.

Nếu tài khoản nhập chính xác, quá trình liên kết và xác thực thành công (hình 179).

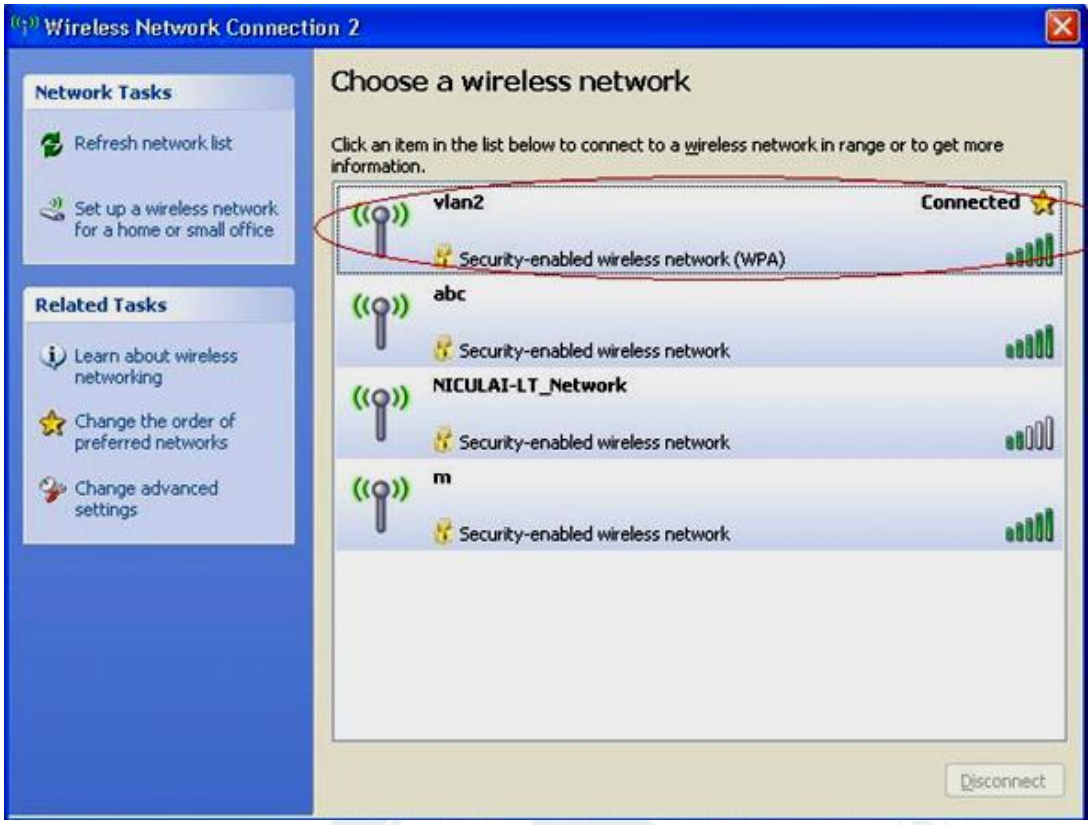


Hình 176



Hình 177

Hình 178



Hình 179