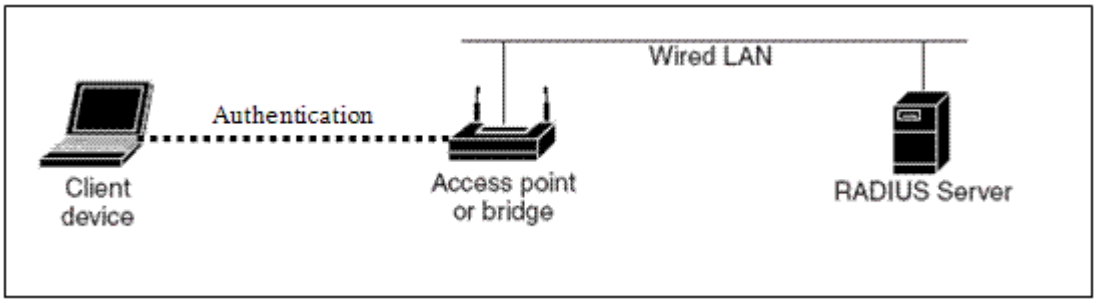
Cấu hình xác thực bằng RADIUS server



Mạng WLAN bản thân nó là không bảo mật, tuy nhiên đối với mạng có dây nếu bạn không có 1 sự phòng ngừa hay cấu hình bảo vệ gì thì nó cũng chẳng bảo mật gì. Điểm mấu chốt để tạo ra 1 mạng WLAN bảo mật là phải triển khai các phương pháp bảo mật thiết yếu cho WLAN để giúp cho hệ thống mạng của mình được an toàn hơn.
Trong bài LAB này ta sẽ thảo luận các đặc điểm và cách cấu hình RADIUS server. Nhằm ngăn chặn những truy cập mạng trái phép mà mình không mong muốn. Khi đó client muốn truy cập vào mạng thì phải đăng nhập đúng **user name** và **password** hợp lợi. Quá trình xác thực này được điều khiển bởi RADIUS server.

Mô tả yêu cầu:
• Cấu hình RADIUS server trên Win 2003, tạo user và password cho các client dự định tham gia vào mạng
• Bật tính năng xác thực EAP Authentication với RADIUS server trên AP Aironet (bằng webpage và CLI).
• Cho PC tham gia vào mạng, kiểm tra kết nối.

Thiết bị yêu cầu : 1 Access point Aironet 1131, 3 pc có gắn card wireless, 1 pc làm RADIUS server.

Các bước thực hiện :

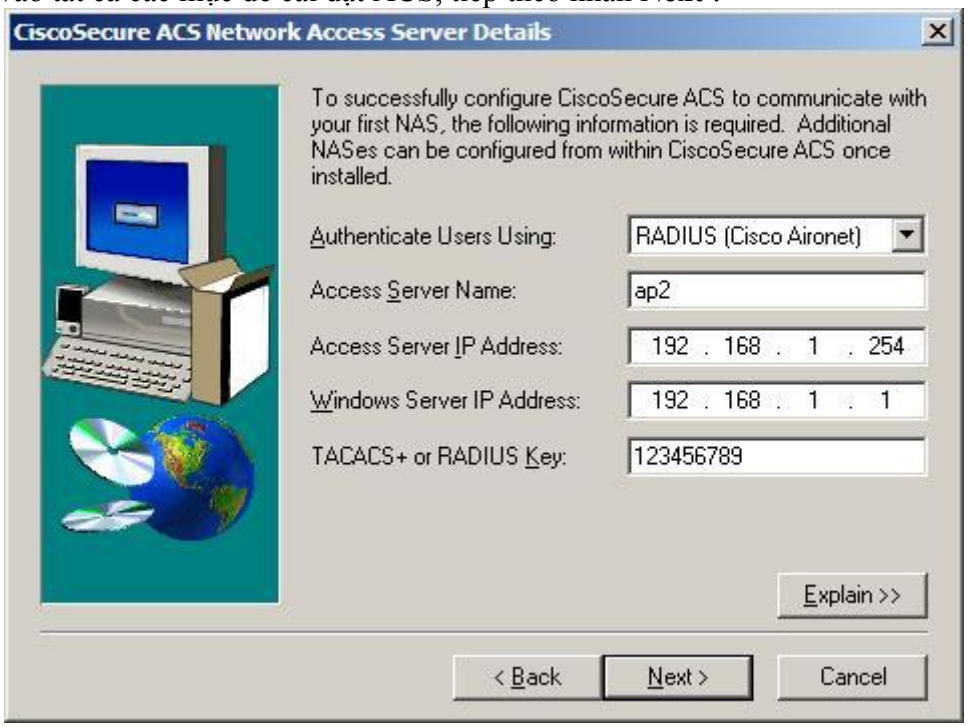
1. Cấu hình RADIUS server trên win 2003:

• Cài đặt phần mềm Cisco Secure ACS v3.2 trên pc chạy win 2003 để làm server.

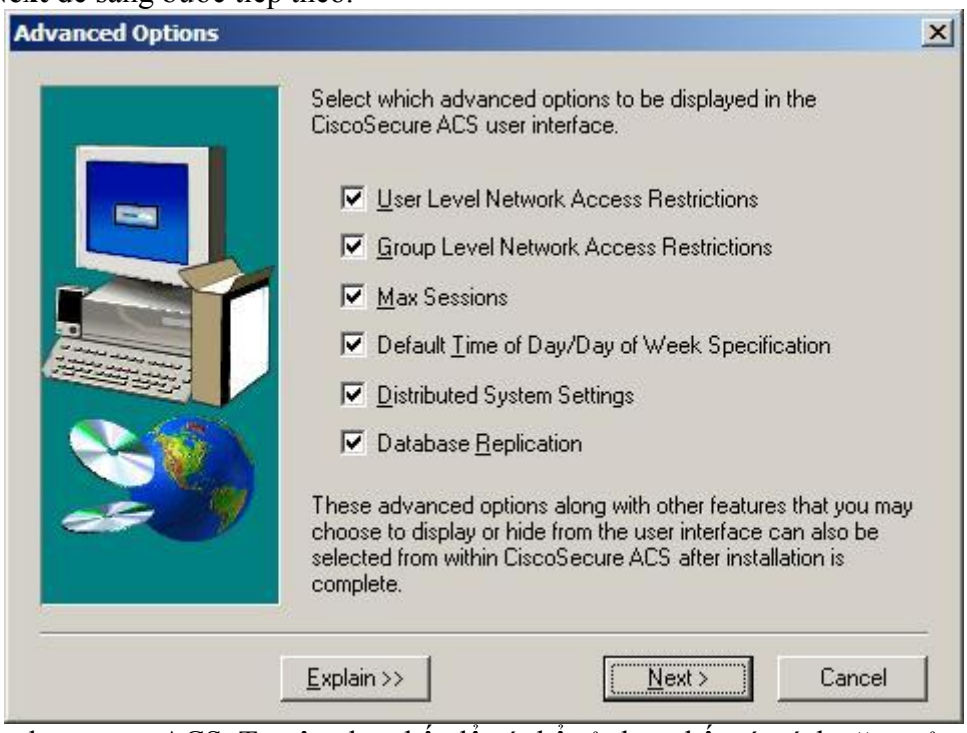
Double click vào file setup.exe trong thư mục chứa phần mềm ACS để tiến hành cài đặt.

Màn hình setup hiện ra :

Check vào tất cả các mục để cài đặt ACS, tiếp theo nhấn **Next** :

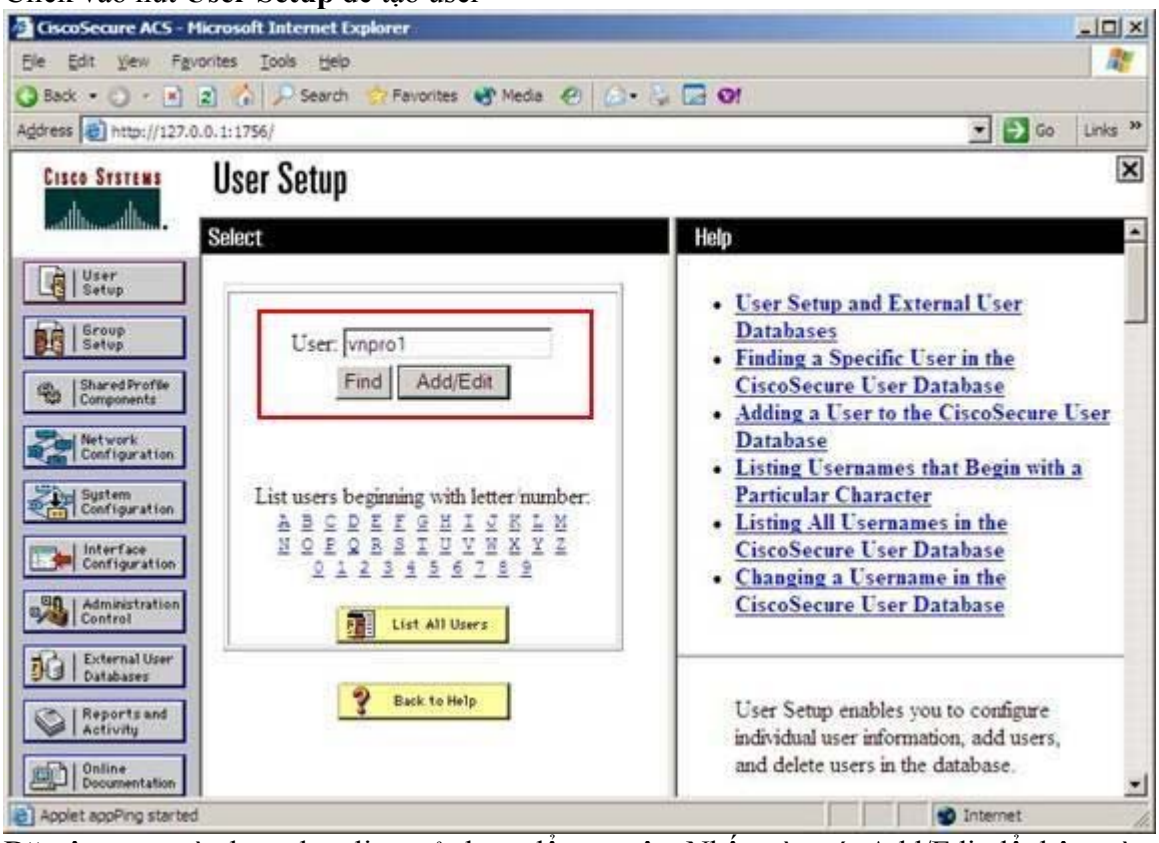


Authenticate Users Using : chọn thiết bị tương ứng mà ta sử dụng. Ở đây do ta sử dung Access point là Aironet nên ta chọn là **RADIUS** (Cisco Aironet).
Access Server Name: tùy chọn đặt tên cho thiết bị. Ta nên đặt trùng tên với Access point mà ta muốn cấu hình để dễ phân biệt.
Access Server IP Address: Địa chỉ IP của AP mà ta cần cấu hình để PC server có thể truy cập tới AP. Trong trường hợp này địa chỉ của AP là 192.168.1.254
Windown Server IP Address: địa chỉ IP của Server làm RADIUS. Chẳng hạn như 192.168.1.1
TACACS + or RADIUS Key: đặt key cho RADIUS server phải trùng với key của AP.
Nhấn **Next** để sang bước tiếp theo.

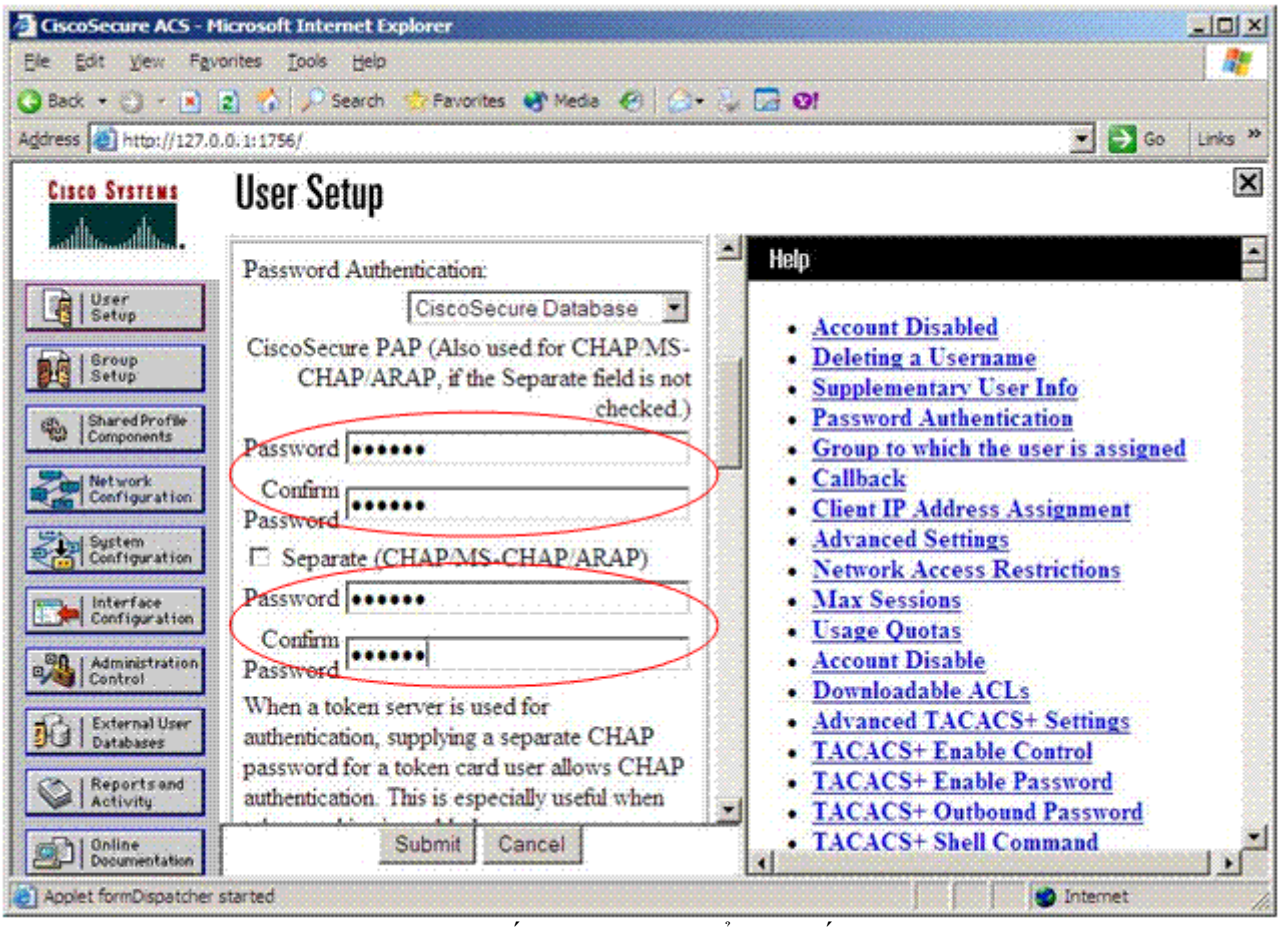


Các tùy chọn trong ACS. Ta nên chọn hết để có thể sử dụng hết các tính năng của ACS.
Nhấn **Next** và tiếp theo nhấn **Finish** để hoàn thành quá trình cài đặt .
• Tạo User và password :
Giao diện chính của ACS:

Click vào nút **User Setup** để tạo user

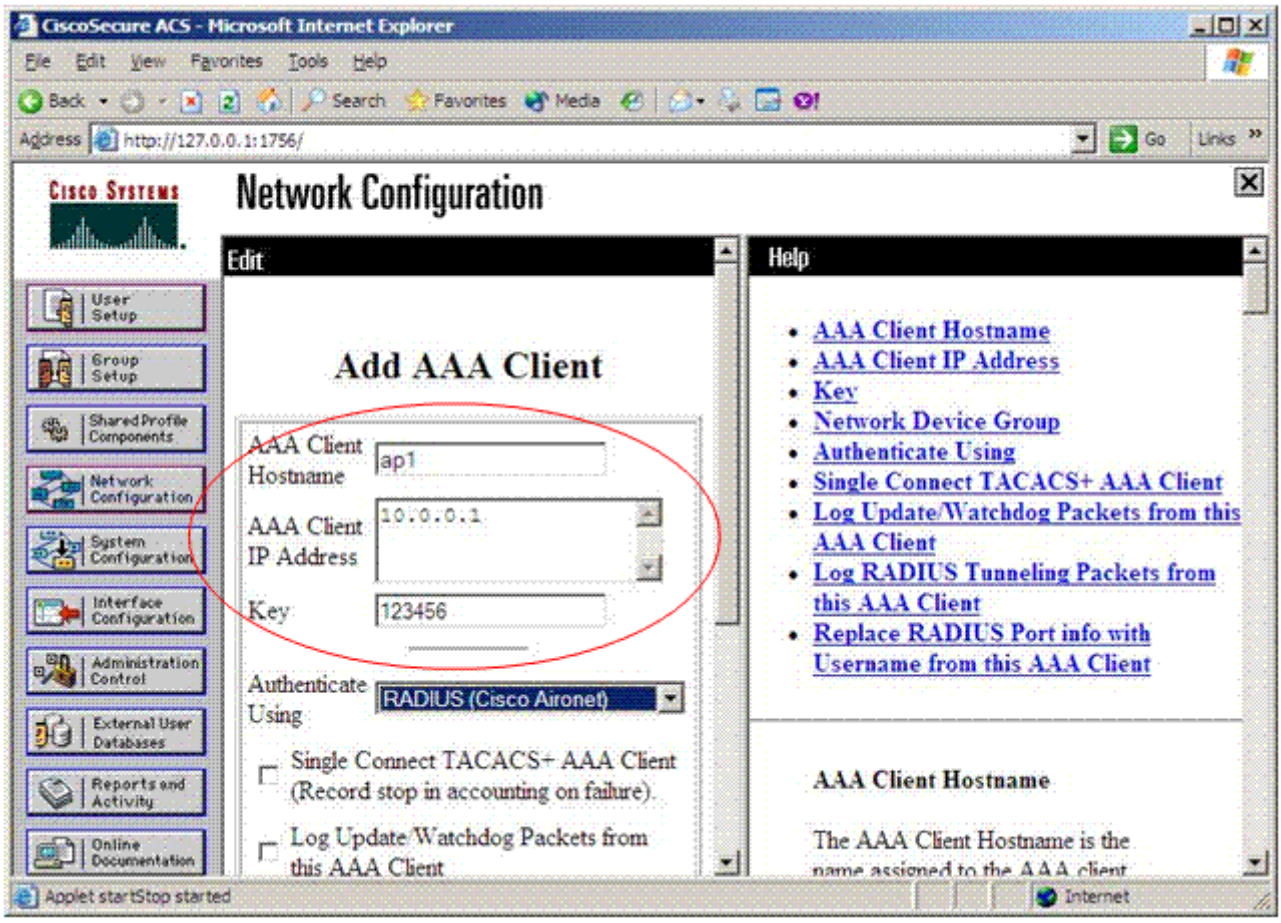


Đặt tên user tuỳ chọn cho client sử dụng để truy cập. Nhấn vào nút Add/Edit để thêm vào cấu hình. Ta có thể add nhiều user tuỳ theo nhu cầu.



Đặt Password cho user vừa tạo. xong nhấn nút **Submit** để hoàn tất .

• Ngoài ra ta có thể thay đổi cấu hình mạng ban đầu đã thiết lập trong quá trình cài đặt hoặc thêm cấu hình tùy chọn. bằng cách nhấn vào nút **Network Configuration**.



Ta có thể tạo cấu hình tùy mục đích sử dụng ở đây. Sau khi tạo xong nhấn **Submit+Restart** để hoàn tất cài đặt.

Lưu ý : Phần mềm ACS đòi hỏi phải chạy trên môi trường Java. Do đó trước khi cài đặt yêu cầu phải cài **Java Runtime Environment**.

Sau khi setup ACS xong thì khi mở trình duyệt ACS vẫn chưa chạy. Khi đó ta chọn **Tool > Internet Option > Security** , chọn **levlels Low** để cho phép java start

2. Bật tính năng xác thực EAP Authentication với RADIUS server trên AP Aironet:

+Thực hiện trên webpage:

• Đặt địa chỉ IP của PC trùng với địa chỉ của AP. Trường hợp này địa chỉ của AP là 192.168.1.254, ta đặt cho PC là 192.168.1.2
• Kết nối giữa PC với AP thông qua cáp thẳng
• Mở trình duyệt web lên, điền địa chỉ của AP là 192.168.1.254 vào thanh địa chỉ, màn hiện đăng nhập hiện ra yêu cầu nhập user name và password. mặc định user name là **Cisco**, Password là **Cisco**
Hinh đăng nhập user name và pass
• Giao diện chính của AP

Hình giao dien chính của AP

Chọn mục EXPRESS SECURITY

Hình trong mục EXPRESS SECURITY

Chọn SSID là **vnpro**
Chon mục **Broadcast Beacon** để quảng bá SSID
Chọn mục radisus
Đặt IP của server là 192.168.1.1
Đặt Secrect key trùng với key của server pc
nhấn apply => hoàn tất cài đặt.

+Cấu hình bằng CLI:

• Vào mode config bật tính năng AAA

ap(config)# **aaa new-model**

• Định nghĩa AAA Server Groups

ap(config)#**aaa group server radius** rad_eap
ap(config-sg-radius)#**server** 192.168.1.1 **auth-port** 1645 **acct-port** 1646

• Cho phép xác thực trên RADIUS

ap(config)#**aaa authentication login** eap_methods **group** rad_eap

• Tạo SSID và cho phép SSID đó tham gia xác thực RADIUS, đồng thời quảng bá SSID đó qua ngoài

ap(config)#**dot11** ssid ap1
ap(config-ssid)#**authentication open eap** eap_methods
ap(config-ssid)#**authentication network-eap** eap_methods

ap(config-ssid)#**guest-mode**

• Chỉ ra địa chỉ IP của server, port dùng để Authentication Request, port dùng để accounting request và key :

ap(config)# **radius-server host** 192.168.1.1 a**uth-port** 1645 acct-port 1646 key 123456

• Vào mode interface bât tính năng xác thực trên interface và cho phép quảng bá ssid ra interface này

ap(config)#**interface dot11radio 0**
ap(config-if)#**encryption mode** wep mandatory
ap(config-if)#**ssid** ap1
ap(config-if)#no shut
ap(config-if)#end
ap#**wr**

Cấu hình tham khảo:

ap#sh running-config
Building configuration...

Current configuration : 2430 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 1EdQk$vBu/6AkF37mOFlG07co6i1
!
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.1.1 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
!

```
dot11 ssid ap2
authentication open eap eap_methods
authentication network-eap eap_methods
guest-mode
!
power inline negotiation prestandard source
--More-- !
!
username Cisco password 7 047802150C2E
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode wep mandatory
!
ssid ap2
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
--More-- bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
```

--More-- duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
hold-queue 160 in
!
interface BVI1
ip address 192.168.1.254 255.255.255.0
no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779...onfig/help/eag
ip radius source-interface BVI1
!
radius-server host 10.0.0.2 auth-port 1645 acct-port 1646 key 7 1446405858517C
!
control-plane
!
bridge 1 route ip
--More-- !
!
!
line con 0
line vty 0 4
!
end

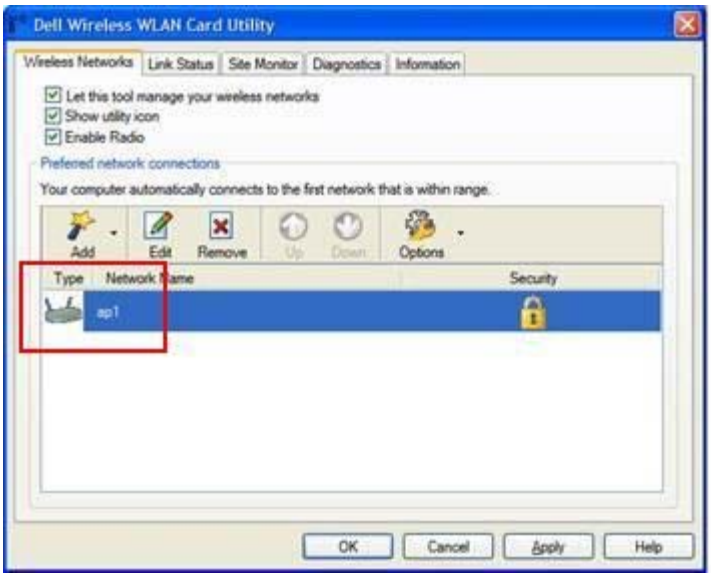
3. kiểm tra kết nối :

Trước khi cho PC tham gia vào mạng, bật tín năng xác thực trên trên card wireless

Trên PC tạo kết nối với mạng có SSID là ap1 vừa được thiết lập.

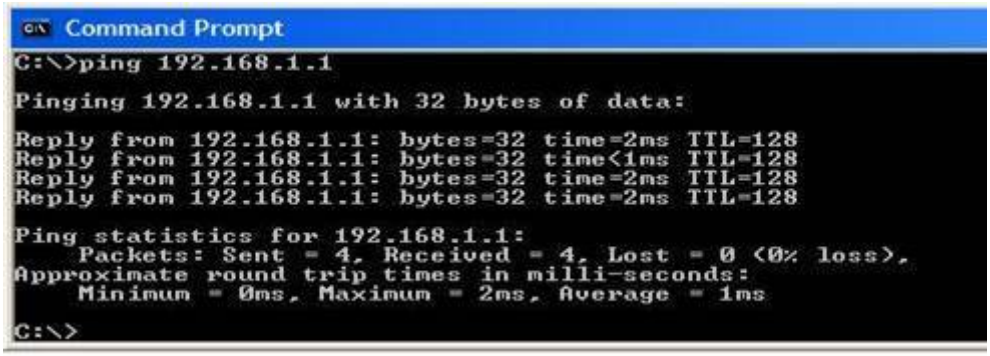
Click vào nút **Add**

tên SSID của mạng mà mình muốn kết nối, chọn kiểu xác thực là **LEAP** và đánh dấu chọn vào mục **Prompt for user name and password** . Nhấn **OK**



1 kết nối được tạo ra với mạng có SSID là **ap1**. Để kết nối với mạng trên, ta click chuột phải và chọn **conect**. Khi đó server sẽ tiến hành xác thực và yêu cầu mình nhập **user name** và **password**.

Nếu client nhập sai user name và password thì sẽ không kết nối tới mạng được. khi đó trên màn hình CLI của AP sẽ báo Authentication Failed. Và bắt buộc client phải đăng nhập lại. sau khi nhập đúng user name và password thì sẽ kết nối được
Để kiểm tra kết nối ta sẽ tiến hành Ping tới server, đặt địa chỉ IP của client trùng lớp mạng với server.



=>ping thành công, kết nối hoàn tất

[Nguồn: VnPro biên soạn]