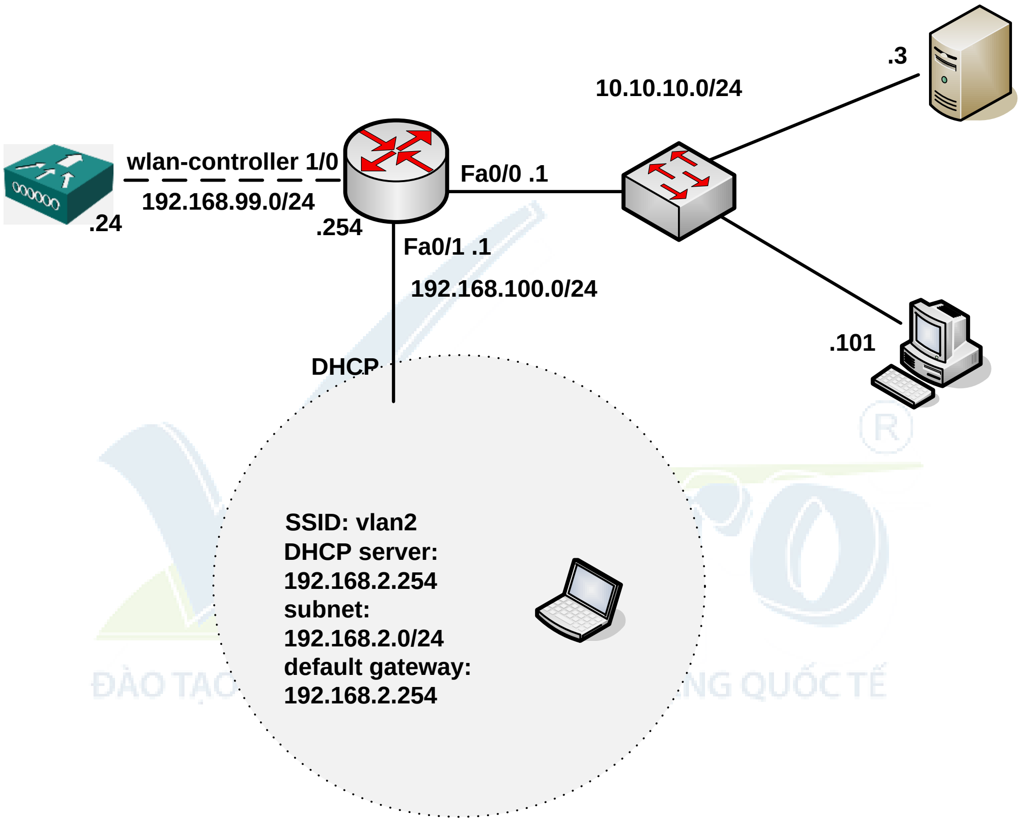
LAB 5: Xác thực dot1x dùng kiểu LEAP

Yêu cầu

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

Sơ đồ



Hình 64

IP của int wlan-controller là 192.168.99.254.

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 abc
!
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
!
```

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 67.

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.**

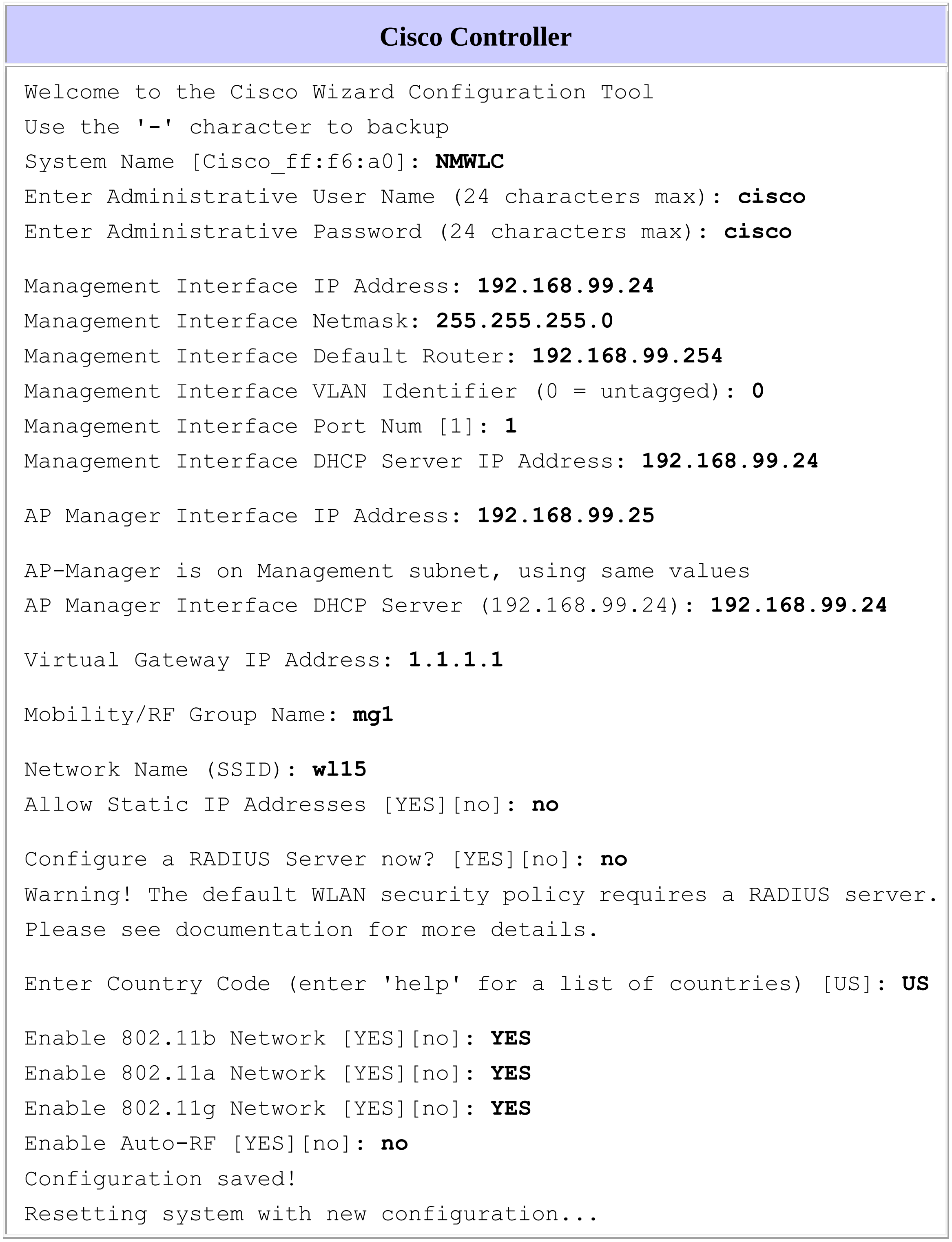
c. Kiểm tra đảm bảo Router có thể ping thấy WLC module.

```
    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. Từ PC ping đến WLC để kiểm tra kết nối IP với WLC đã thông chưa.

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
```



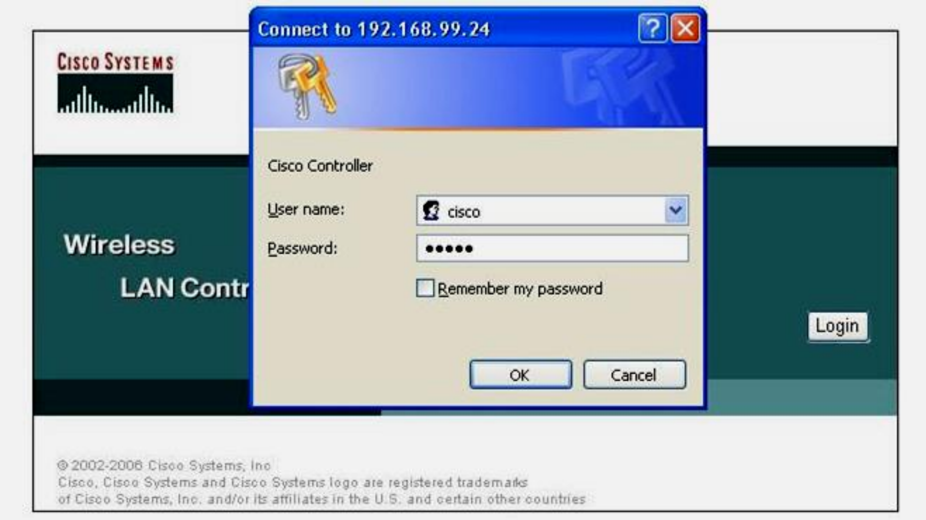
Cisco Controller

```
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 65

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 66.
Cấu hình đồng bộ thời gian cho WLC với R2811 (hình 67).



Connect to 192.168.99.24

Cisco Controller

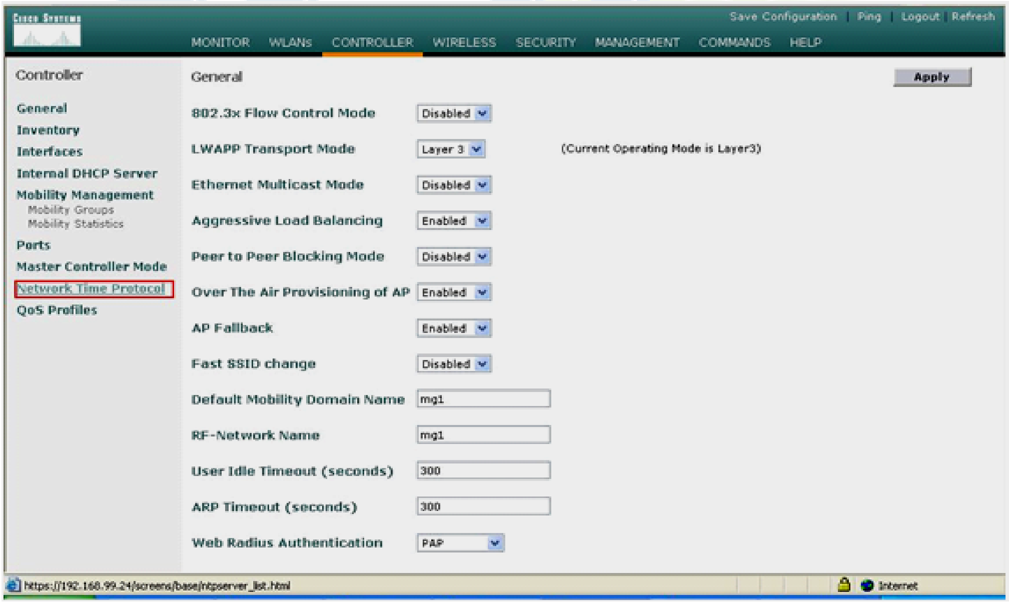
User name: cisco

Password: •••••

□ Remember my password

© 2002-2006 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

Hình 66



General

802.3x Flow Control Mode	Disabled	
LWAPP Transport Mode	Layer 3	(Current Operating Mode is Layer3)
Ethernet Multicast Mode	Disabled	
Aggressive Load Balancing	Enabled	
Peer to Peer Blocking Mode	Disabled	
Over The Air Provisioning of AP	Enabled	
AP Fallback	Enabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	mg1	
RF-Network Name	mg1	
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	

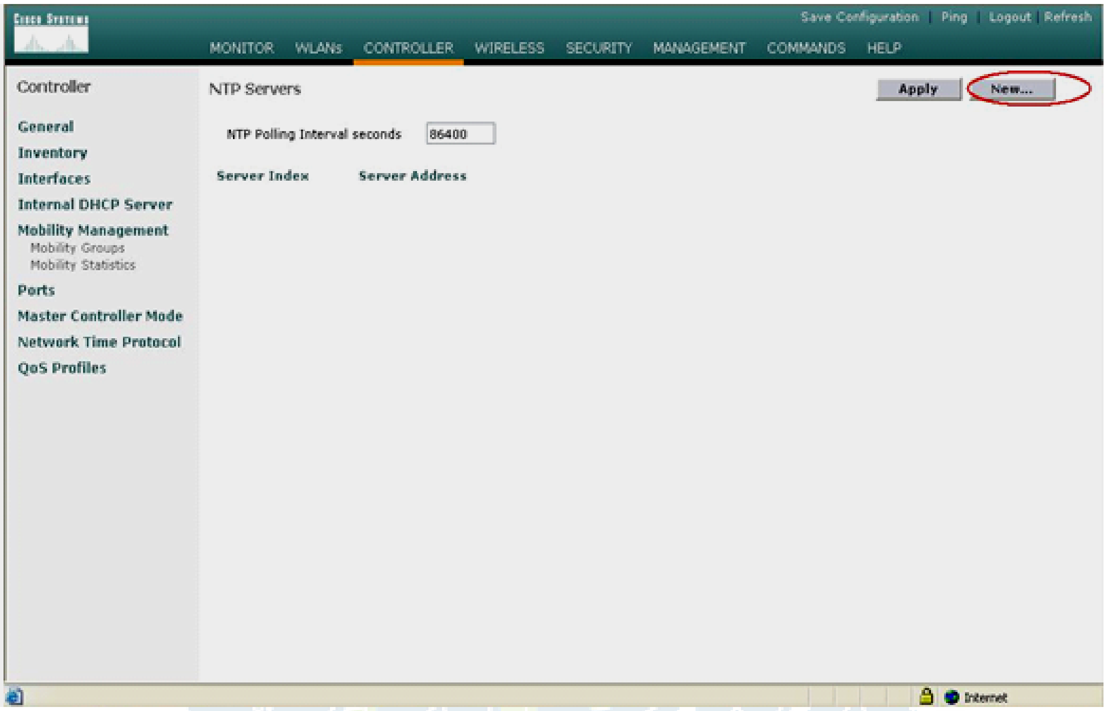
https://192.168.99.24/screens/base/ntpserver_list.html

Hình 67

Chọn New để khai báo thời gian mới cho server (hình 68), cần cấu hình trên router 2811 là thiết bị cấp thời gian clock chủ đạo dùng câu lệnh:

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

Chọn **Apply** (hình 69).

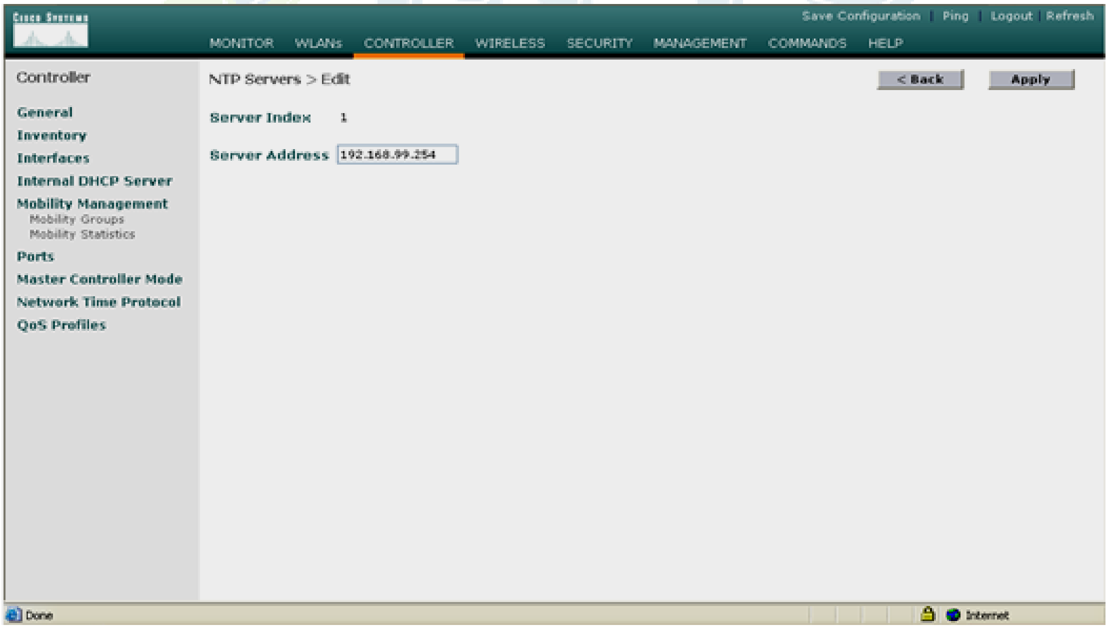


NTP Servers

NTP Polling Interval seconds 86400

Server Index Server Address

Hình 68



NTP Servers > Edit

Server Index 1

Server Address 192.168.99.254

Hình 69

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 70.

Cấu hình các thông số cho Wireless Client (hình 71).

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

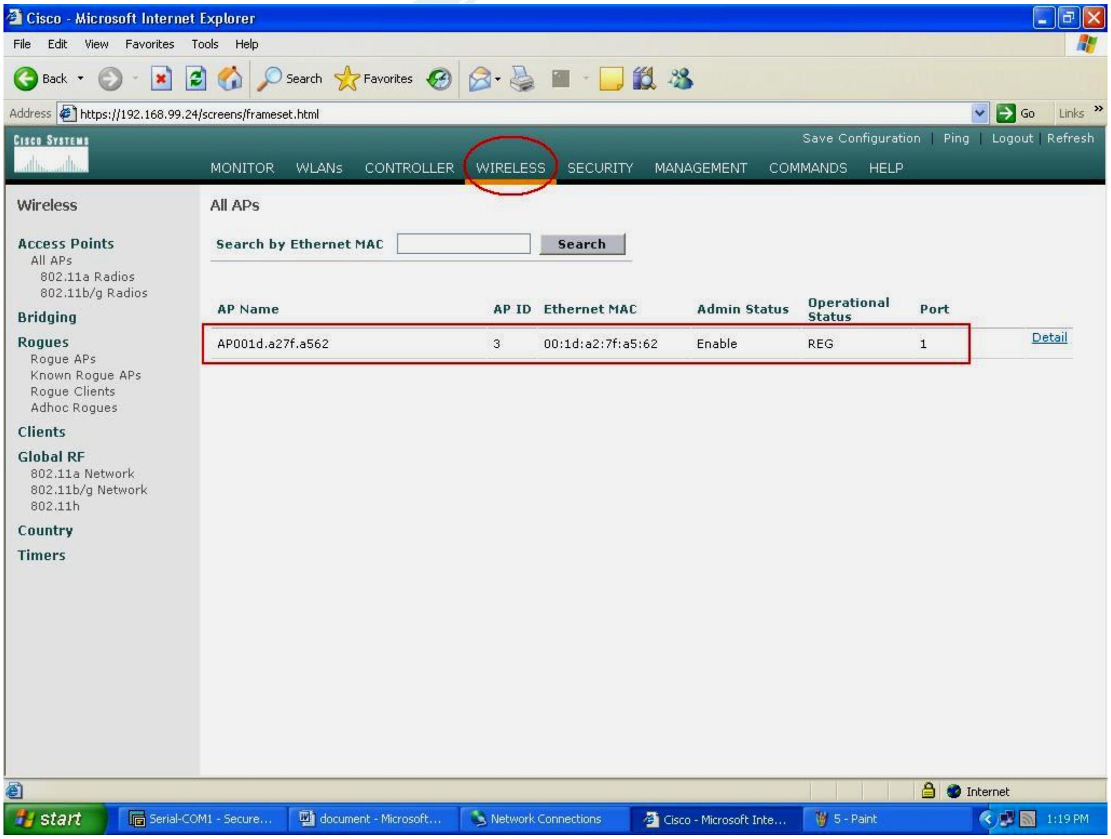
Nhập tên Interface và VLAN (trong trường hợp này giả định wireless client dùng vlan2 có địa chỉ mạng 192.168.2.0/24) sau đó click **Apply**.

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 72).

Kiểm tra lại cấu hình.

Kết quả thu được (hình 73).

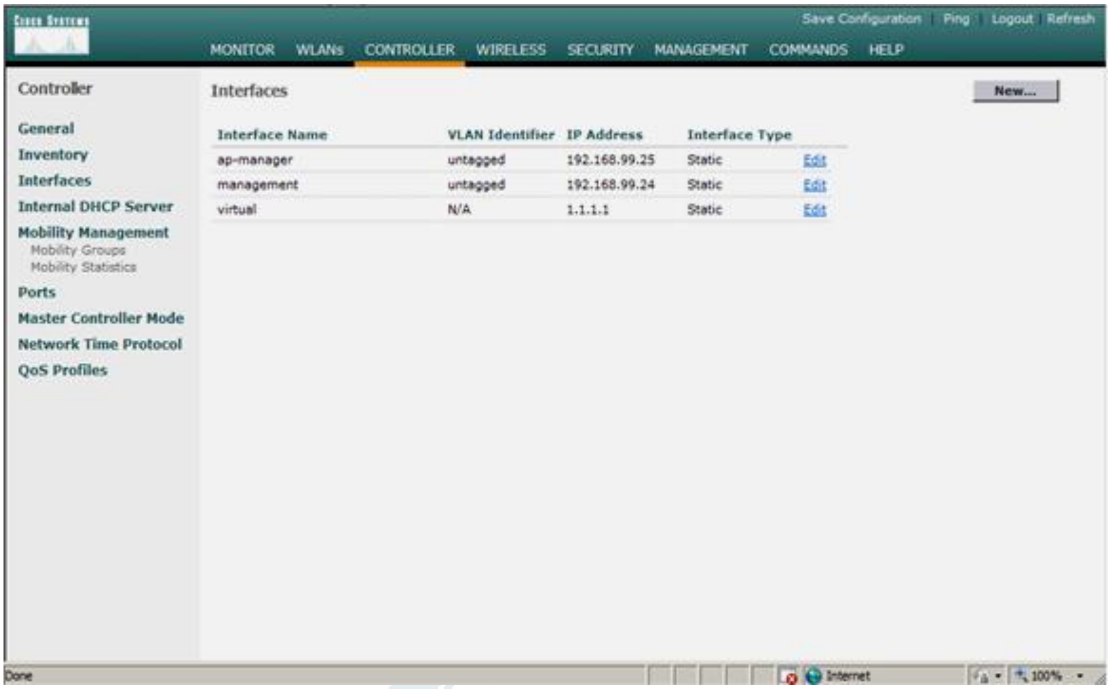


All APs

Search by Ethernet MAC

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
AP001d.a27f.a562	3	00:1d:a2:7f:a5:62	Enable	REG	1	Detail

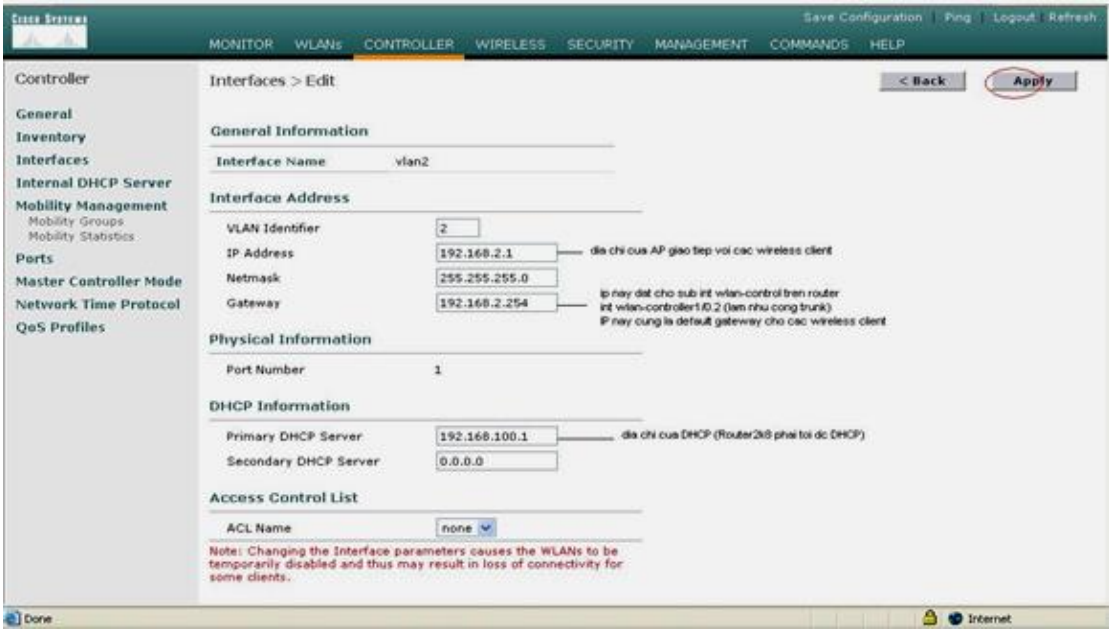
Hình 70



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	
ap-manager	untagged	192.168.99.25	Static	Edit
management	untagged	192.168.99.24	Static	Edit
virtual	N/A	1.1.1.1	Static	Edit

Hình 71



Interfaces > Edit

General Information

Interface Name: vlan2

Interface Address

VLAN Identifier: 2

IP Address: 192.168.2.1 — dia chi cua AP giao tiep voi cac wireless client

Netmask: 255.255.255.0

Gateway: 192.168.2.254 — ip nay dat cho sub int wlan-control tren router
int wlan-controller1/0.2 (lam nhu cong trunk)
IP nay cung la default gateway cho cac wireless client

Physical Information

Port Number: 1

DHCP Information

Primary DHCP Server: 192.168.100.1 — dia chi cua DHCP (Router2k8 phai toi dc DHCP)

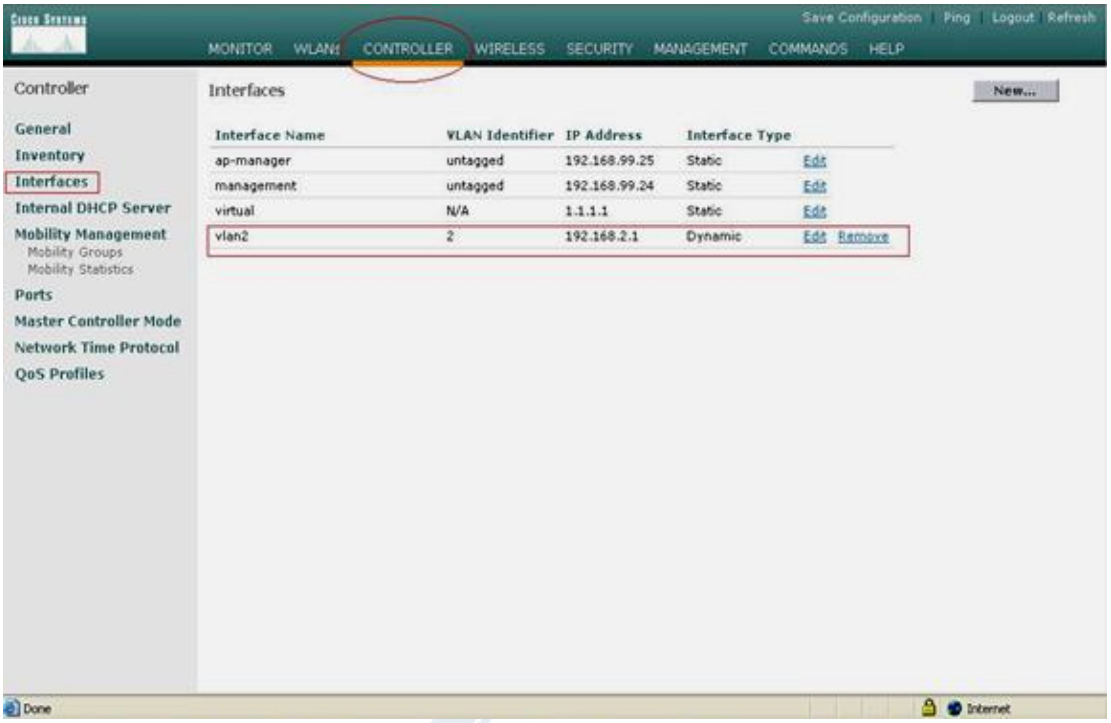
Secondary DHCP Server: 0.0.0.0

Access Control List

ACL Name: none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

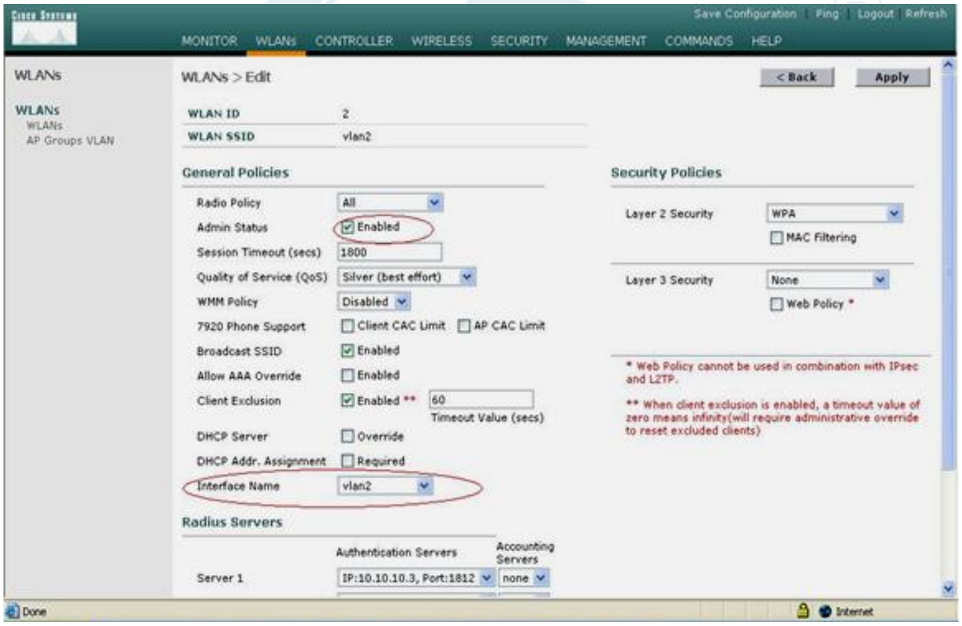
Hình 72



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type		
ap-manager	untagged	192.168.99.25	Static	Edit	
management	untagged	192.168.99.24	Static	Edit	
virtual	N/A	1.1.1.1	Static	Edit	
vlan2	2	192.168.2.1	Dynamic	Edit	Remove

Hình 73



WLANs > Edit

WLAN ID 2

WLAN SSID vlan2

General Policies

Radio Policy: All

Admin Status: ☑ Enabled

Session Timeout (secs): 1800

Quality of Service (QoS): Silver (best effort)

WMM Policy: Disabled

7920 Phone Support: □ Client CAC Limit □ AP CAC Limit

Broadcast SSID: ☑ Enabled

Allow AAA Override: □ Enabled

Client Exclusion: ☑ Enabled ** 60 Timeout Value (secs)

DHCP Server: □ Override

DHCP Addr. Assignment: □ Required

Interface Name: vlan2

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.10.10.3, Port:1812	none

Security Policies

Layer 2 Security: WPA

□ MAC Filtering

Layer 3 Security: None

□ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Hình 74

- 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**. Click **Apply**.
- Chọn **vlan2** từ thanh thực đơn **Interface Name** ở cuối cửa sổ, và click **Apply** (hình 74).
- Trong trường hợp này, SSID vlan2 được kết hợp với **Interface Name vlan2**.

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.

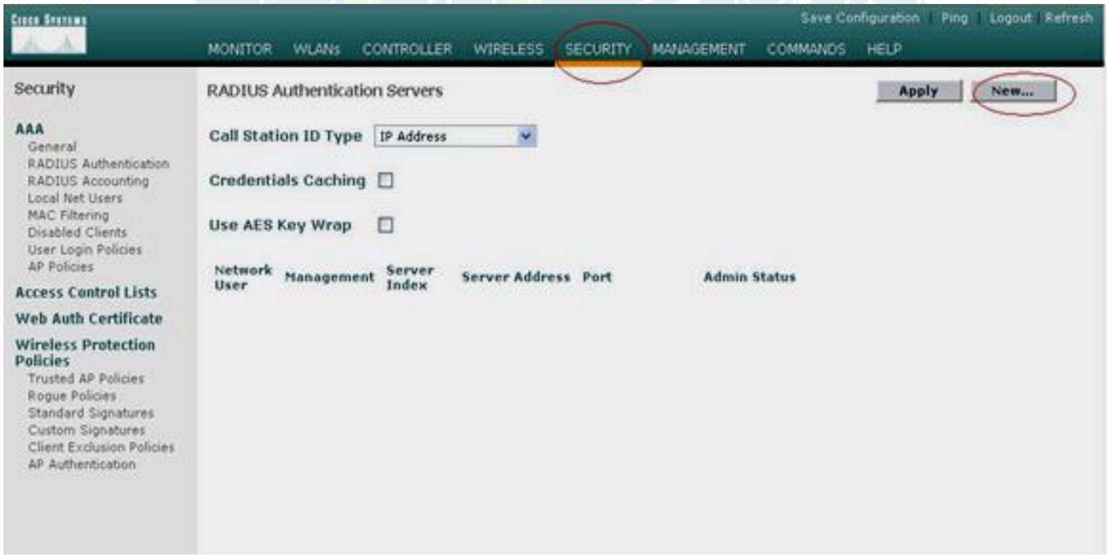
```
R1(config)#interface wlan-controller 1/0.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip address 192.168.2.254 255.255.255.0
```

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 75).



RADIUS Authentication Servers

Call Station ID Type: IP Address

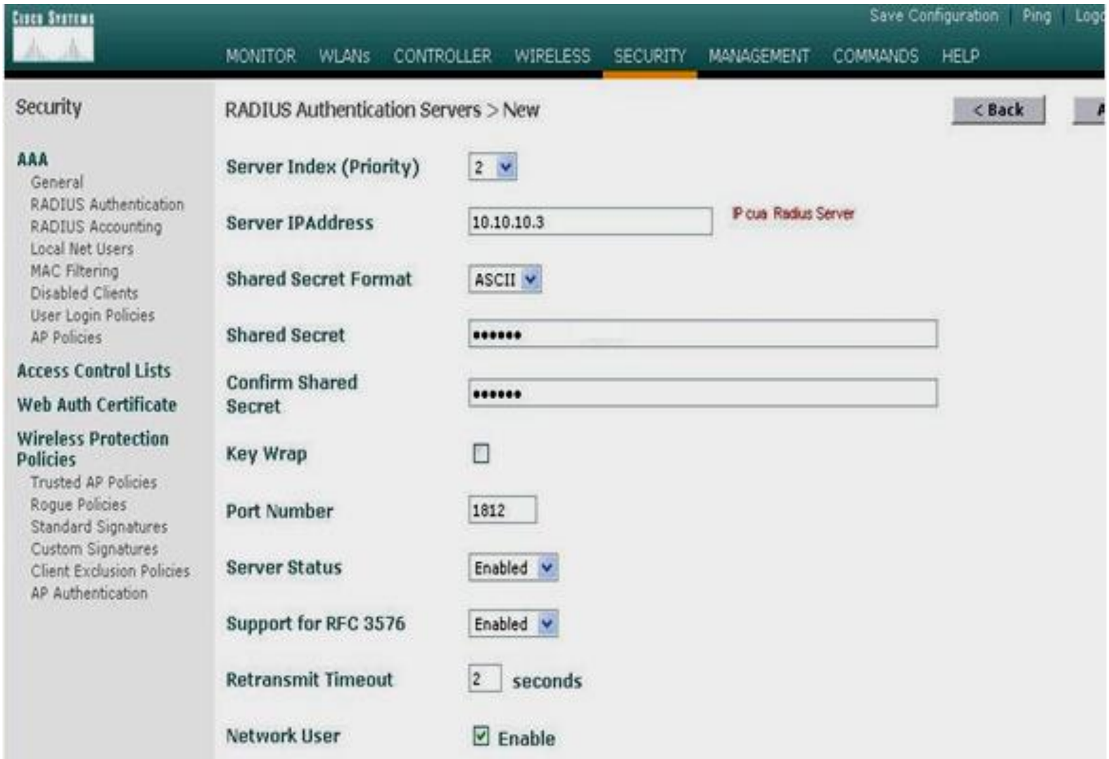
Credentials Caching ☐

Use AES Key Wrap ☐

Network User	Management	Server Index	Server Address	Port	Admin Status

Hình 75

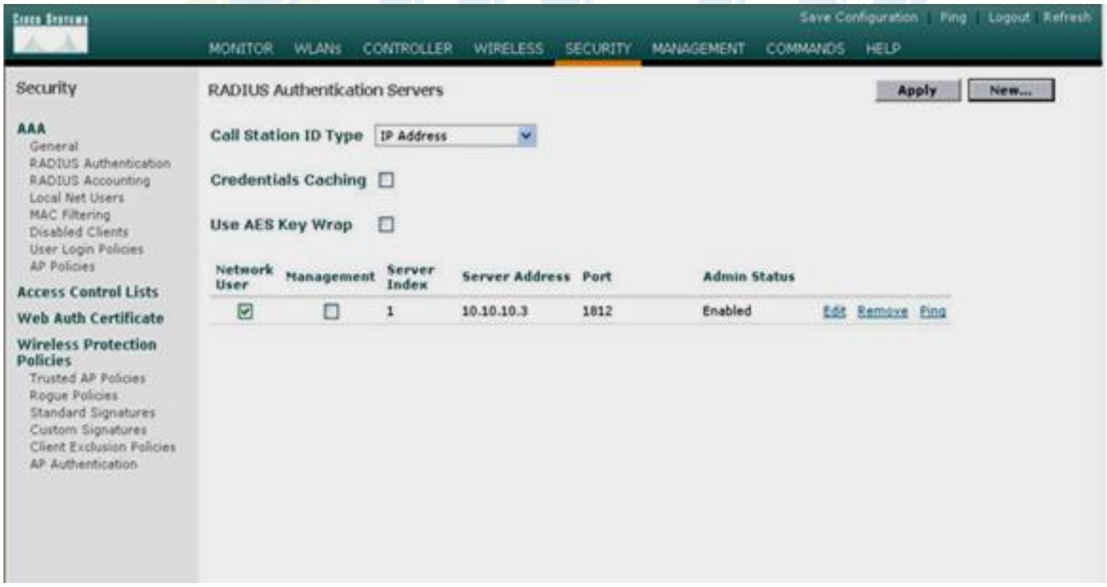
Khai báo sự tồn tại của ACS server (đóng vai trò máy chủ xác thực Radius) – hình 78. Chọn Apply (hình 77).



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IPAddress	10.10.10.3 IP của Radius Server
Shared Secret Format	ASCII
Shared Secret	••••••
Confirm Shared Secret	••••••
Key Wrap	□
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Retransmit Timeout	2 seconds
Network User	☑ Enable

Hình 76



RADIUS Authentication Servers

Call Station ID Type: IP Address

Credentials Caching □

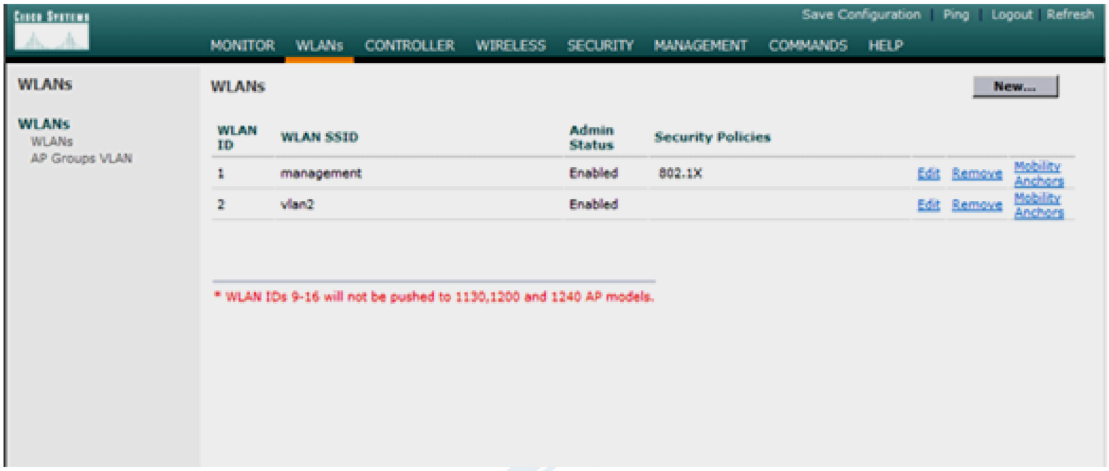
Use AES Key Wrap □

Network User	Management	Server Index	Server Address	Port	Admin Status	
☑	□	1	10.10.10.3	1812	Enabled	Edit Remove Ping

Hình 77

Cấu hình xác thực LEAP.

Vào WLAN để chọn kiểu xác thực, dùng edit để chỉnh sửa thông tin của SSID vlan2 (hình 78).



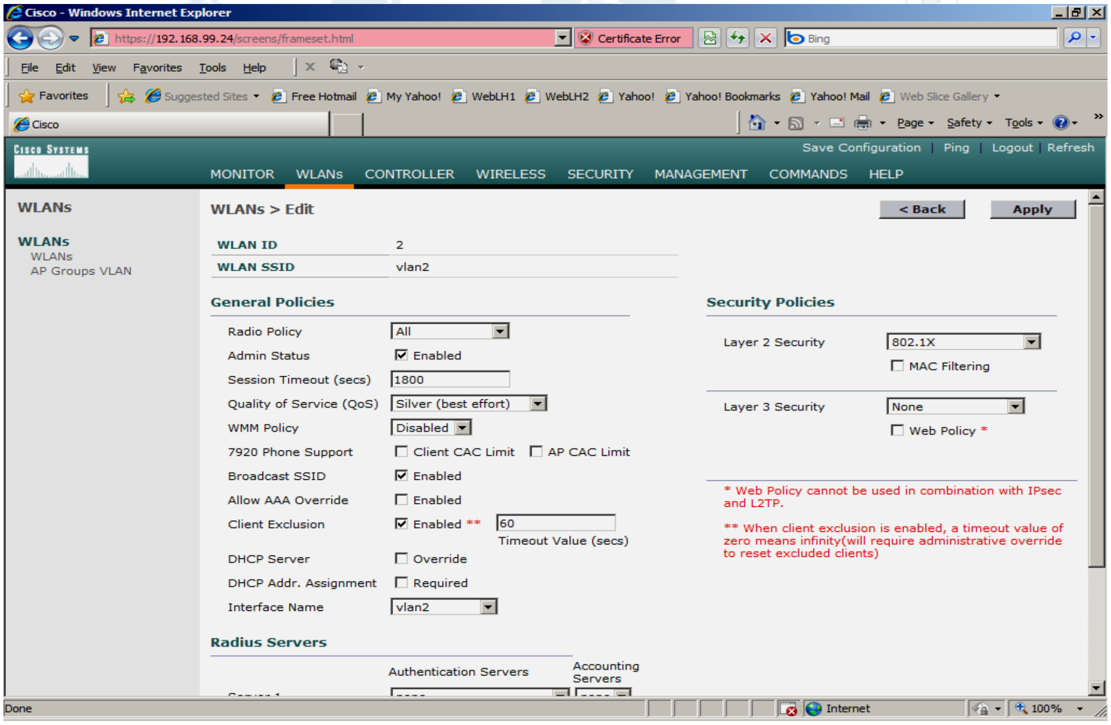
WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	management	Enabled	802.1X	Edit	Remove	Mobility Anchors
2	vlan2	Enabled		Edit	Remove	Mobility Anchors

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Hình 78

Chọn 802.1X trong phần Layer 2 security (hình 79).



WLANs > Edit

WLAN ID	2
WLAN SSID	vlan2

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	1800
Quality of Service (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Phone Support	□ Client CAC Limit □ AP CAC Limit
Broadcast SSID	☑ Enabled
Allow AAA Override	□ Enabled
Client Exclusion	☑ Enabled ** 60 Timeout Value (secs)
DHCP Server	□ Override
DHCP Addr. Assignment	□ Required
Interface Name	vlan2

Security Policies

Layer 2 Security	802.1X □ MAC Filtering
Layer 3 Security	None □ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

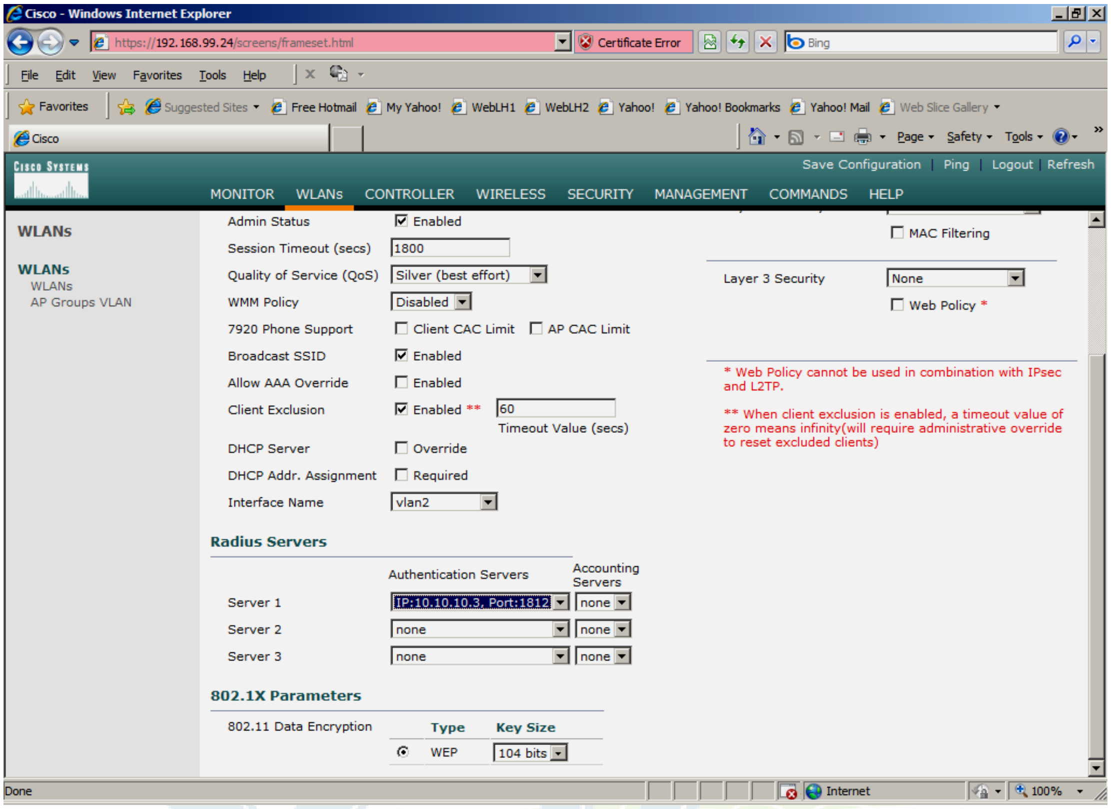
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Radius Servers

Authentication Servers Accounting Servers

Hình 79

Trong phần server1 chọn 10.10.10.3 (hình 80).


Cisco - Windows Internet Explorer
https://192.168.99.24/screens/frameset.html
Certificate Error
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
WLANs
WLANs
AP Groups VLAN

Admin Status ☑ Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support □ Client CAC Limit □ AP CAC Limit
Broadcast SSID ☑ Enabled
Allow AAA Override □ Enabled
Client Exclusion ☑ Enabled ** 60 Timeout Value (secs)
DHCP Server □ Override
DHCP Addr. Assignment □ Required
Interface Name vlan2

□ MAC Filtering
Layer 3 Security None
□ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.10.10.3, Port:1812	none
Server 2	none	none
Server 3	none	none

802.1X Parameters

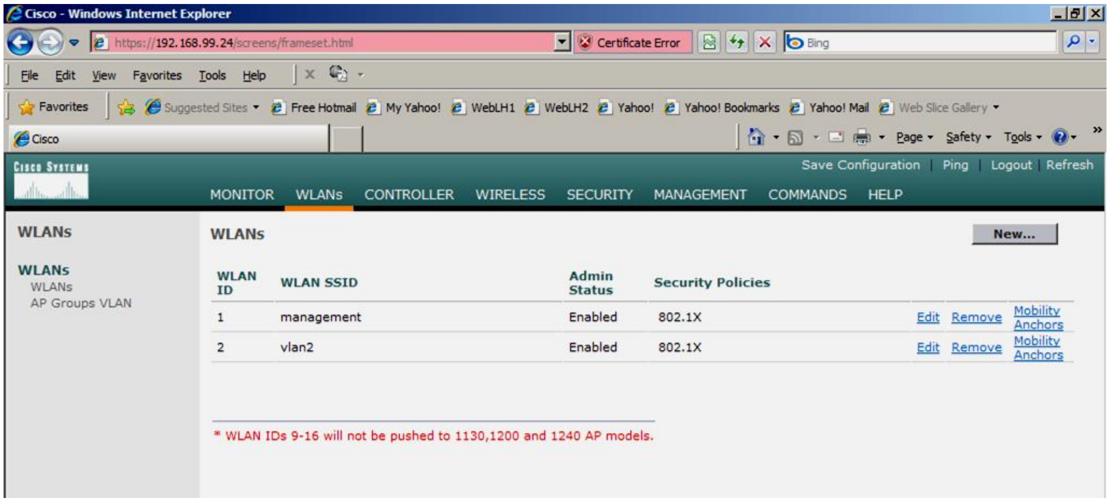
802.11 Data Encryption		Type	Key Size
	●	WEP	104 bits

Done Internet 100%

Hình 80

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 81).


Cisco - Windows Internet Explorer
https://192.168.99.24/screens/frameset.html
Certificate Error
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
WLANs
WLANs
AP Groups VLAN
New...

WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies			
1	management	Enabled	802.1X	Edit	Remove	Mobility Anchors
2	vlan2	Enabled	802.1X	Edit	Remove	Mobility Anchors

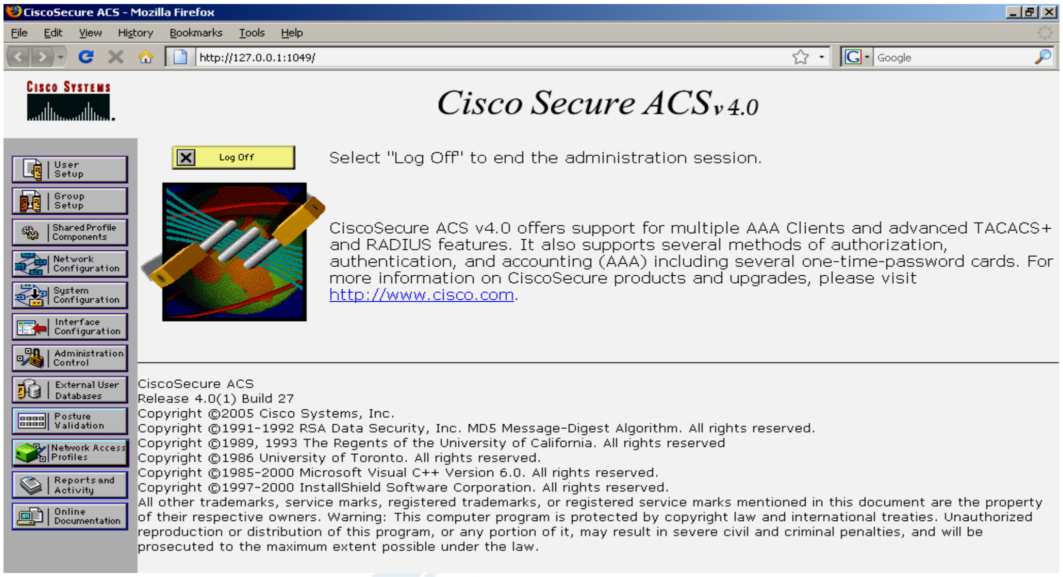
* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Hình 81

Cấu hình trên ACS hỗ trợ xác thực bằng LEAP.

Truy nhập vào đường liên kết cấu hình ACS (hình 82).

Tạo thêm tài khoản người dùng mới (hình 83).

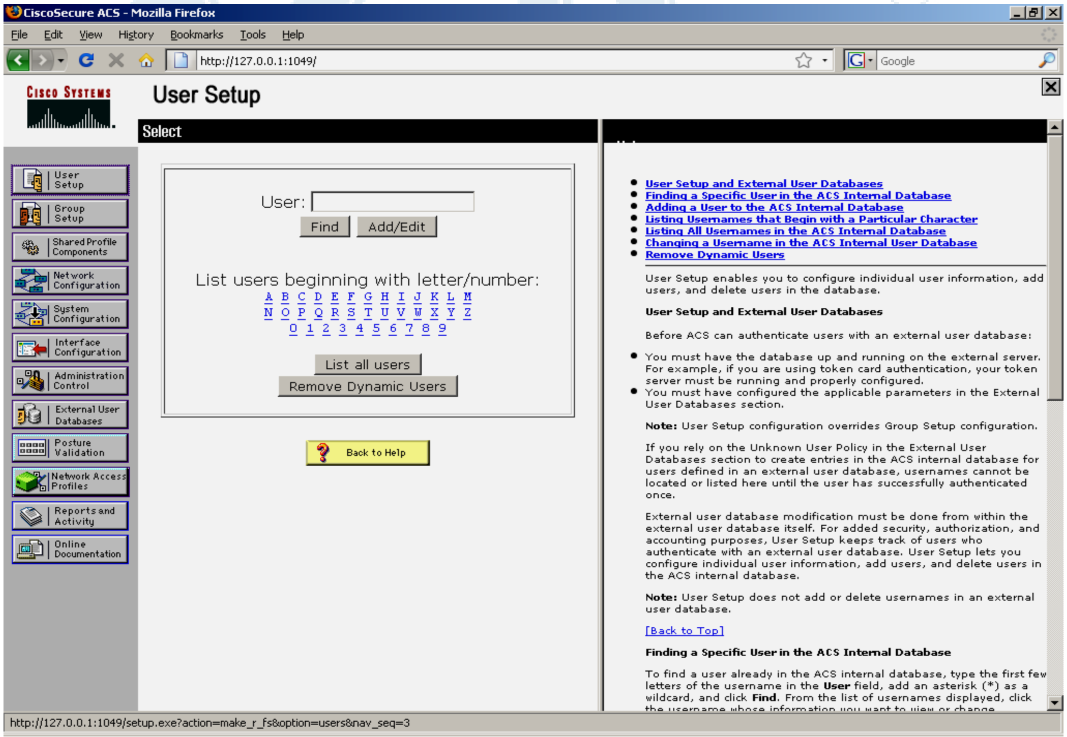


Select "Log Off" to end the administration session.

CiscoSecure ACS v4.0 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 4.0(1) Build 27
Copyright ©2005 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Hình 82


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://127.0.0.1:1049/
Google
Cisco Systems
User Setup
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User:
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
[Back to Top]
http://127.0.0.1:1049/setup.exe?action=make_r_fs&option=users&nav_seq=3

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

Note: User Setup does not add or delete usernames in an external user database.

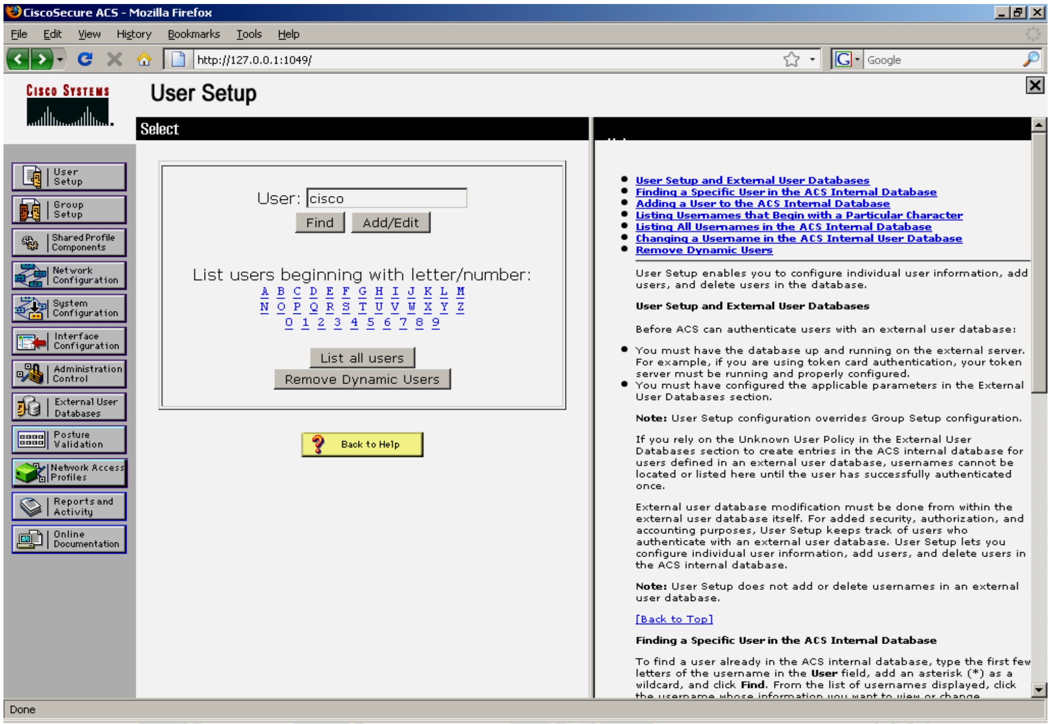
Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the **User** field, add an asterisk (*) as a wildcard, and click **Find**. From the list of usernames displayed, click the username whose information you want to view or change

Hình 83

Nhập vào Username: cisco (hình 84).

Nhập Password: cisco123 → chọn submit (hình 85).



User Setup

Select

User: cisco

Find | Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

List all users

Remove Dynamic Users

Back to Help

- User Setup and External User Databases
- Finding a Specific User in the ACS Internal Database
- Adding a User to the ACS Internal Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the ACS Internal Database
- Changing a Username in the ACS Internal User Database
- Remove Dynamic Users

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

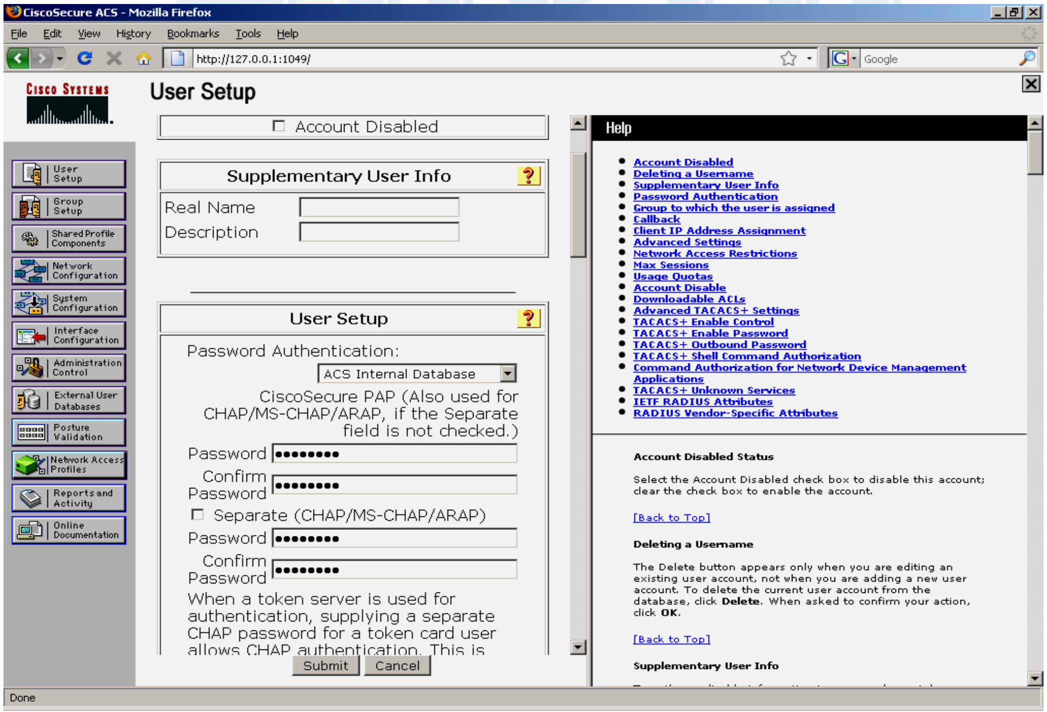
Note: User Setup does not add or delete usernames in an external user database.

[Back to Top]

Finding a Specific User in the ACS Internal Database

To find a user already in the ACS internal database, type the first few letters of the username in the **User** field, add an asterisk (*) as a wildcard, and click **Find**. From the list of usernames displayed, click the username whose information you want to view or change

Hình 84



User Setup

☐ Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ••••••••

Confirm Password ••••••••

☐ Separate (CHAP/MS-CHAP/ARAP)

Password ••••••••

Confirm Password ••••••••

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is

Submit | Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

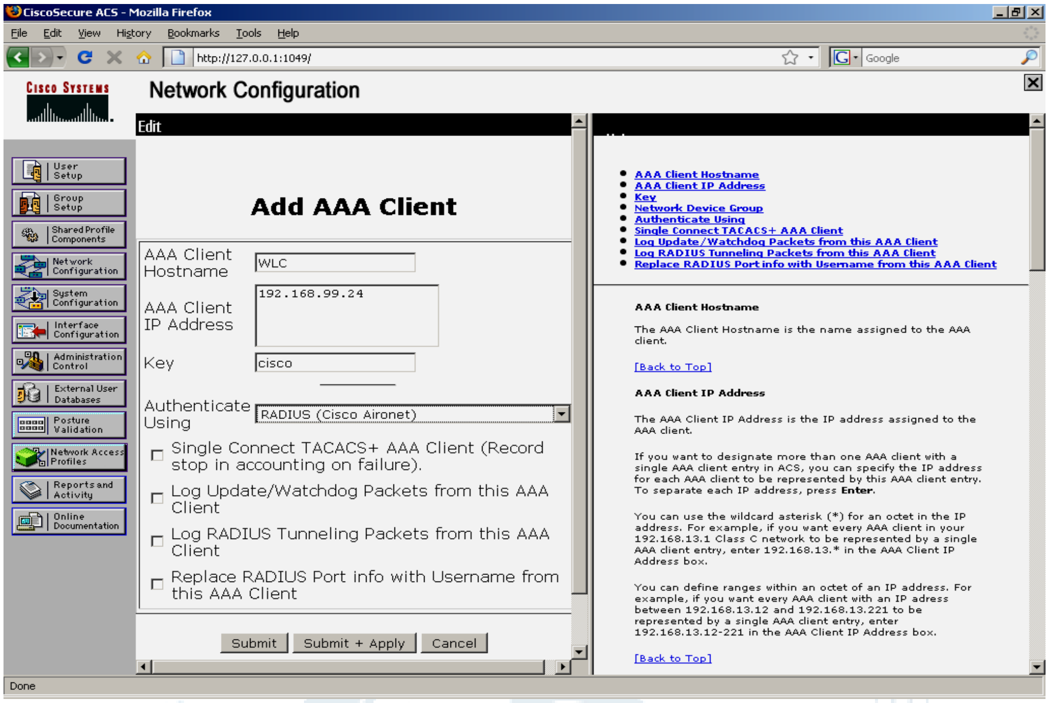
[Back to Top]

Supplementary User Info

Hình 85

Khai báo sự tồn tại của WLC trên ACS (hình 86).

Chọn Submit + Apply và xem kết quả (hình 87).



Network Configuration

Add AAA Client

AAA Client Hostname	WLC
AAA Client IP Address	192.168.99.24
Key	cisco
Authenticate Using	RADIUS (Cisco Aironet)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

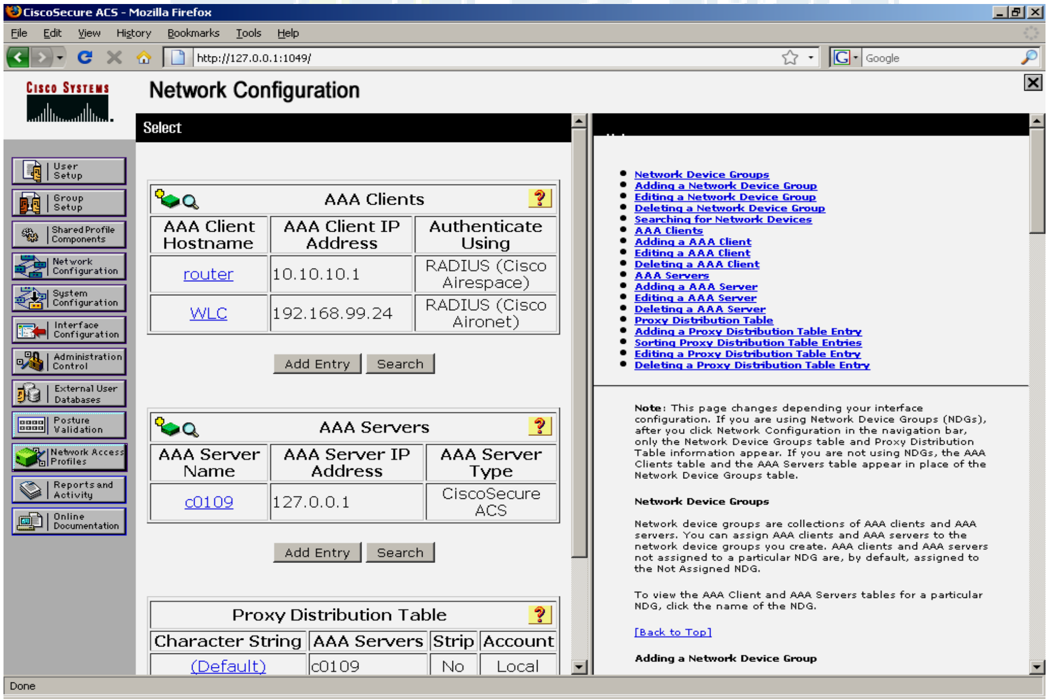
If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP adress between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

[Back to Top]

Hình 86



Network Configuration

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
router	10.10.10.1	RADIUS (Cisco Airespace)
WLC	192.168.99.24	RADIUS (Cisco Aironet)

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
c0109	127.0.0.1	CiscoSecure ACS

Proxy Distribution Table

Character String	AAA Servers	Strip	Account
(Default)	c0109	No	Local

- Network Device Groups
- Adding a Network Device Group
- Editing a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG.

To view the AAA Client and AAA Servers tables for a particular NDG, click the name of the NDG.

[Back to Top]

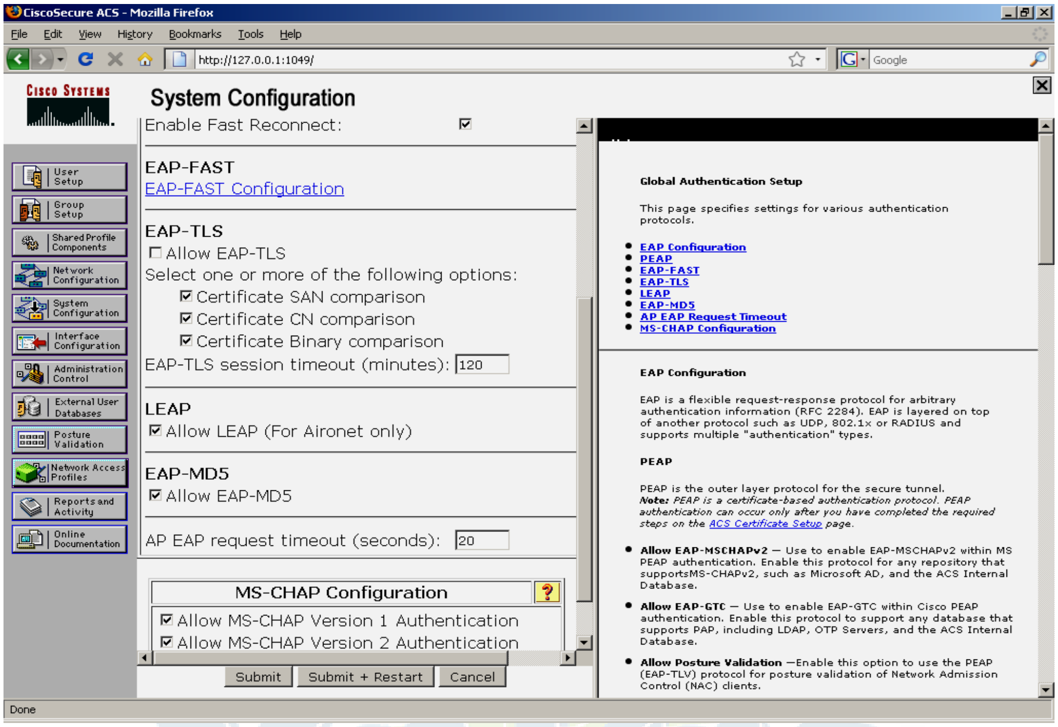
Adding a Network Device Group

Hình 87

Khai báo kiểu xác thực LEAP trên ACS.

Chọn system configuration.

Chọn check box LEAP để kích hoạt LEAP (hình 88).



System Configuration

Enable Fast Reconnect: ☑

EAP-FAST

EAP-FAST Configuration

EAP-TLS

□ Allow EAP-TLS

Select one or more of the following options:

☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

LEAP

☑ Allow LEAP (For Aironet only)

EAP-MD5

☑ Allow EAP-MD5

AP EAP request timeout (seconds): 20

MS-CHAP Configuration

☑ Allow MS-CHAP Version 1 Authentication

☑ Allow MS-CHAP Version 2 Authentication

Global Authentication Setup

This page specifies settings for various authentication protocols.

- EAP Configuration
- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- AP EAP Request Timeout
- MS-CHAP Configuration

EAP Configuration

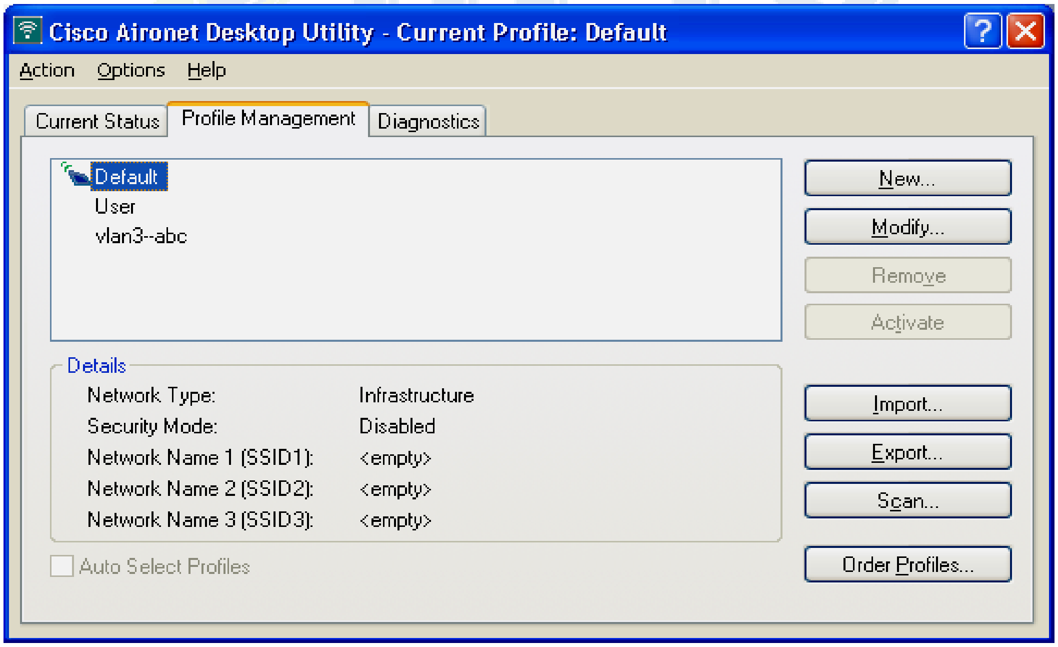
EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

PEAP

PEAP is the outer layer protocol for the secure tunnel.
Note: *PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.*

- **Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supportsMS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow Posture Validation** —Enable this option to use the PEAP (EAP-TLV) protocol for posture validation of Network Admission Control (NAC) clients.

Hình 88



Details

Network Type:	Infrastructure
Security Mode:	Disabled
Network Name 1 (SSID1):	<empty>
Network Name 2 (SSID2):	<empty>
Network Name 3 (SSID3):	<empty>

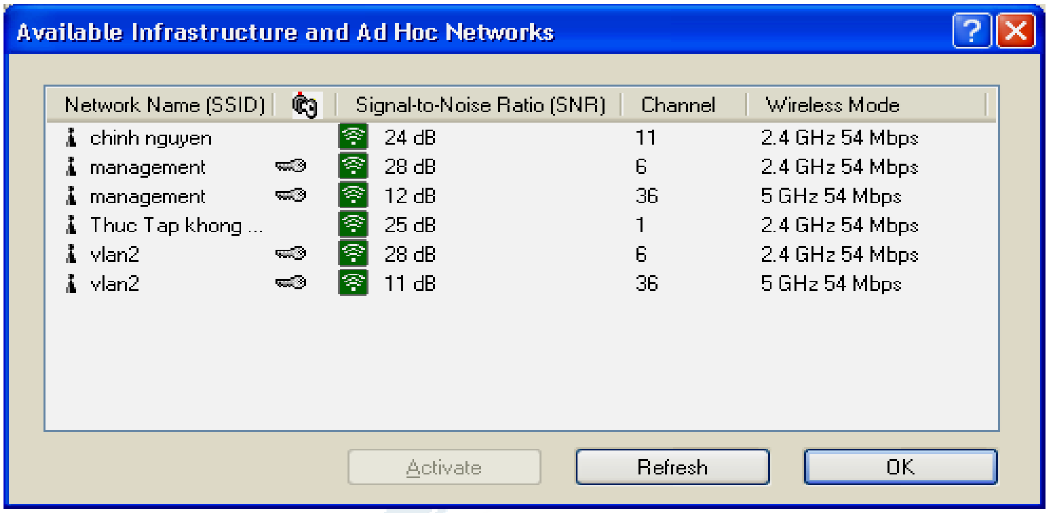
Hình 89

Cấu hình client quy định xác thực kiểu LEAP.

Khởi tạo chương trình Cisco Aironet Desktop Utility (hình 89).

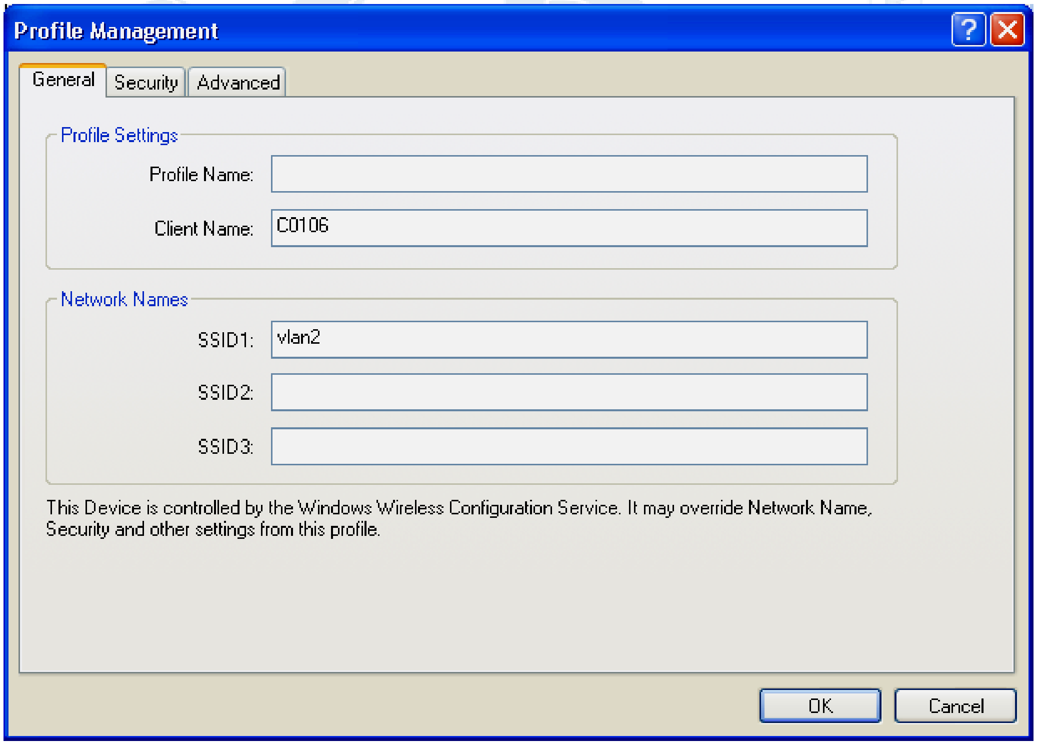
Chọn Scan để tìm SSID vlan2.

Chọn vlan 2→ OK (hình 90).



Network Name (SSID)		Signal-to-Noise Ratio (SNR)	Channel	Wireless Mode
chinh nguyen		24 dB	11	2.4 GHz 54 Mbps
management	🔑	28 dB	6	2.4 GHz 54 Mbps
management	🔑	12 dB	36	5 GHz 54 Mbps
Thuc Tap khong ...		25 dB	1	2.4 GHz 54 Mbps
vlan2	🔑	28 dB	6	2.4 GHz 54 Mbps
vlan2	🔑	11 dB	36	5 GHz 54 Mbps

Hình 90



Profile Settings

Profile Name:

Client Name: C0106

Network Names

SSID1: vlan2

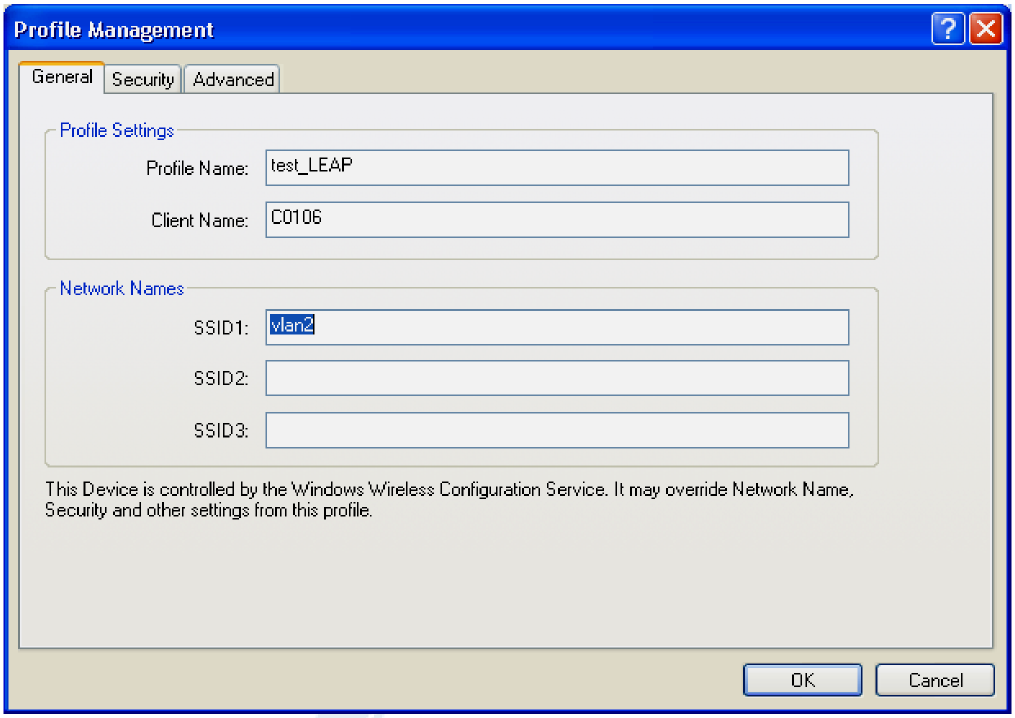
SSID2:

SSID3:

This Device is controlled by the Windows Wireless Configuration Service. It may override Network Name, Security and other settings from this profile.

Hình 91

Điền thông tin để tạo profile mới (hình 92).



Profile Settings

Profile Name: test_LEAP

Client Name: C0106

Network Names

SSID1: vlan2

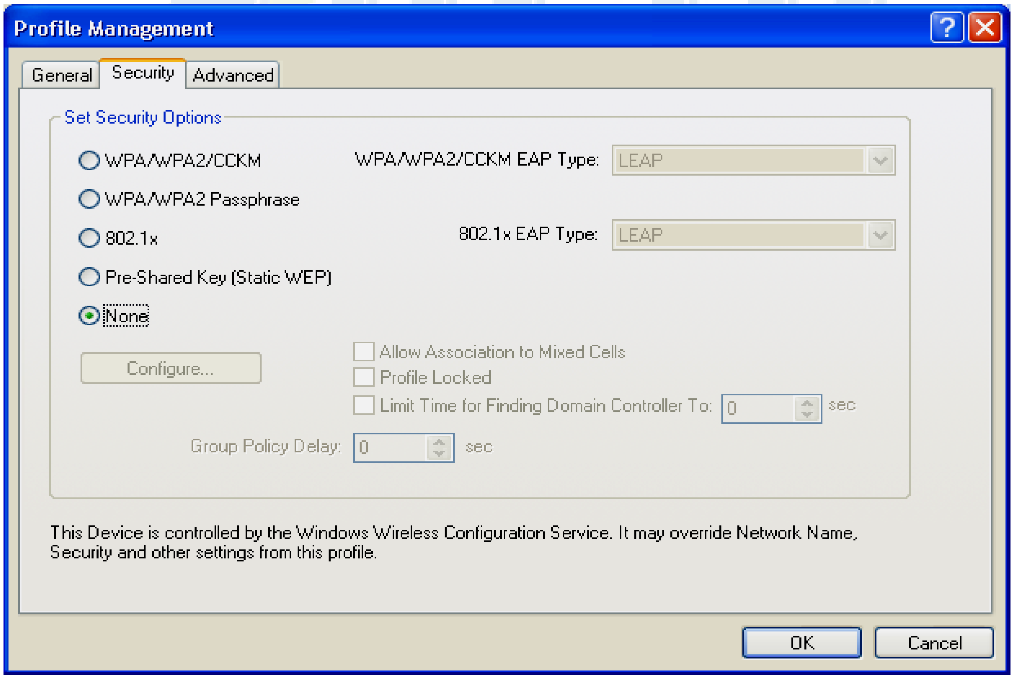
SSID2:

SSID3:

This Device is controlled by the Windows Wireless Configuration Service. It may override Network Name, Security and other settings from this profile.

Hình 92

Vào tab security (hình 93).



Set Security Options

○ WPA/WPA2/CCKM

WPA/WPA2/CCKM EAP Type: LEAP

○ WPA/WPA2 Passphrase

○ 802.1x

802.1x EAP Type: LEAP

○ Pre-Shared Key (Static WEP)

● None

□ Allow Association to Mixed Cells

□ Profile Locked

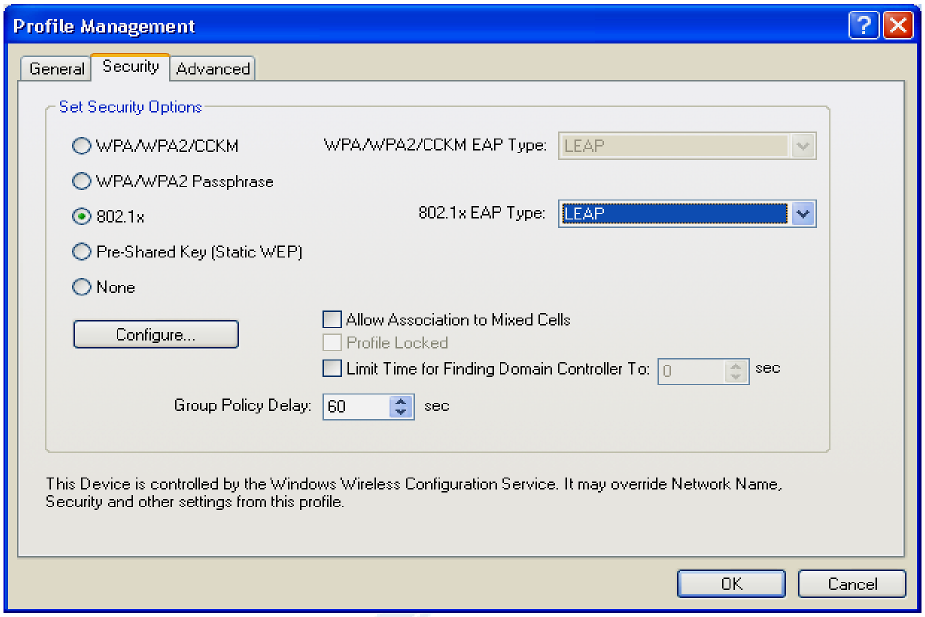
□ Limit Time for Finding Domain Controller To: 0 sec

Group Policy Delay: 0 sec

This Device is controlled by the Windows Wireless Configuration Service. It may override Network Name, Security and other settings from this profile.

Hình 93

Trong 802.1x EAP Type, chọn LEAP, chọn Configure (hình 94).



Profile Management

General | Security | Advanced

Set Security Options

○ WPA/WPA2/CCKM — WPA/WPA2/CCKM EAP Type: LEAP

○ WPA/WPA2 Passphrase

● 802.1x — 802.1x EAP Type: LEAP

○ Pre-Shared Key (Static WEP)

○ None

Configure...

□ Allow Association to Mixed Cells

□ Profile Locked

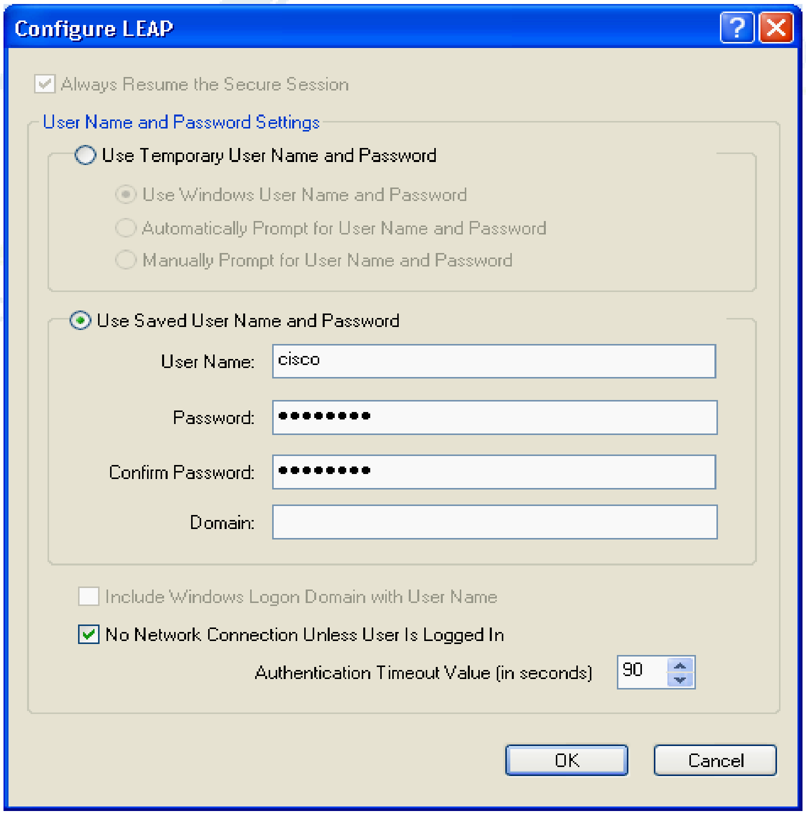
□ Limit Time for Finding Domain Controller To: 0 sec

Group Policy Delay: 60 sec

This Device is controlled by the Windows Wireless Configuration Service. It may override Network Name, Security and other settings from this profile.

OK | Cancel

Hình 94



Configure LEAP

☑ Always Resume the Secure Session

User Name and Password Settings

○ Use Temporary User Name and Password

● Use Windows User Name and Password

○ Automatically Prompt for User Name and Password

○ Manually Prompt for User Name and Password

● Use Saved User Name and Password

User Name: cisco

Password: •••••••••

Confirm Password: •••••••••

Domain:

□ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

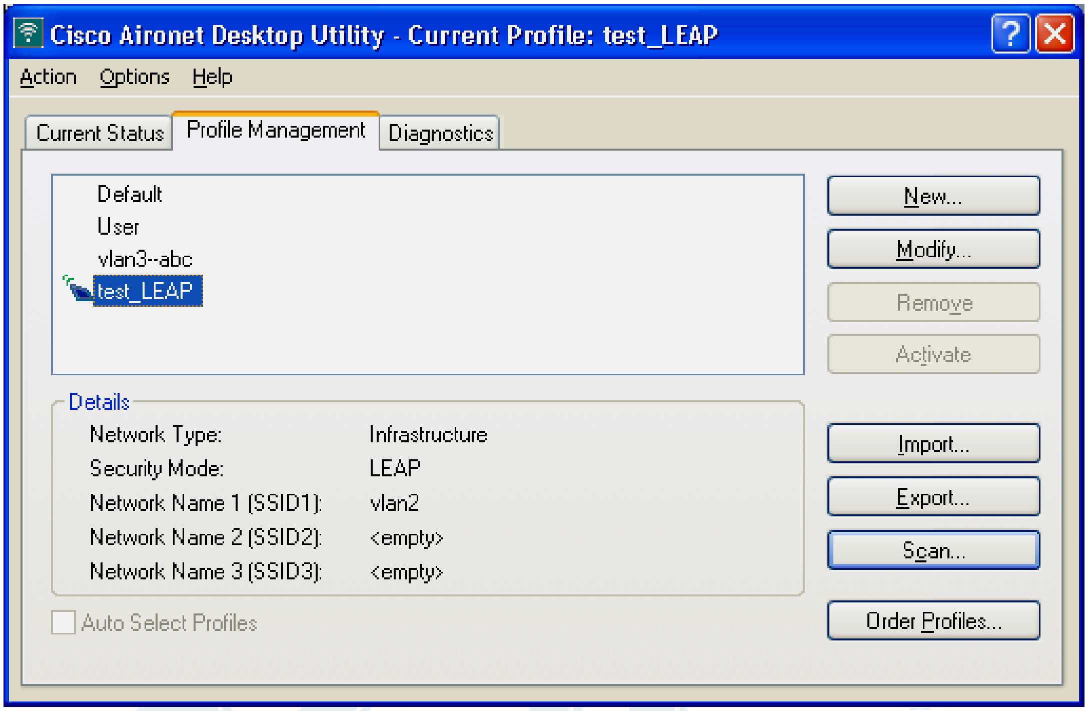
Authentication Timeout Value (in seconds) 90

OK | Cancel

Hình 95

Điền thông tin username và password, nhấn OK (hình 95).

Kết quả (hình 96).



Cisco Aironet Desktop Utility - Current Profile: test_LEAP

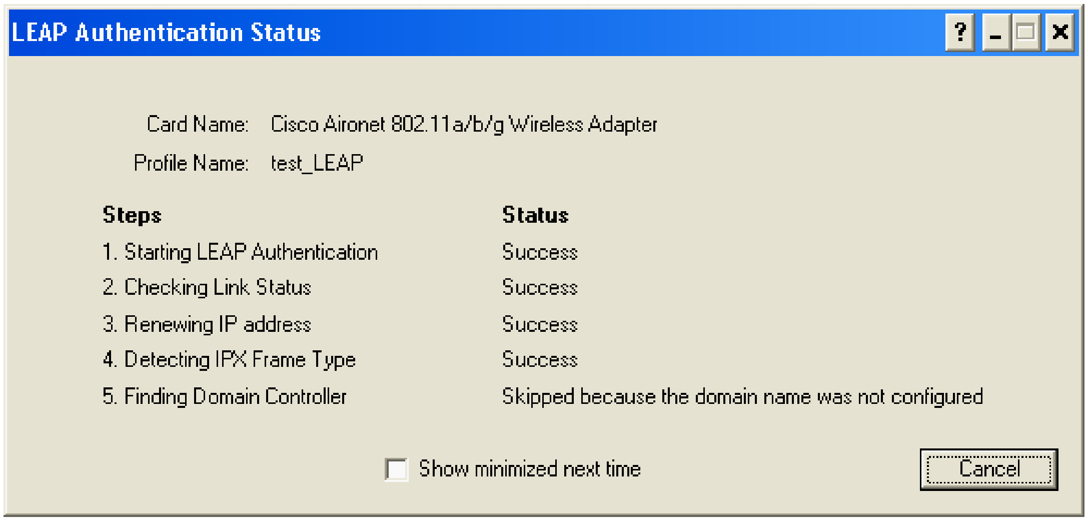
Details

Network Type: Infrastructure
Security Mode: LEAP
Network Name 1 (SSID1): vlan2
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

□ Auto Select Profiles

Hình 96

Kết nối thành công (hình 97).



LEAP Authentication Status

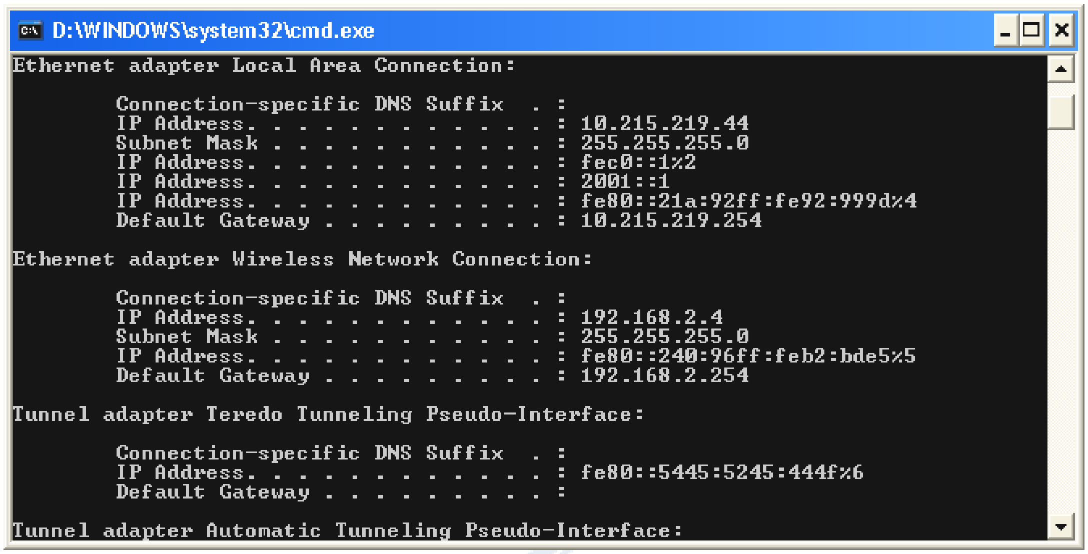
Card Name: Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name: test_LEAP

Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured

□ Show minimized next time

Hình 97

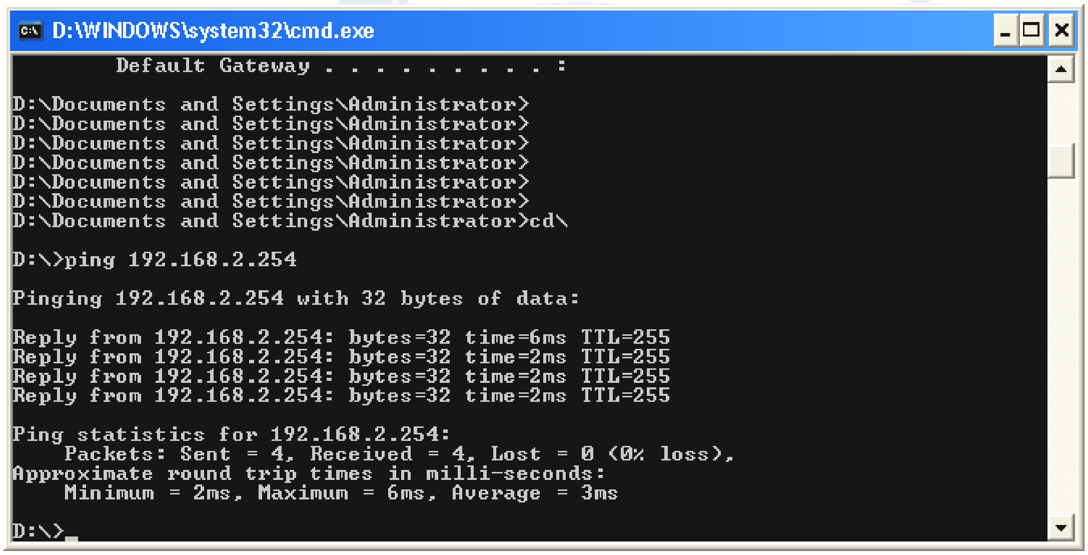
Kiểm tra kết quả bằng lệnh C:\>ipconfig /all trong cửa sổ cmd của Window (hình 98).



```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.215.219.44
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fec0::1%2
        IP Address. . . . . . . . . . . . : 2001::1
        IP Address. . . . . . . . . . . . : fe80::21a:92ff:fe92:999d%4
        Default Gateway . . . . . . . . . : 10.215.219.254

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::240:96ff:feb2:bde5%5
        Default Gateway . . . . . . . . . : 192.168.2.254

Tunnel adapter Teredo Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5445:5245:444f%6
        Default Gateway . . . . . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:
```

Hình 98

Ping kiểm tra kết quả (hình 99).



```
        Default Gateway . . . . . . . . . :

D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>
D:\Documents and Settings\Administrator>cd\

D:\>ping 192.168.2.254

Pinging 192.168.2.254 with 32 bytes of data:

Reply from 192.168.2.254: bytes=32 time=6ms TTL=255
Reply from 192.168.2.254: bytes=32 time=2ms TTL=255
Reply from 192.168.2.254: bytes=32 time=2ms TTL=255
Reply from 192.168.2.254: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.2.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms

D:\>_
```

Hình 99