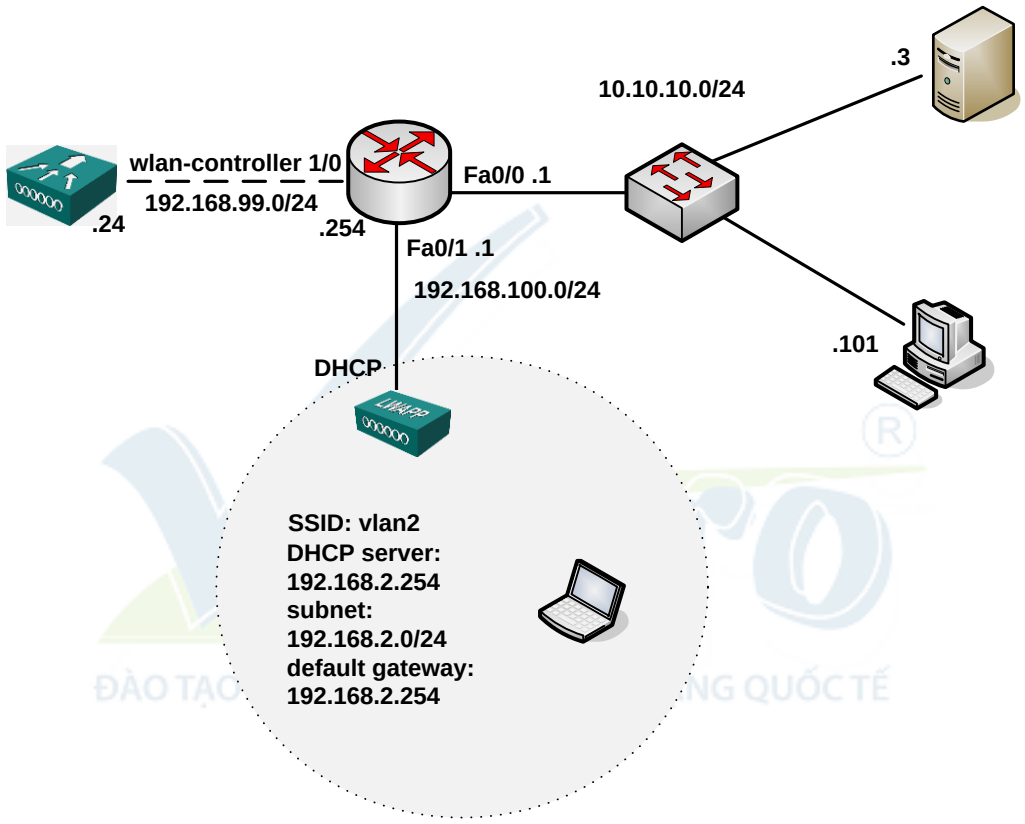
LAB 6: Xác thực dot1x dùng kiểu FAST

Mô tả

Bài lab này mô tả cách xác thực dot1x dùng cơ chế FAST, các thiết bị dùng trong bài bao gồm ACS của Cisco, wireless client adapter của Cisco, WLAN Controller và Lightweight Access Point.

Sơ đồ



Hình 100

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
!
scheduler allocate 20000 1000
!
End
```

ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG QUỐC TẾ

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
c2811(config-if)#end
```

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 101.

Sau khi khởi động lại WLC,tiếp tục thực hiện các bước 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.

ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG QUỐC TẾ

```
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
```

Từ PC ping WLC kiểm tra kết nối IP đã thông.

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...
```

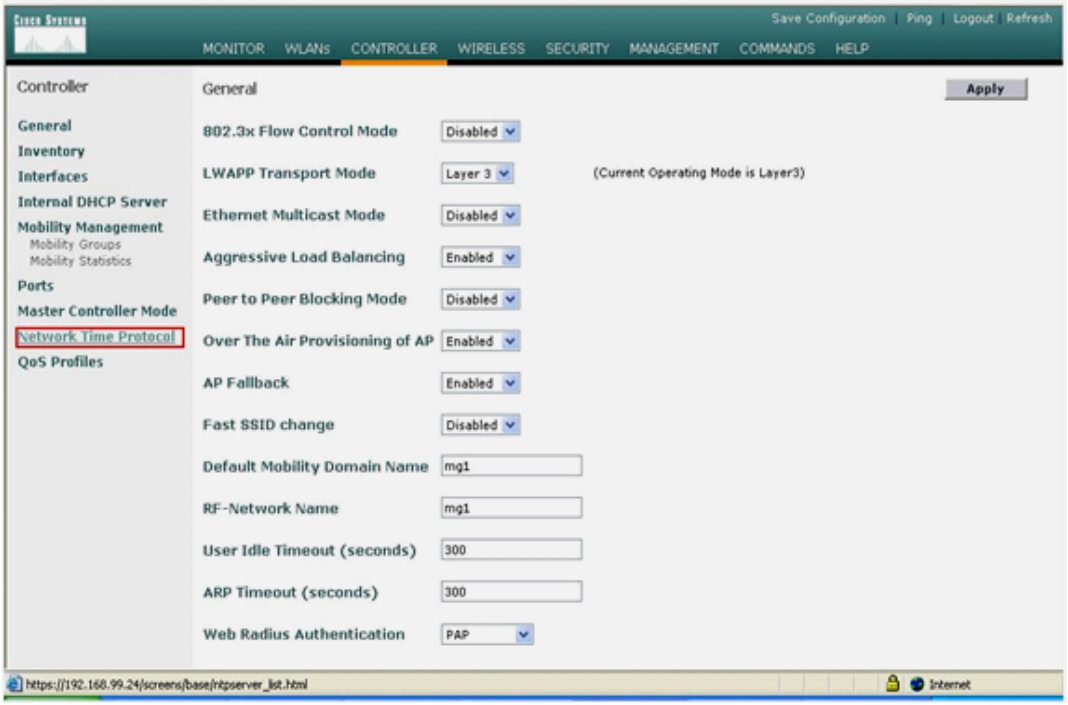
Hình 101

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. Chọn Login, nhập username: cisco, password: cisco (username và password cấu hình trong bước 1) – hình 102.

Hình 102

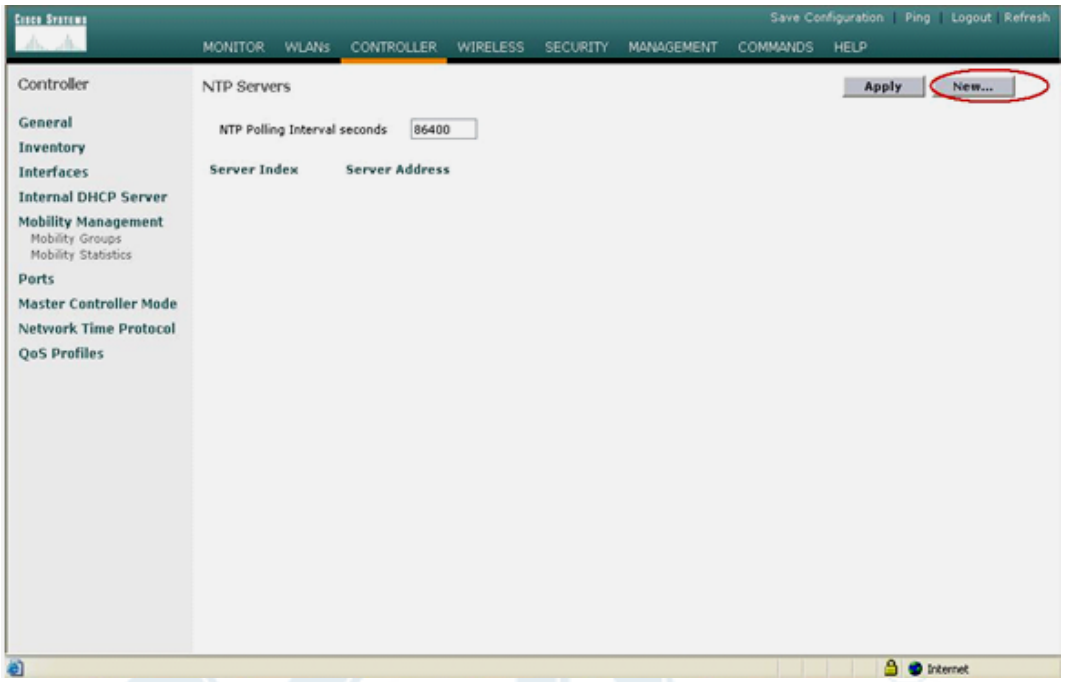
Cấu hình đồng bộ thời gian cho WLC với R2811 (hình 103).



Hình 103

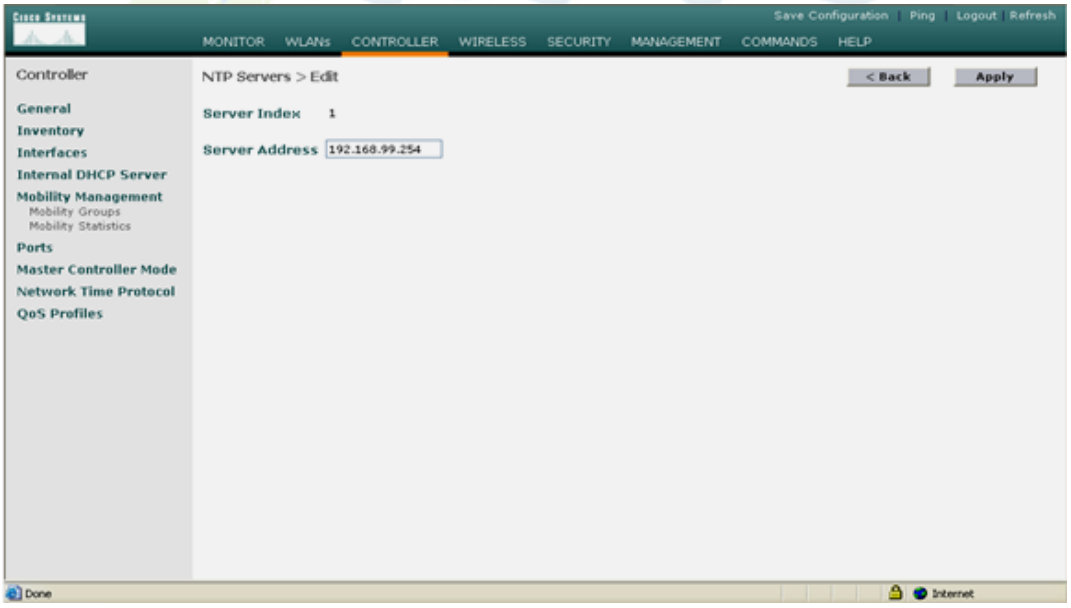
Chọn New để khai báo thời gian mới cho server (hình 104), cần cấu hình để router 2811 là thiết bị cấp thời gian clock chủ đạo. Sử dụng lệnh:

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



Hình 104

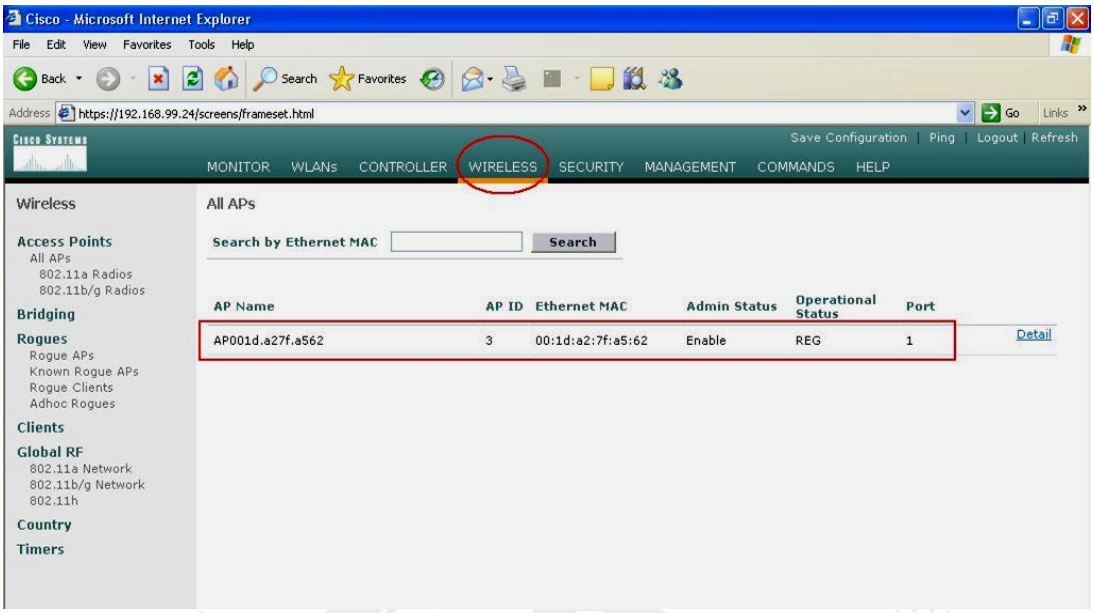
Chọn **Apply** (hình 105).



Hình 105

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.

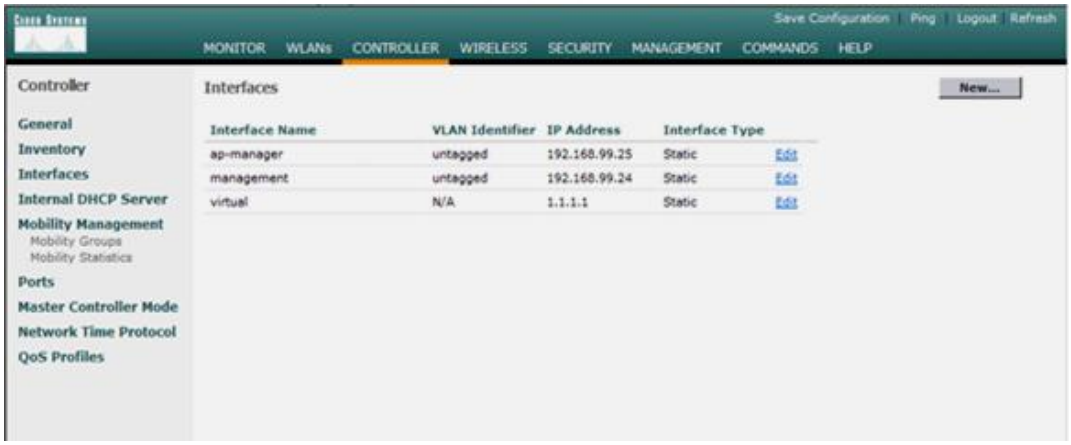
Khi quá trình đăng ký thành công thì trên WLC sẽ có kết quả như sau, chú ý cột Operational Status có trạng thái REG (registered – đã đăng ký) – hình 106.



Hình 106.

Cấu hình các thông số cho Wireless Client (hình 107).

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

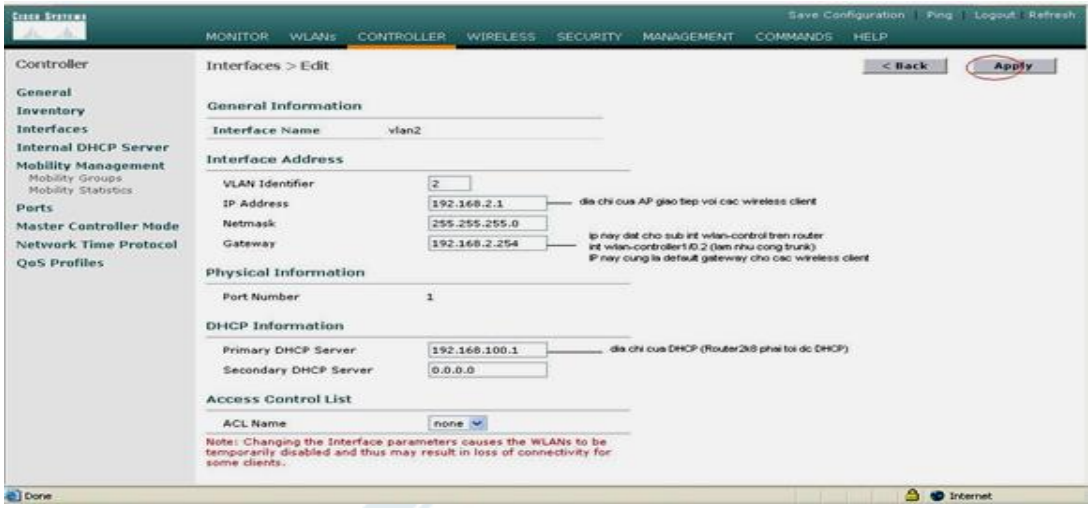


Hình 107

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.

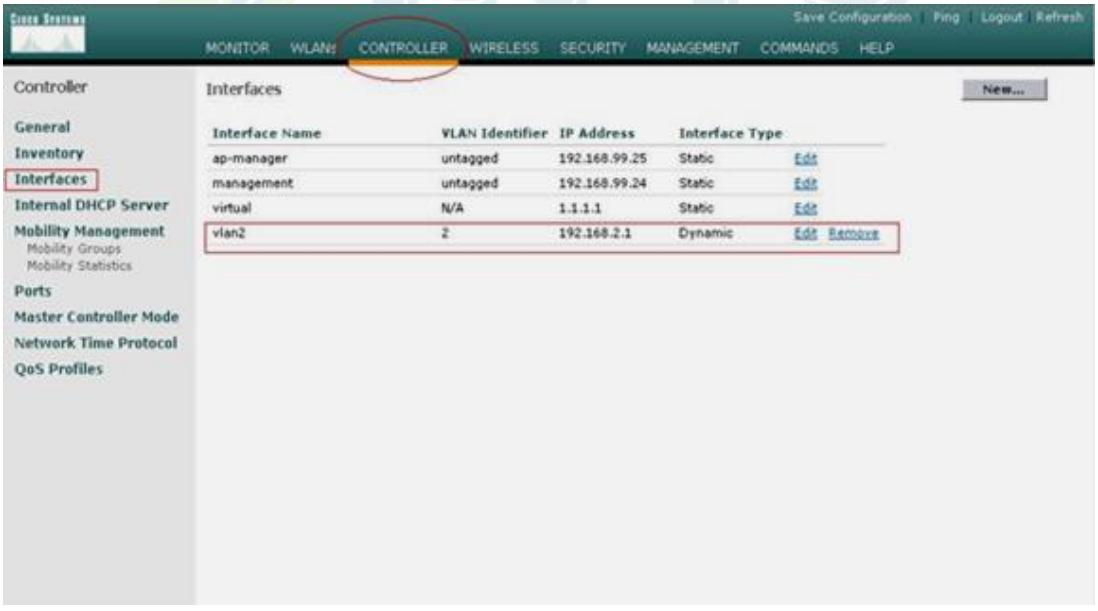
Nhập địa chỉ IP (địa chỉ này đại diện một giao tiếp trên thiết bị WLC), Netmask, Gateway và địa chỉ IP của DHCP Server, click **Apply** (hình 108).



Hình 108

Kiểm tra lại cấu hình.

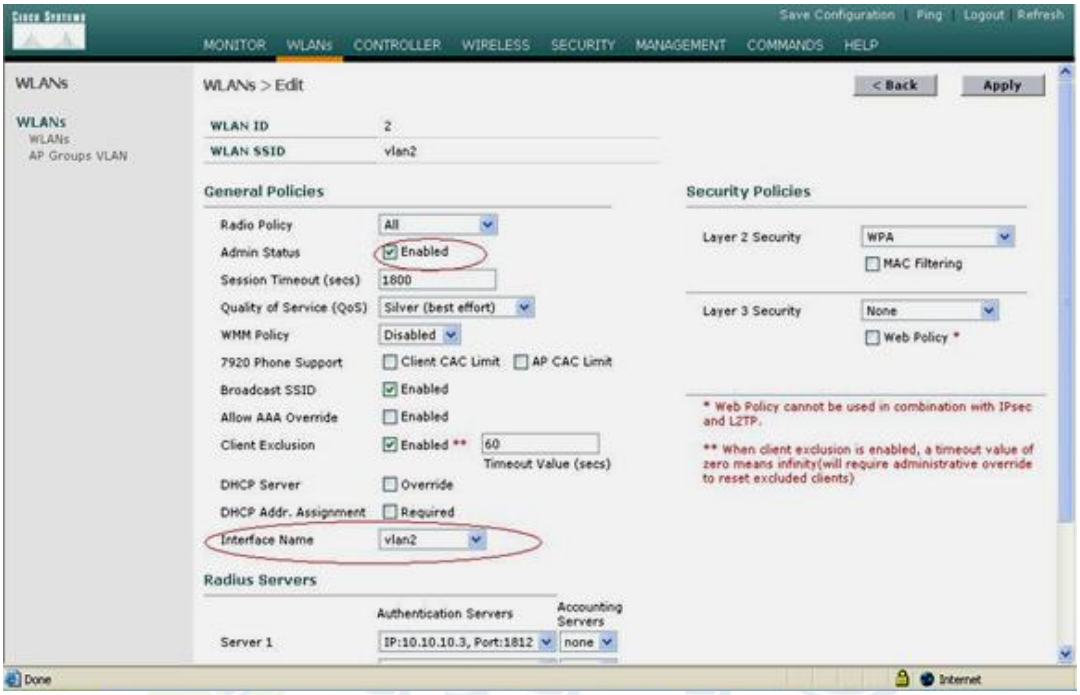
Kết quả thu được (hình 109).



Hình 109

- Chọn tab **WLANs** trên thanh menu ở góc trên cửa sổ, và click **New…**
- Nhập vào service set identifier (SSID). Trong ví dụ này, ta nhập vào SSID tên là **vlan2. C**lick **Apply.**
- Chọn **vlan2** từ thanh thực đơn **Interface Name** ở cuối cửa sổ, và click **Apply** (hình 110).

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



Hình 110

ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG QUỐC TẾ

Trên router 2811, cấu hình thêm cổng phục vụ cho lớp mạng 192.168.2.0/24 qua vlan2 đồng thời cấu hình DHCP server cho lớp mạng này.

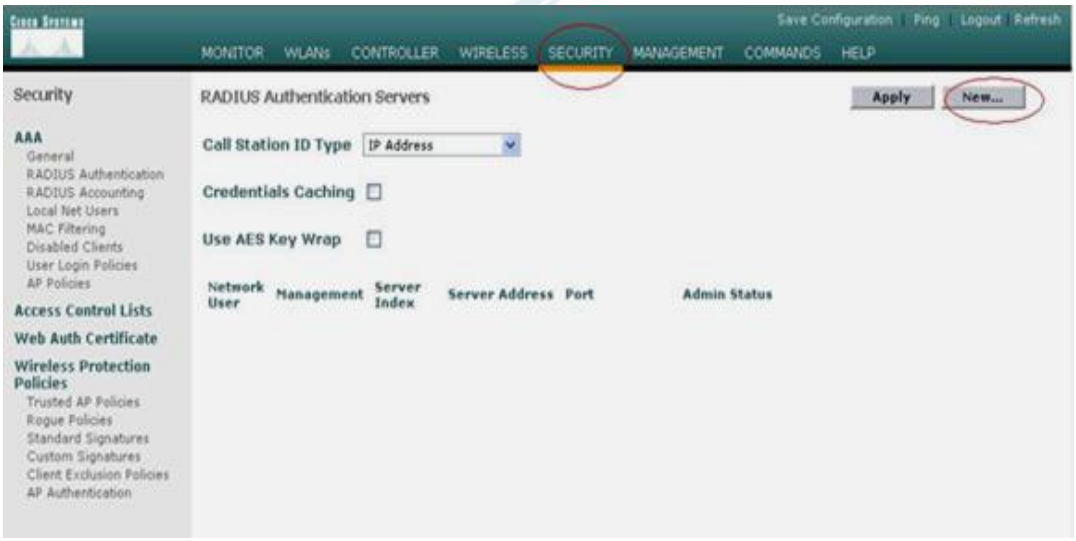
```
R1(config)# interface wlan-controller1/0.2
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip address 192.168.2.254 255.255.255.0
```

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
```

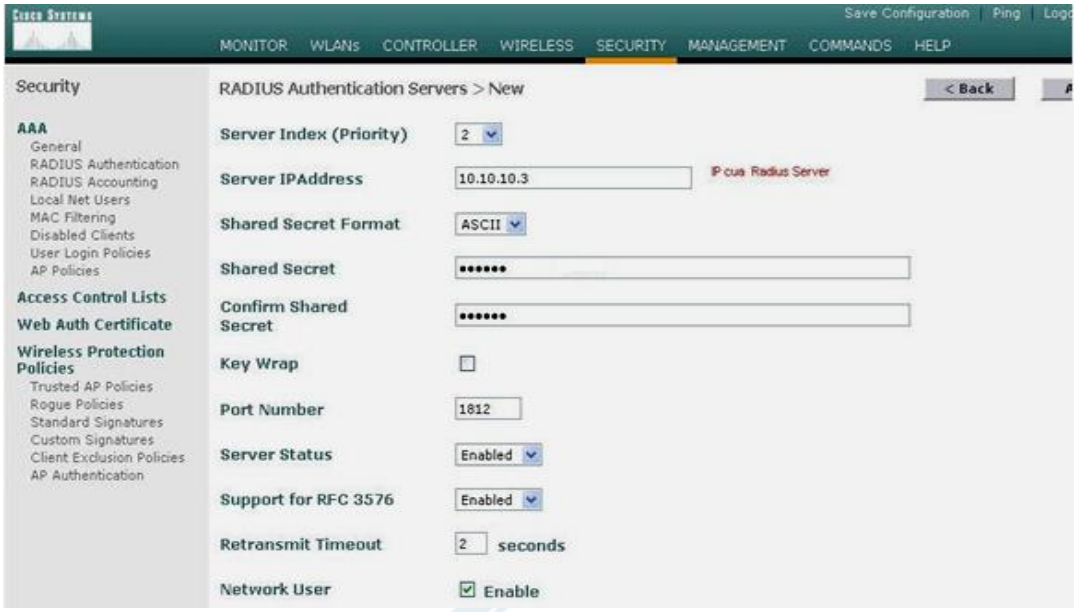
Bước 3: Cấu hình các tham số xác thực dot1x trên WLC.

Chọn Security → New (hình 111).



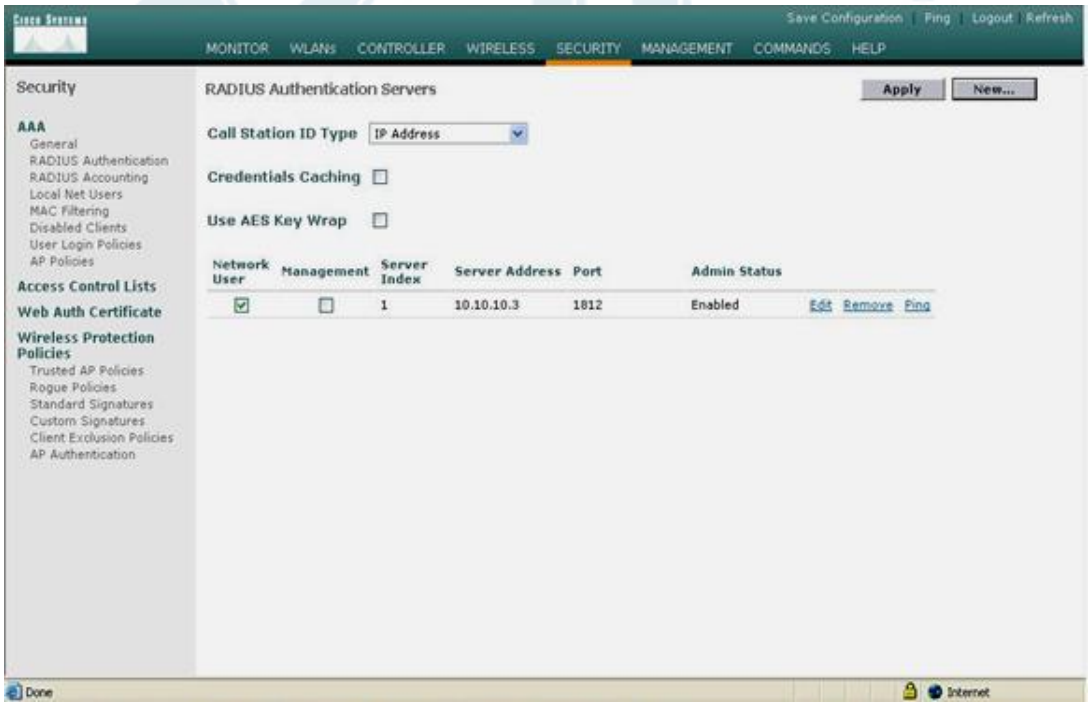
Hình 111

Khai báo sự tồn tại của ACS server (đóng vai trò máy chủ xác thực Radius) – hình 112



Hình 112

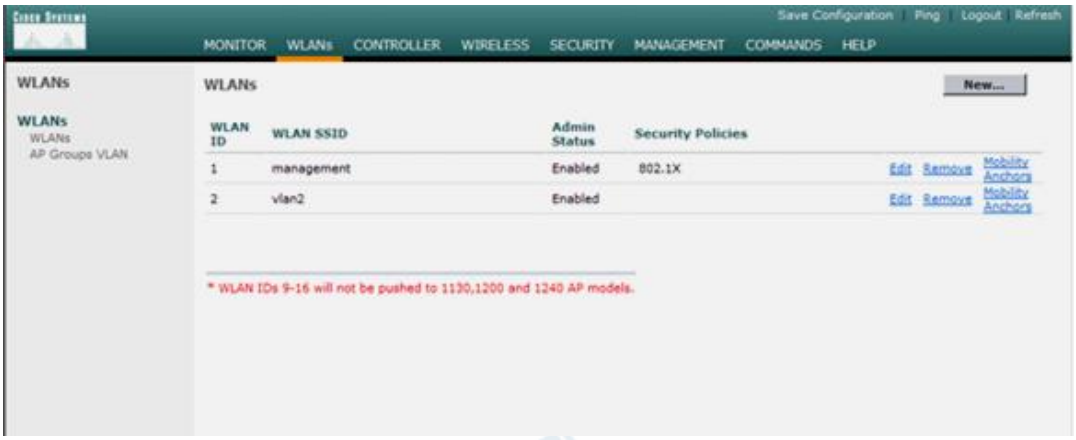
Chọn Apply (hình 113).



Hình 113

Cấu hình xác thực FAST.

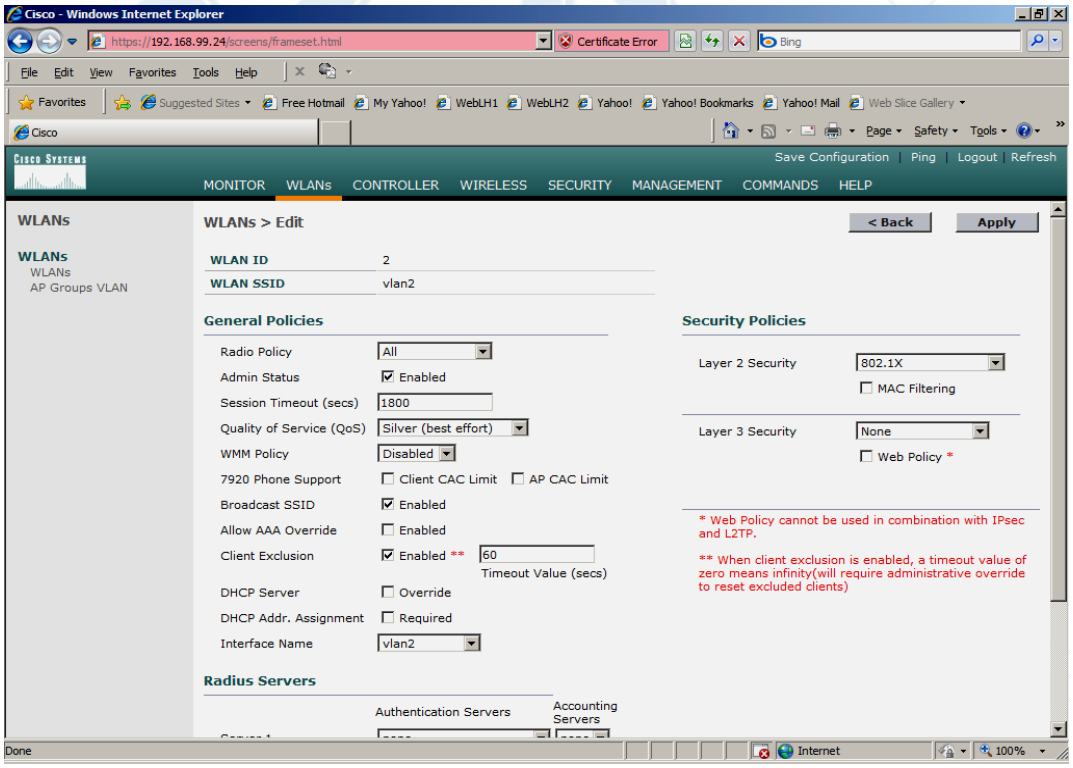
Vào WLANs để chọn kiểu xác thực. Dùng edit để chỉnh sửa thông tin của SSID vlan2 (hình 114).



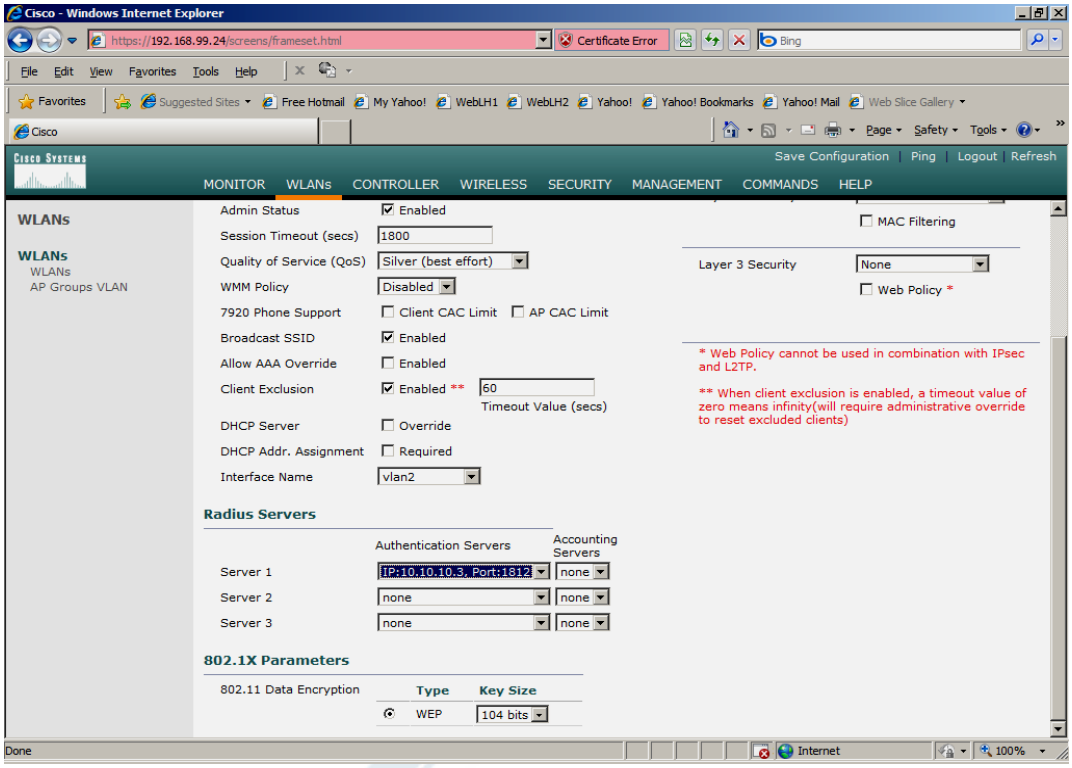
Hình 114

Chọn 802.1X trong phần Layer 2 security (hình 115).

Trong phần server1 chọn 10.10.10.3 (hình 116).



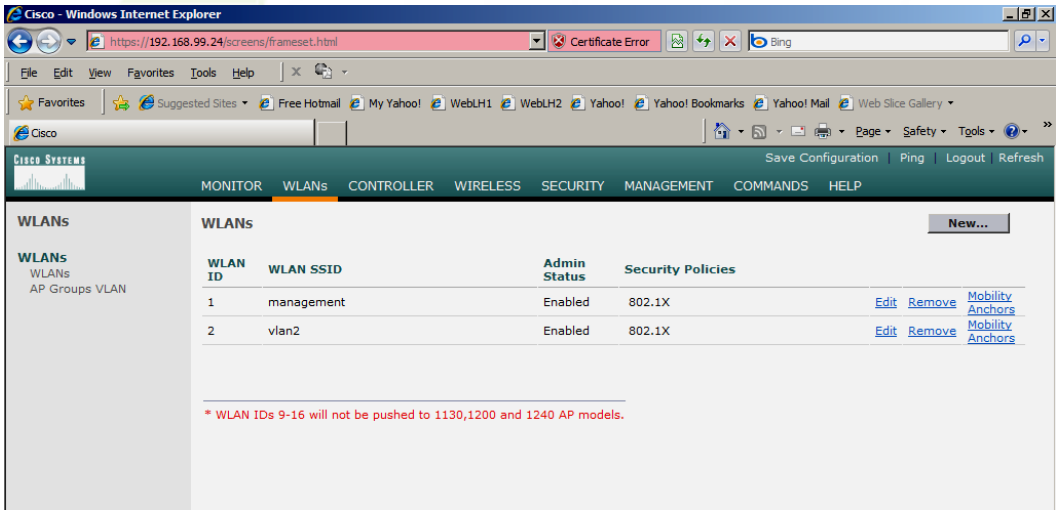
Hình 115



Hình 116

Nhấn Apply, nếu có câu hiển thị thông báo các client đang kết nối sẽ bị đứt kết nối chọn OK.

Quan sát kết quả (hình 117).



Hình 117

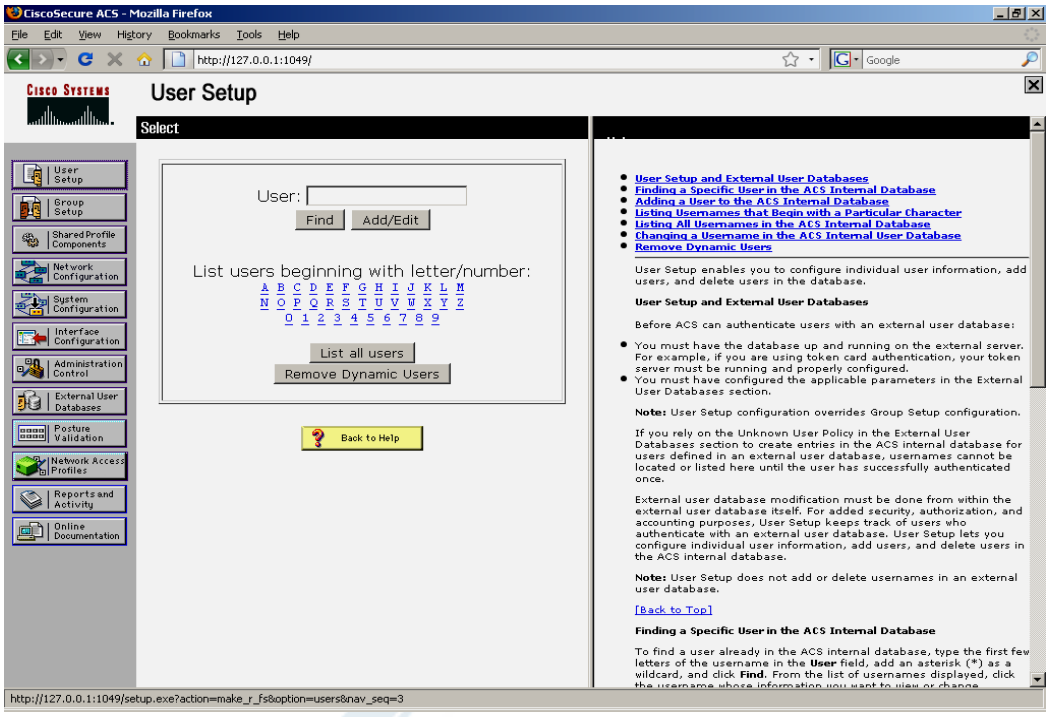
Cấu hình trên ACS hỗ trợ xác thực bằng FAST.

Truy nhập vào đường liên kết cấu hình ACS (hình 118).

Hình 118

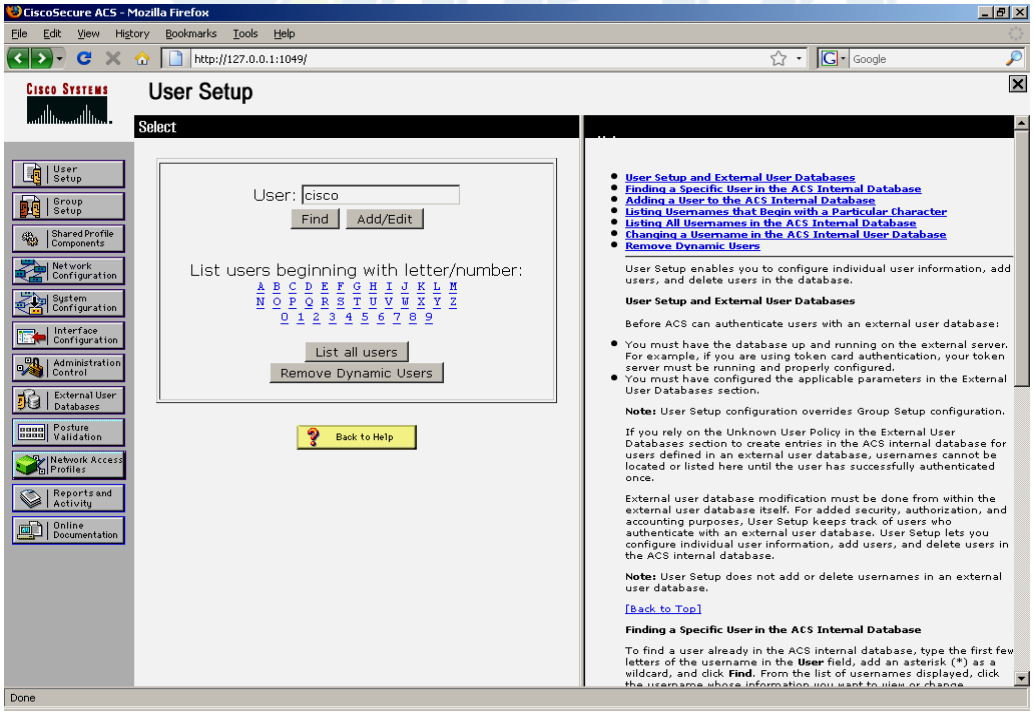
VnPro
ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG QUỐC TẾ

Tạo thêm tài khoản người dùng mới (hình 119).



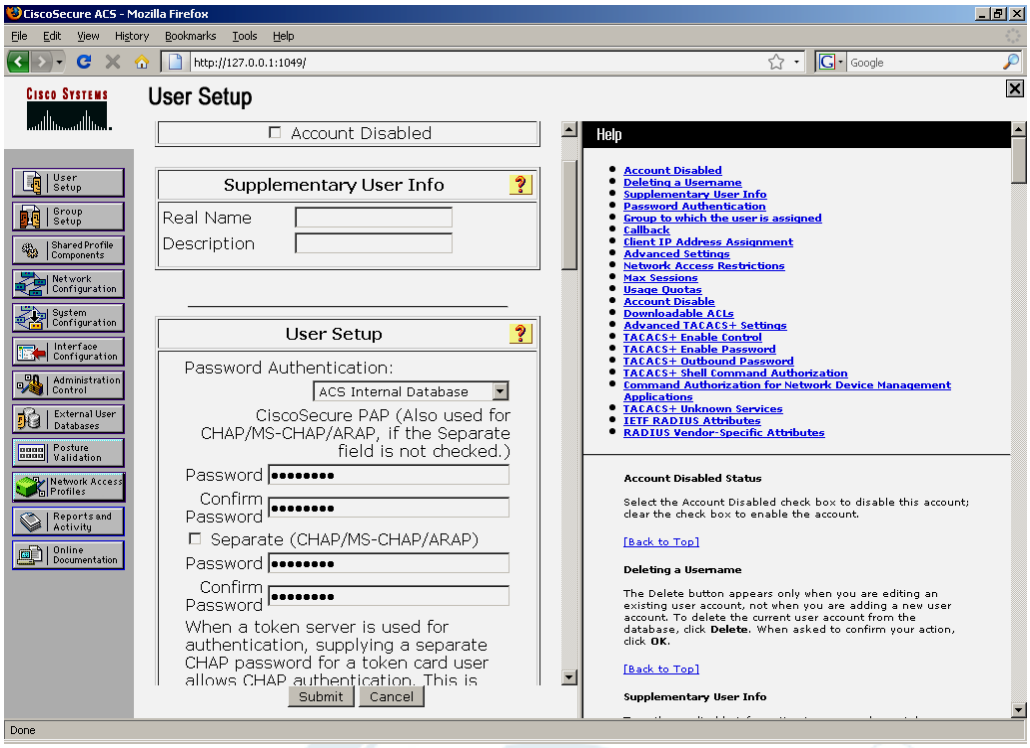
Hình 119

Nhập Username: cisco (hình 120).



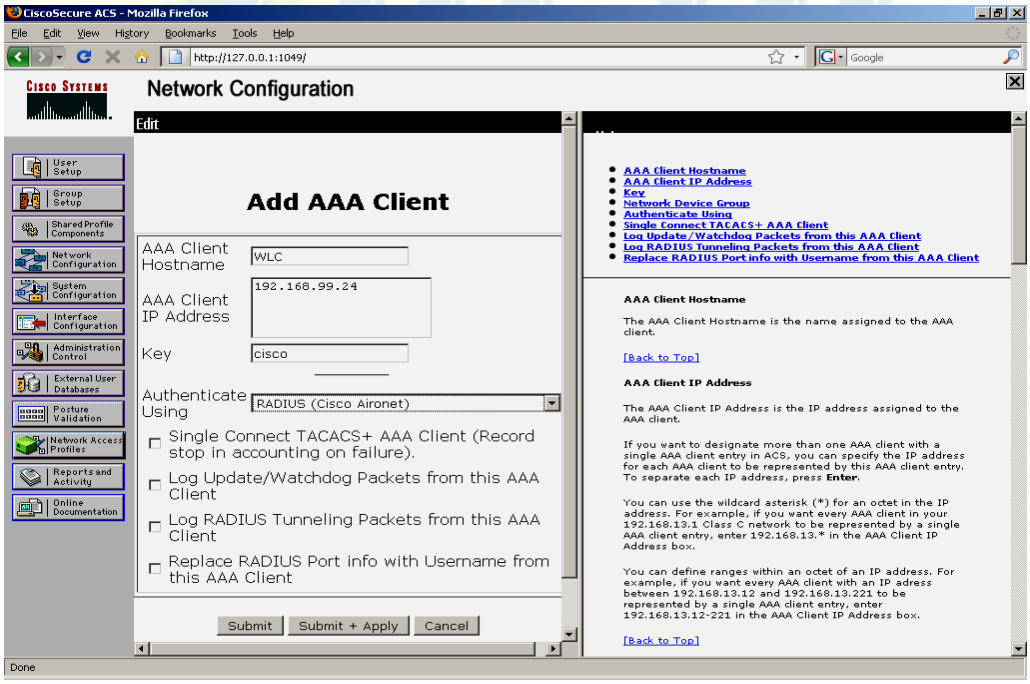
Hình 120

Nhập Password: cisco123 → chọn submit (hình 121).



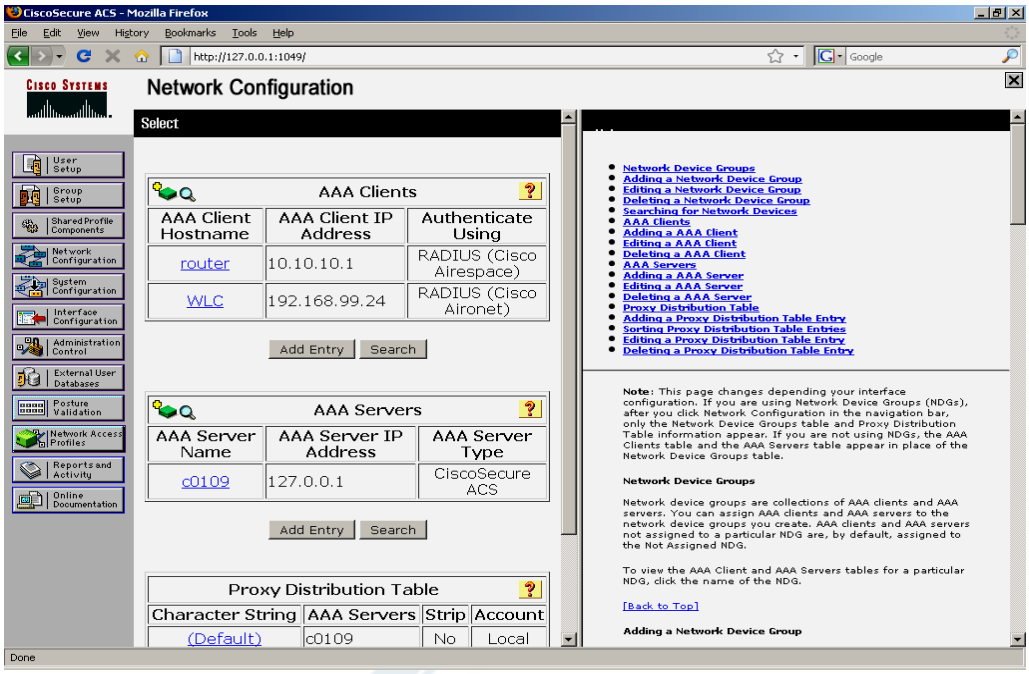
Hình 121

Khai báo sự tồn tại của WLC trên ACS (hình 122).



Hình 122

Chọn Submit + Apply và xem kết quả (hình 123).

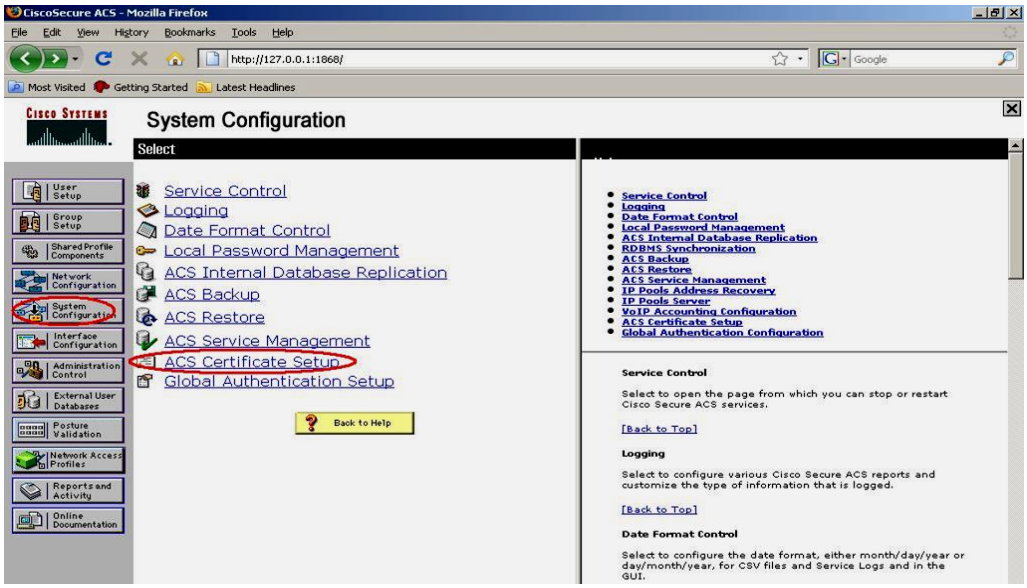


Hình 123

Khai báo kiểu xác thực FAST trên ACS.

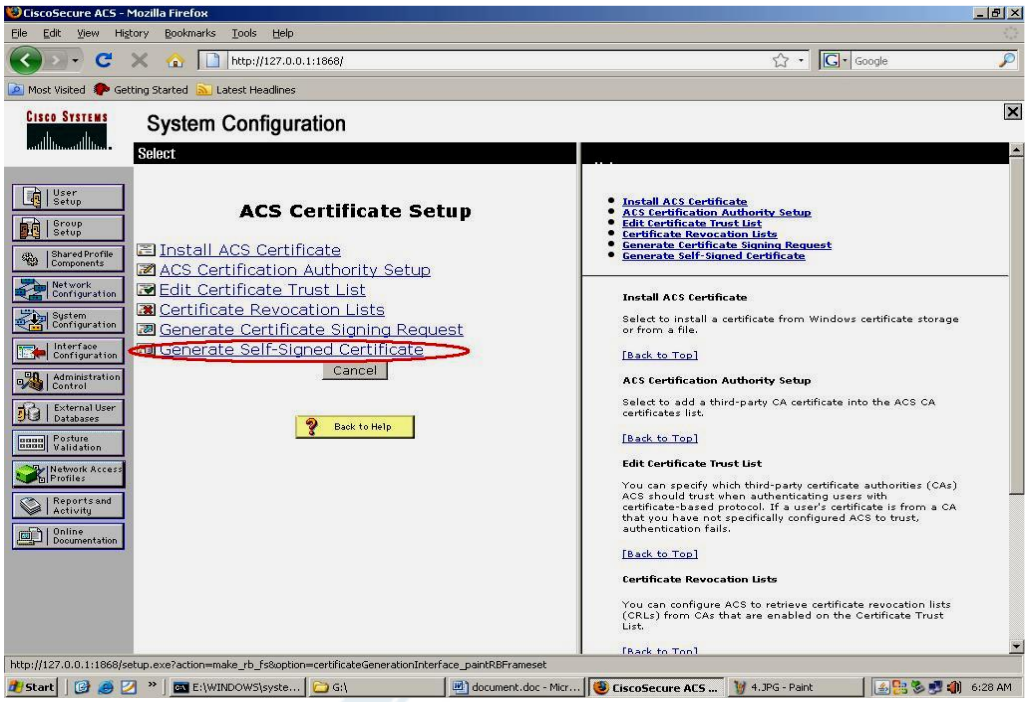
Để xác thực kiểu FAST, ACS server phải có chứng thực điện tử, thực hiện thao tác tự tạo chứng thực điện tử trên server ACS.

Vào System configuration -> ACS Certificate Setup (hình 124).



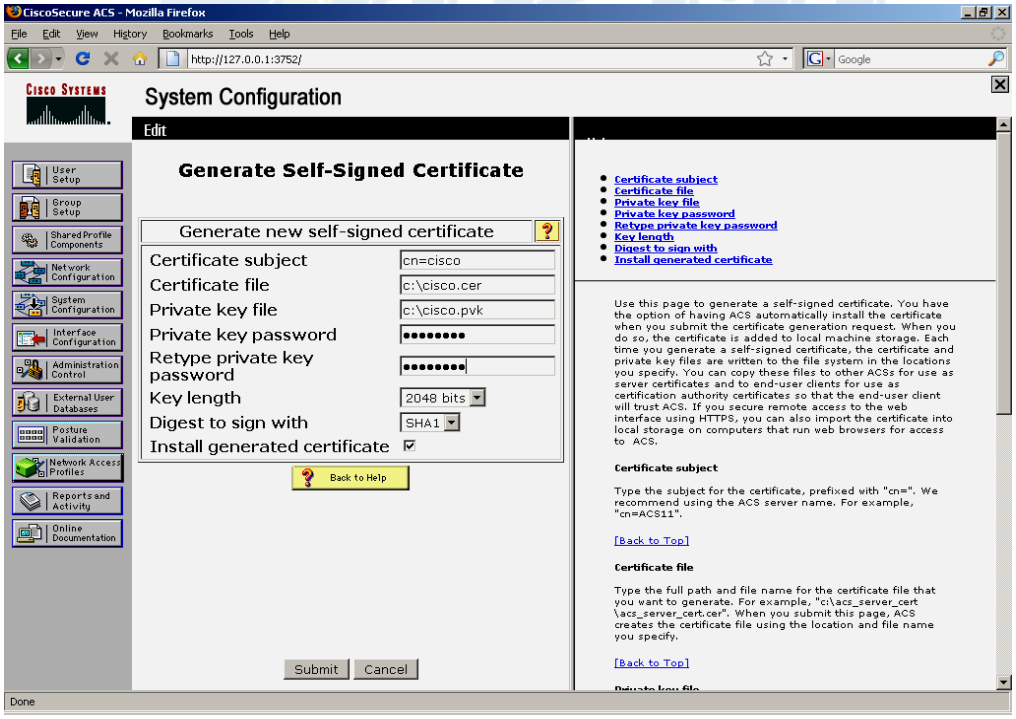
Hình 124

Chọn Generate Self-Signed Certificate (hình 125).



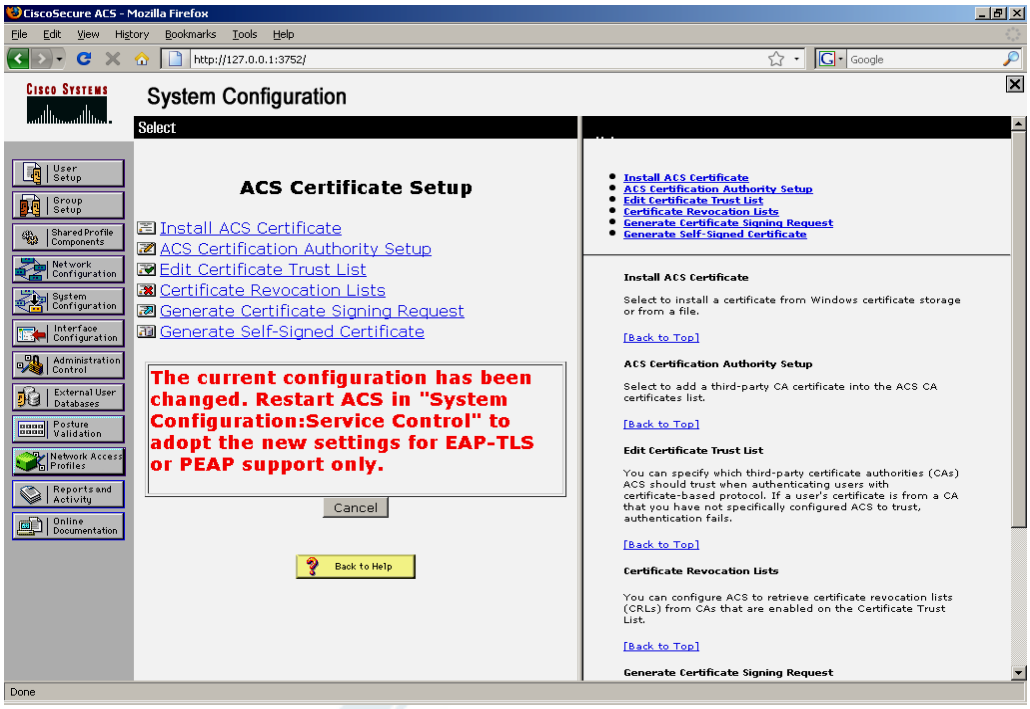
Hình 125

Nhập các thông tin cần thiết theo, sau đó chọn submit (hình 126).



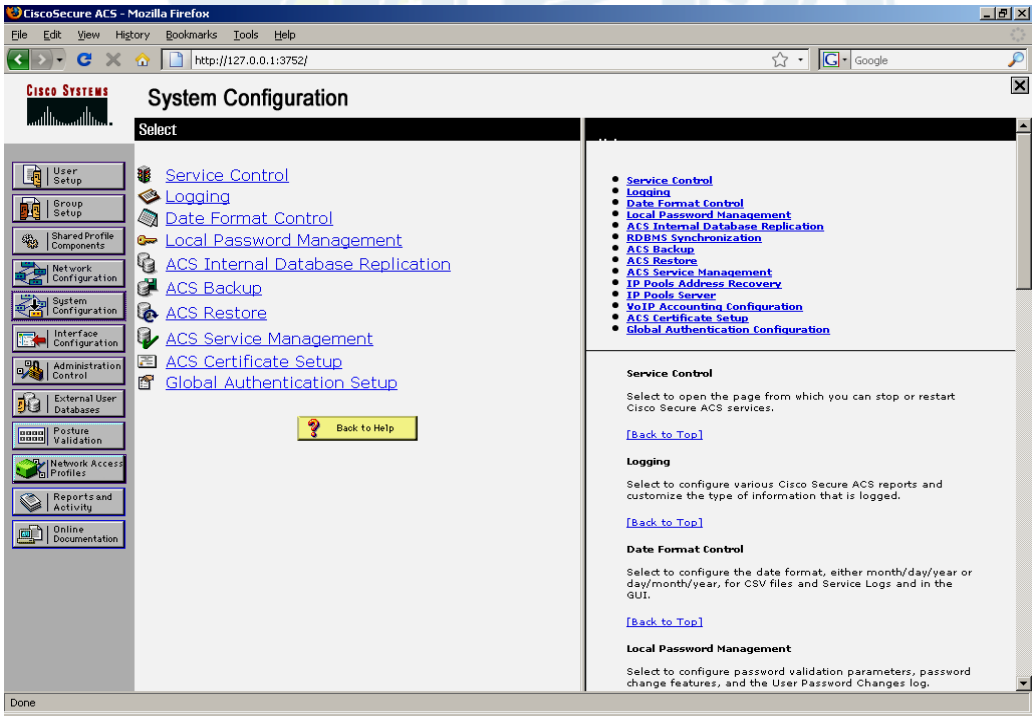
Hình 126

Xuất hiện thông báo sau (hình 127).



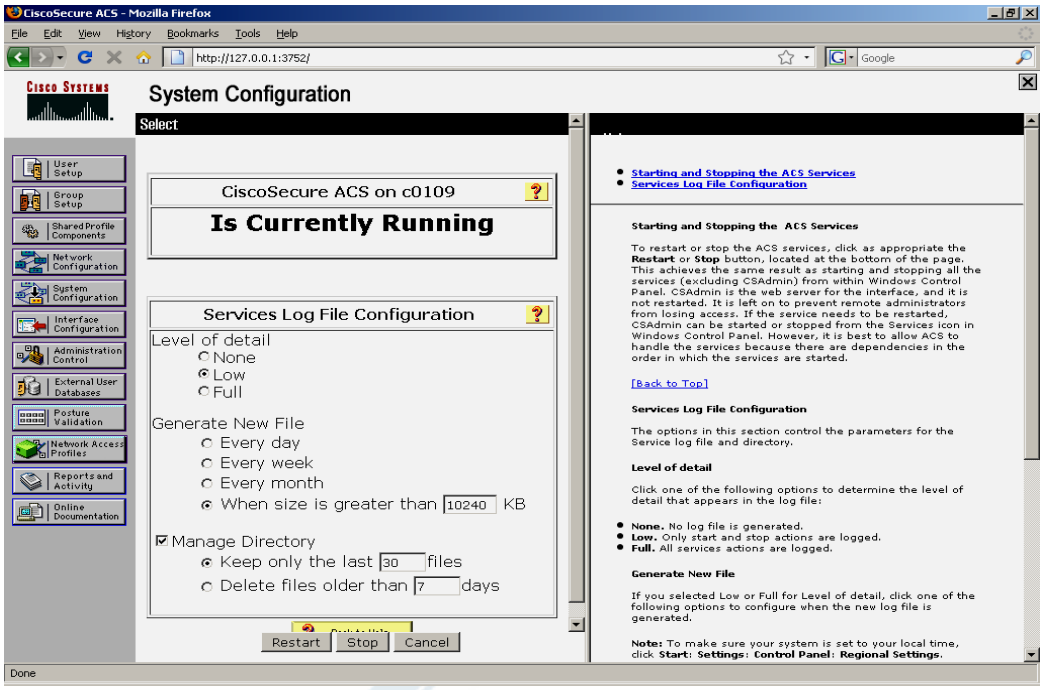
Hình 127

Vào system configuration --> Service Control (hình 128).



Hình 128

Chọn Restart, dịch vụ ACS sẽ được khởi tạo lại (hình 129).

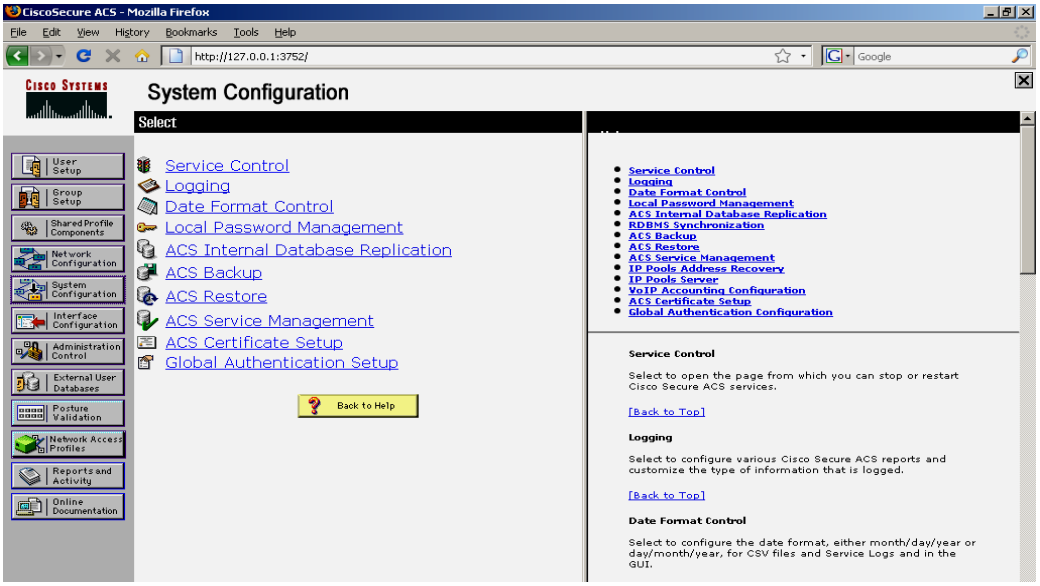


Hình 129

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.

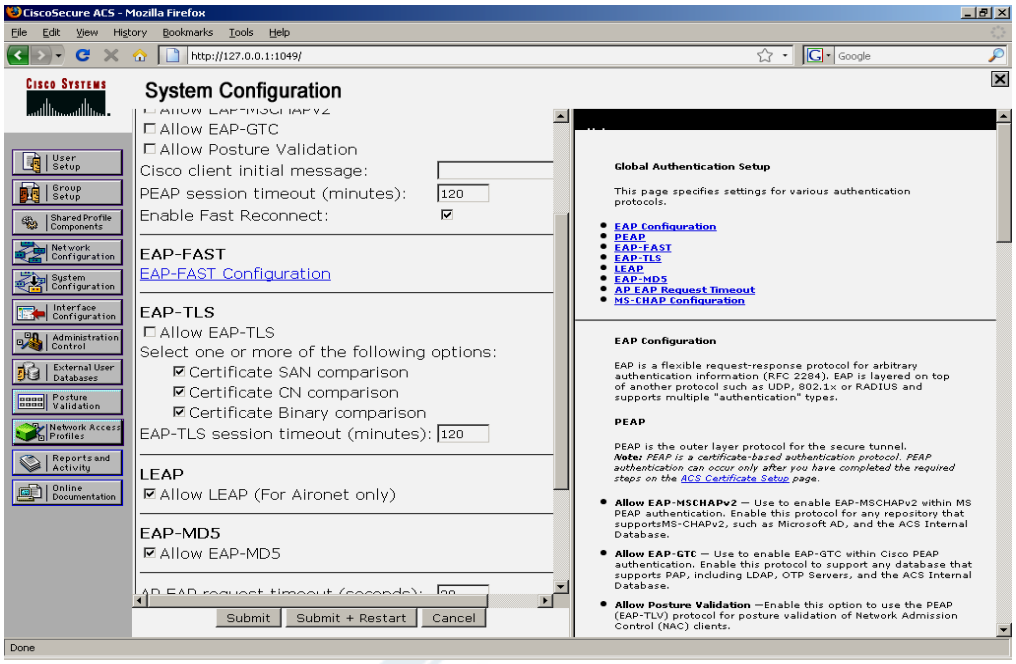
Cấu hình hỗ trợ cơ chế xác thực theo FAST.

Vào System Configuration --> Global Authentication Setup (hình 130).



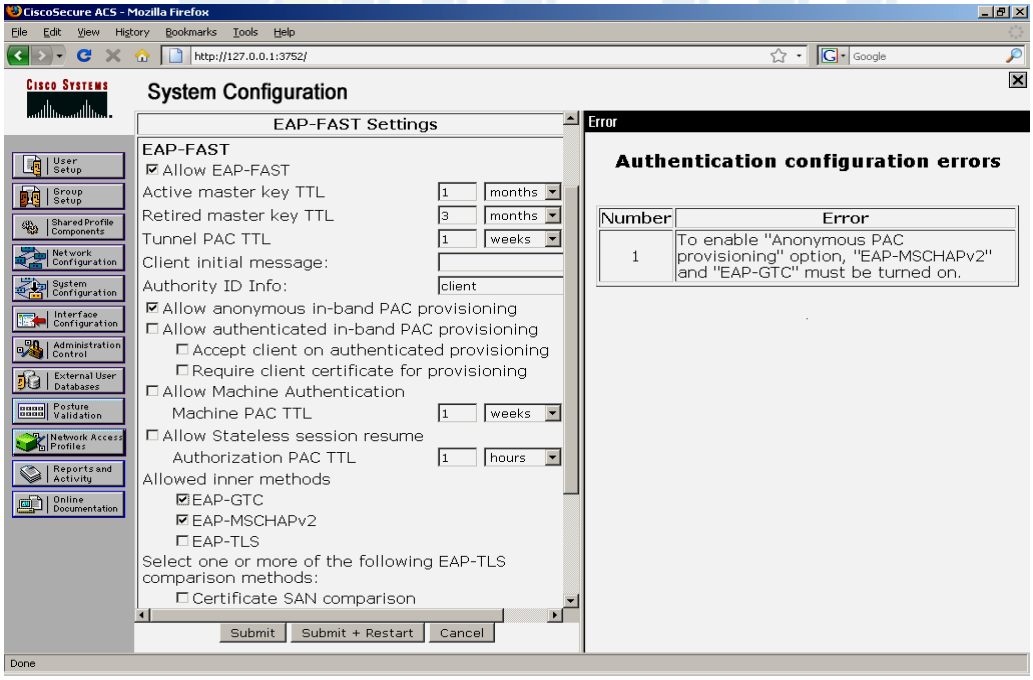
Hình 130

Chọn EAP – FAST Configuration (hình 131).



Hình 131

Chọn bật tính năng EAP – FAST, cấu hình các tham số còn lại, hỗ trợ các giá trị bảo mật định danh được cung cấp từ máy bất kỳ và cho phép xác thực bên trong dùng cơ chế EAP – MSCHAPv2. Chọn Submit + Restart (hình 132).



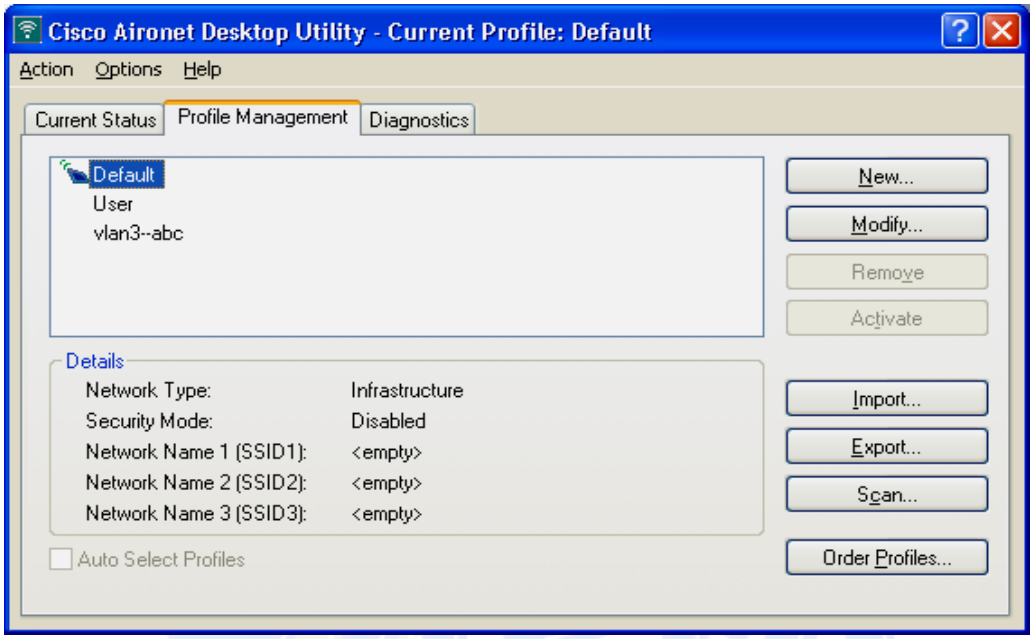
Hình 132

Cấu hình Wireless client hỗ trợ kiểu xác thực FAST.

Do WINXP không hỗ trợ cơ chế xác thực này nên vẫn dùng chương trình Cisco Aironet Desktop Utility (yêu cầu card gắn trong là của hãng Cisco).

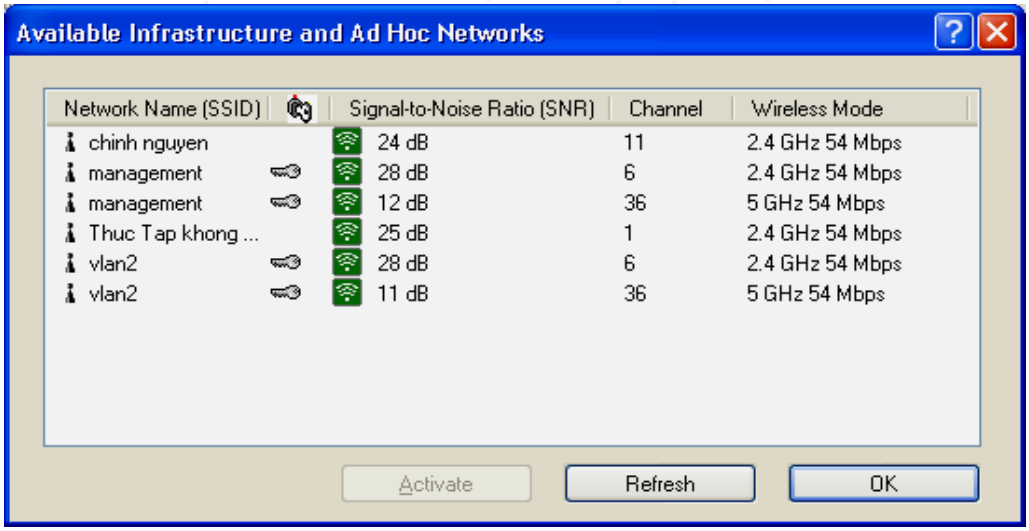
Trước tiên chép file cisco.cer trên máy chủ ACS và chạy file này trên PC nhằm import certificate này vào trong PC.

Khởi tạo chương trình Cisco Aironet Desktop Utility (hình 133).



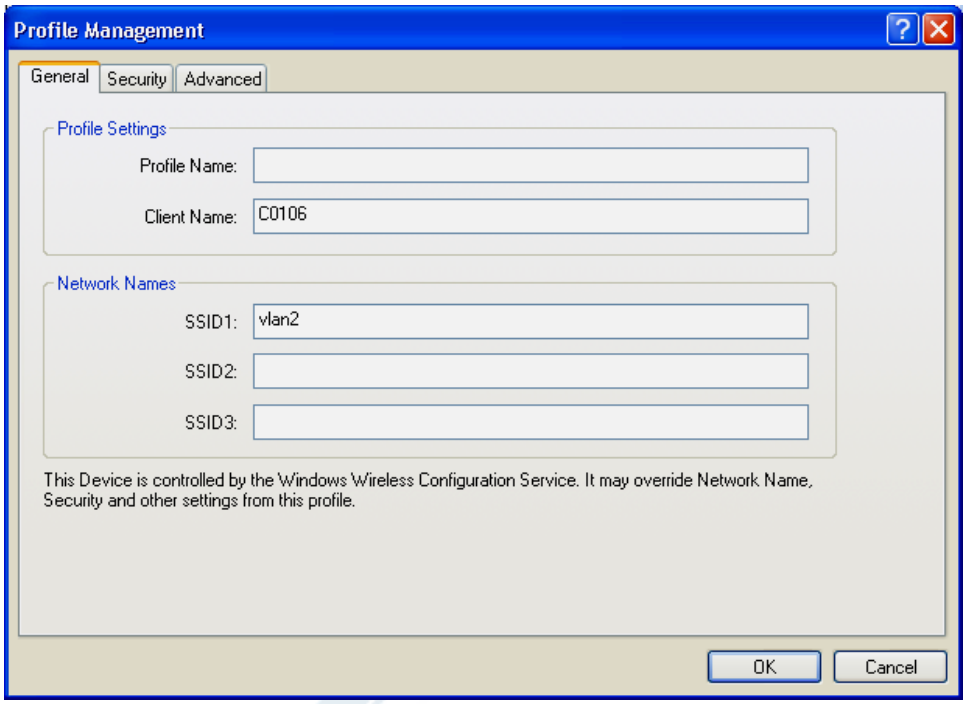
Hình 133

Chọn Scan để tìm thông tin của vùng wireless có SSID vlan 2 (hình 134).



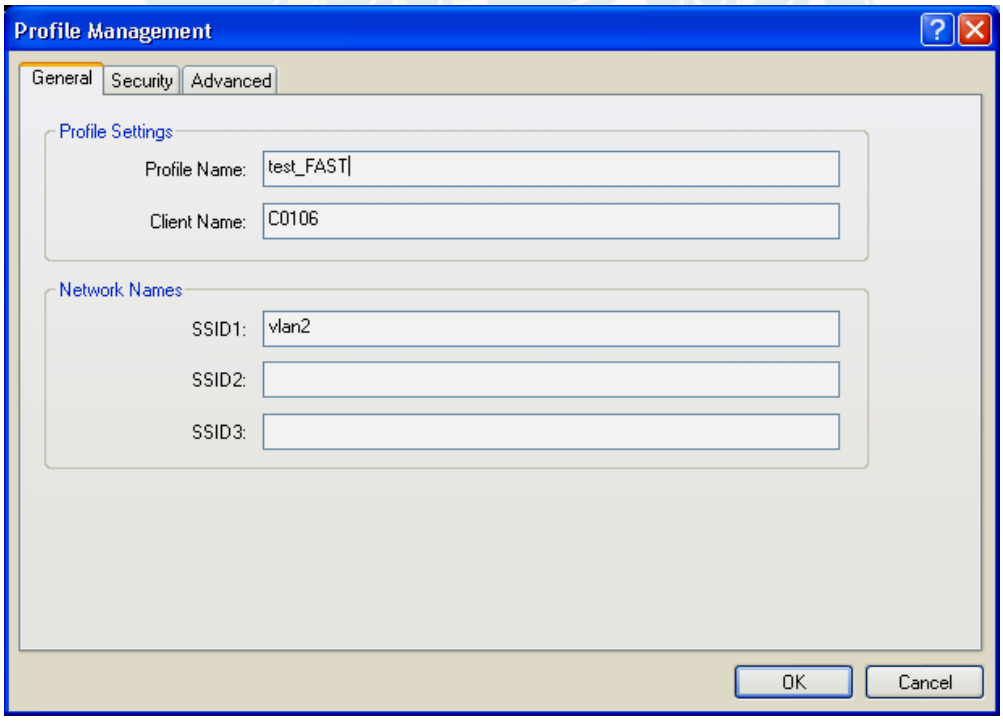
Hình 134

Chọn vlan2 → OK (hình 135).



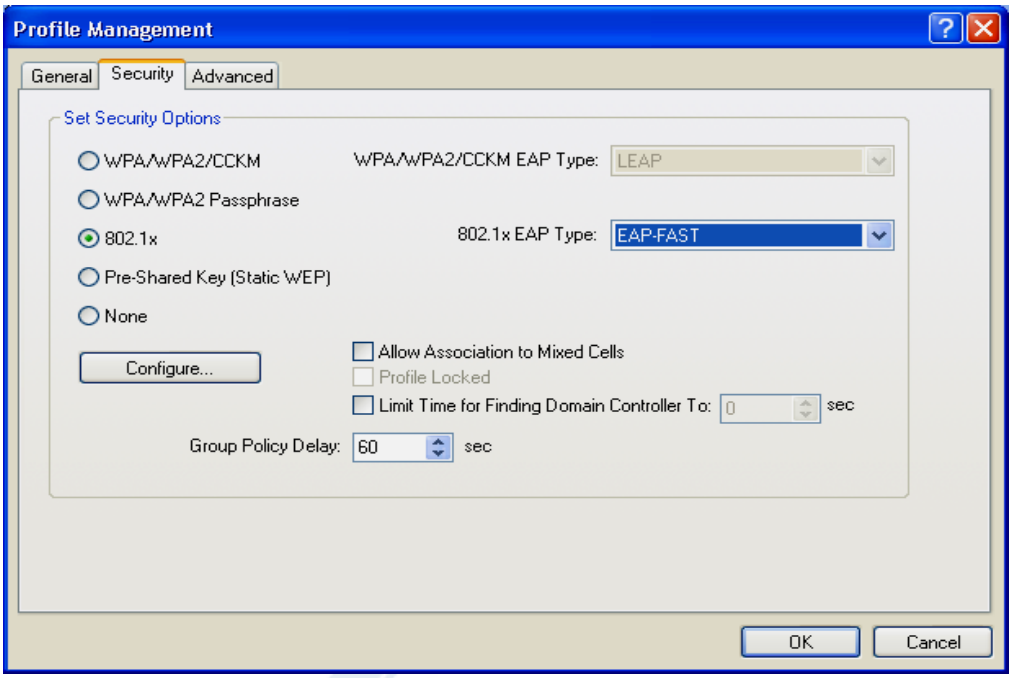
Hình 135

Điền thông tin bổ sung tên profile (hình 136).

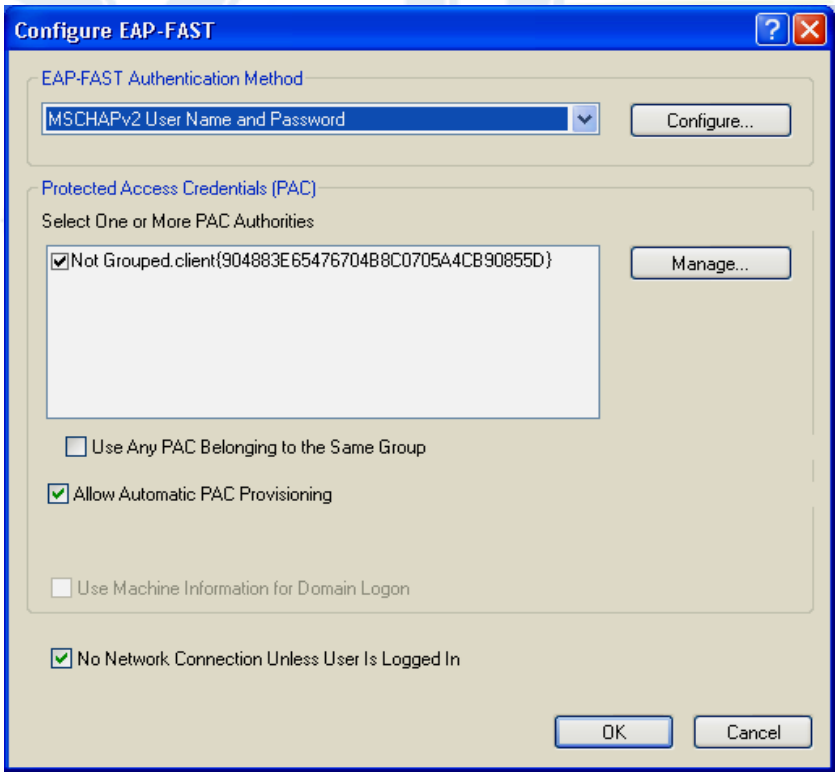


Hình 136

Chọn kiểu xác thực là 802.1X với dạng là EAP-FAST, sau đó chọn configure để cấu hình các tham số của EAP-FAST (hình 137).



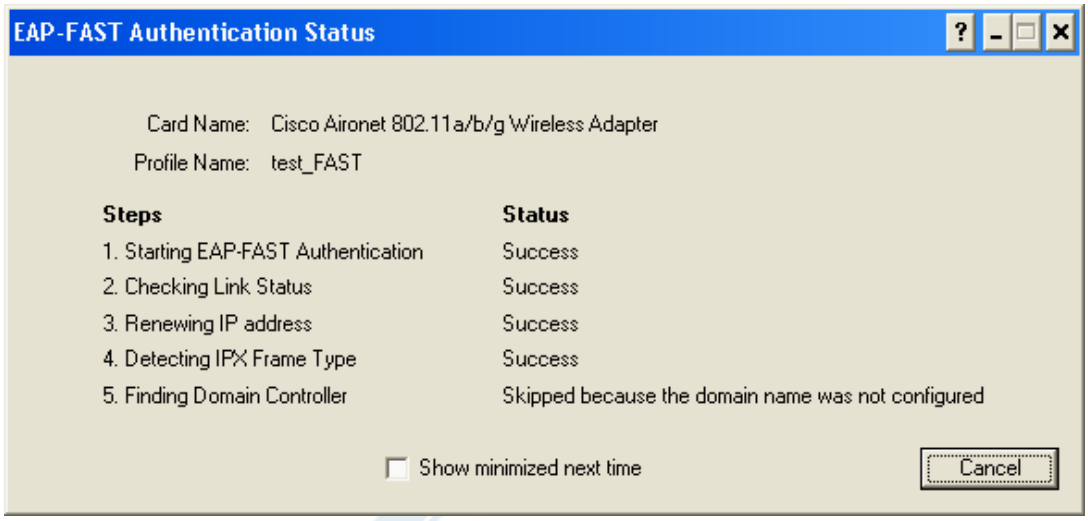
Hình 137



Hình 138

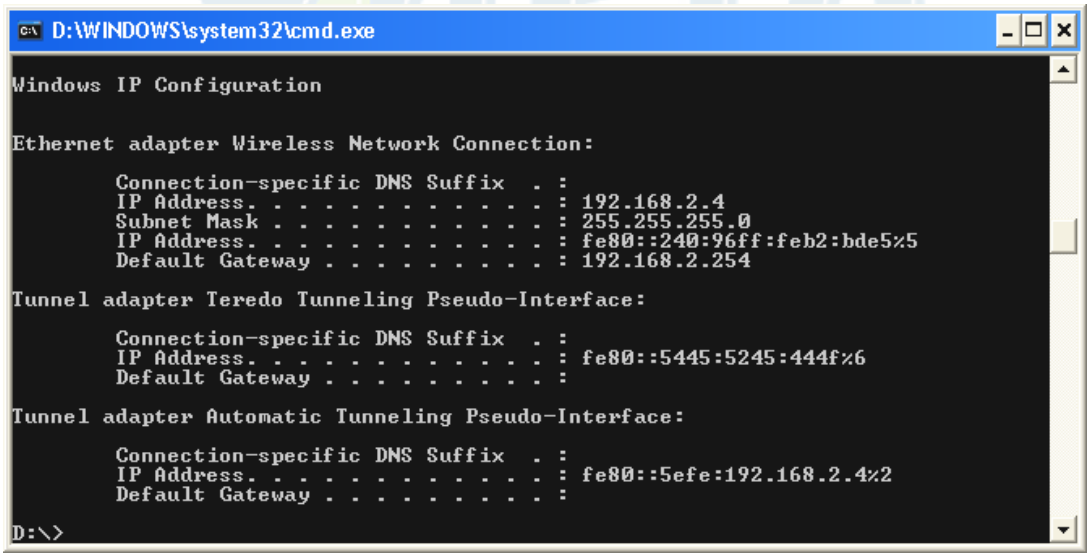
Chọn phương thức xác thực là Username và Password. Nếu như cập nhật thông tin cisco.cer thành công thì thông tin bảo mật từ server sẽ hiện lên. Sau đó chọn OK để hoàn tất quá trình cập nhật thông tin (hình 138).

Quá trình liên kết sẽ tiến hành tự động (hình 139).



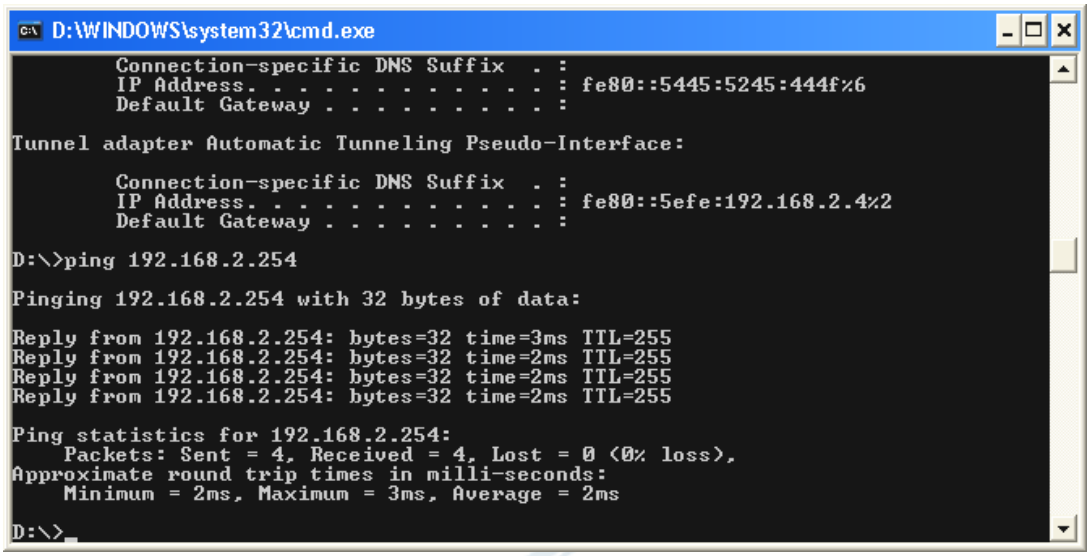
Hình 139

Trên PC, kiểm tra đã nhận được IP thành công.



Hình 140

Ping kiểm tra (hình 141).



Hình 141

VnPro®
ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG QUỐC TẾ