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



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
1
hostname c2811
1
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
enable secret 5 $1$QgGG$mjteEFA5x1onr2X3kuDp50
!
aaa session-id common
1
1
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
I.
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
1
ip dhcp pool vlan2
 network 192.168.2.0 255.255.255.0
  default-router 192.168.2.254
Т
```

LabPro Wireless

```
multilink bundle-name authenticated
!
username admin password 0 admin
1
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
1
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 200000
!
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): w115 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 <u>https://192.168.99.24</u> (hình 144).



Hình 144

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

ավիստուլիր	31		11-11	
	Cisco Controller			
	User name:	🖸 cisco	~	
Wireless	Password:	••••		
LAN Co	ntr	Remember my password		
				Login
		ОК	Cancel	
			4	

Hình 145

Cấu hình đ	ồng bộ thời	gian cho	WLC với R2811	(hình 146).
------------	-------------	----------	---------------	-------------

Conce Searces					Save Co	nfiguration	Ping Logout Refresh
As As	MONITOR WLANS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	General						Apply
General Inventory Interfaces Internal DHCP Server Mobility Management Mobility Groups Mobility Statistics	802.3x Flow Control Mode LWAPP Transport Mode Ethernet Multicost Mode Aggressive Load Balancing	Disabled V Layer 3 V Disabled V Enabled V	(Cur	rent Operating Mo	de is Layer3)		
Ports Master Controller Mode <u>Network Time Protocol</u> QoS Profiles	Peer to Peer Blocking Mode Over The Air Provisioning of AP Fallback Fast SSID change	Disabled V AP Enabled V Enabled V Disabled V					
	Default Mobility Domain Nar RF-Network Name User Idle Timeout (seconds) ARP Timeout (seconds)	mg1 mg1 () 300 () 300 () () () () () () () () () () () () ()					
https://192.168.99.24/screens/b	Web Radius Authentication	PAP 👻					🔒 🔮 Internet
		ID	146			(R

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.

Controller NTP Servers General NTP Poling Interv Inventory Interfaces Server Index Internal DHCP Server Mobility Management Mobility Kanagement Mobility Extensions	val seconds 86400 Server Address			Apply	New
General NTP Poling Intervi Inventory Interfaces Server Index Internal DHCP Server Mobility Management Mobility Extension	val seconds 86400 Server Address				
Mobility Statistics					
Ports Master Controller Mode Network Time Protocol QoS Profiles					

Hình 147

Chọn Apply (hình 148).

Casco Statema							Save Co	nfiguration Ping	Logout Refresh
A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	NTP Serve	ers > Edit						< Back	Apply
General	Server In	dex 1							
Inventory	Pomor Ac	Idease II	2 140 00 254						
Interfaces	Server A	idress 1	2.100.77.204						
Mobility Management Mobility Groups Mobility Statistics									
Ports									
Master Controller Mode									
Network Time Protocol									
QoS Profiles									
Done								🗳 🙂 🖻	ternet

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.

🗿 Cisco - Microsoft Internet	Explorer						
File Edit View Favorites 1	Tools Help						1
🚱 Back 🔹 🕥 🕤 💌	🛐 🚮 🔎 Search 🤺 Favorites 🥝	Ø• 🎍	🖩 - 📴 🇱 4	8			
Address 🛃 https://192.168.99.24	4/screens/frameset.html					~	ラ Go 🛛 Links 🂙
Cisco Systems alling adding	MONITOR WLANS CONTROLLER	WIRELES	SECURITY MAI	NAGEMENT COM	Save Configurati IMANDS HELP	on Ping	Logout Refresh
Wireless	All APs	-					
Access Points All APs 802.11a Radios	Search by Ethernet MAC		Search				
802.11b/g Radios	AP Name	AP ID	Ethernet MAC	Admin Status	Operational	Port	
Rogues Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues	AP001d.a27f.a562	3	00:1d:a2:7f:a5:62	Enable	REG	1	Detail
Clients							
Global RF 802.11a Network 802.11b/g Network 802.11b							
Country							
Timers							

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

- Chon Controller > Interfaces > New.

Controller Interfaces New General Inventory Interface Name VLAN Identifier IP Address Interface Type Interfaces ap-manager untagged 192.168.99.24 Static Edd Mobility Management Mobility Statistics N/A 1.1.1.1 Static Edd Network Time Protocol QoS Profiles Network Time Protocol N/A N/A N/A N/A	Casta District	wowmon		CONTROLLER	WARD FRE	SCORTS-	MUNICEMENT	Save Ci	Mouration	Ping Logout Refr
Interface Name VLAN Identifier IP Address Interface Type Inventory ap-manager untagged 192.168.99.25 Static Edit Interfaces management untagged 192.168.99.24 Static Edit Mobility Management MVA 1.1.1 Static Edit Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	Controller	Interfaces	mDans.	CONTROLLER	WINELESS	SECONDIT	PANALESEAT	COMMUNUS	NEOP	New
Intervalory ap-manager untagged 192.168.99.25 Static Edit management untagged 192.168.99.24 Static Edit Mobility Management Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	Inventory	Interface N	ame	VL	AN Identifier	IP Address	Interface	Туре		
Internal DHCP Server virtual N/A 1.1.1.1 Static Ldd Mobility Management wirtual N/A 1.1.1.1 Static Ldd Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	Interfaces	ap-manager		un	tegged	192.168.99.2	5 Static	Edd		
Mobility Management Mobility Management Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles	Internaces	management		un	tegged	192.168.99.2	4 Static	201		
	Mobility Management Mobility Groups Mobility Statistics Ports Master Controller Mode Network Time Protocol QoS Profiles									

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).

Case Station					Save Co	ofiguration Ping	Logout & Refresh
Controller General Inventory Interfaces Internal DHCP Server Mobility Management Mobility Statistics Poorts	MONITOR WLANS CO Interfaces > Edit General Information Interface Name Interface Address VLAN Identifier IP Address	vlan2	SECURITY M	giao tep voi cao v	COMMANDS	- Heck	Apply
Master Controller Mode Network Time Protocol QoS Profiles	Netmask Gateway Physical Information	255.255.255.0	ip nay dat ch int wish cont P nay cung i	o sub int wian-co roller1/0.2 (Jam n a default gateway	ntrol bren router nu cong trunk) r cho cac wireless	clent	
	Port Number DHCP Information	1					
	Primary DHCP Server Secondary DHCP Server Access Control List	192.168.100.1 0.0.0.0	dia chi ci	ua DHCP (Router2	NB phaitoi do DHO	5	
	ACL Name Note: Changing the Interface temporarily disabled and thu some clients.	none v e parameters causes the Wi is may result in loss of conr	LANs to be ectivity for				
Done .						A 🔹 1	nternet

Hình 151

Kiểm tra lại cấu hình.

Kết quả thu được (hình 152).

Anes Sector	MONITOR WLANE		SECURITY M	NANAGEMENT	COMMAN	Configuration	Ping Logout Refr
Controller General	Interfaces	VLAN Identifier	IP Address	Interface T	уре		New
Inventory	ap-manager	untagged	192.168.99.25	Static	Edit		
Interfaces	management	untagged	192.168.99.24	Static	Edit		
Internal DHCP Server	virtual	N/A	1.1.1.1	Static	Edit		
Mobility Management Mobility Groups Mobility Statistics	vian2	2	192.168.2.1	Dynamic	Edd	Retore	
Ports							
Aaster Controller Mode							
Network Time Protocol							
OnS Profiles							



- 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.

WLANS	WLANs > Edit			< Back Apply
WIANS				
WLANS AR Groups VI AN	WLAN SSID	< vlan2		
ar Groups your	General Policies		Security Policies	
	Radio Policy	All	Laver 2 Security	WPA
	Admin Status Session Timeout (secs)	Enabled		MAC Filtering
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None
	WMM Policy	Disabled 💌		Web Policy *
	7920 Phone Support	Client CAC Limit CAC Limit		
	Broadcast SSID	Enabled	B Web Colley analytic	a second in some bis states with 10 years
	Allow AAA Override	Enabled	and L2TP.	e used in combination with sysec
	Client Exclusion	Enabled ** 60	** When client exclus	ion is enabled, a timeout value of
	DHCP Server	Override	to reset excluded clie	ill require administrative override nts)
	DHCP Addr. Assignment	Required		
	Interface Name	vlan2		
	Radius Servers			
		Authentication Servers Accounting Servers		
	Server 1	IP:10.10.10.3, Port:1812 💌 none 💌		

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 192.168.2.254 255.255.0
```

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 \rightarrow New (hình 154).



Hình 154

LabPro Wireless

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

Chọn Apply (hình 156).

Security RADULS Authentication Servers > New Clock AA General RADUSS Accounting Local Net Uners Machine Schemel Machine Schemel Machin Schemel Machine Schemel Machine	And	MONITOR WLANS CONTR	OLLER WIRELESS SECURIT	Y MANAGEMENT COMMANDS	HELP
AA Server Index (Priority) 2 ■ Gerall Book Inter Users Duck Inter Users ACCESS Control Lists Bor Policies Brand Signatures Class Experies Brand AP Policies Brand Signatures Class Experies Brand Signatures Brand Signatures Class Experies Brand Signatures Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Brand Bran	Security	RADIUS Authentication Ser	vers > New		< Back
RADUS Audientication Server IPAddress 1010.0.3 Poue Radus Server RADUS Accounting Local Net Users Shared Secret Format ASCII • Diabled Clients Distriction Folicies Shared Secret Format ASCII • Carcess Control Lists Confirm Shared Secret ••••••• Wireless Protection Policies Confirm Shared Secret •••••• Trusted AP Policies Confirm Shared •••••• Stardard Sipnatures Clent Evolusion Policies Fort Number 1892 Clent Evolusion Policies Server Status Enabled • AP Authentication Support for RFC 3576 Enabled • Hinh 155 Security Retransmit Timeout 2 seconds Security RADUS Authentication Servers Sever Configuration Retree Index Retree Retree Security RADUS Authentikation Servers Apply Network Index Index Security Apply Network AA General R Policies Interes Protection Dise Lapp Policies R Marcellines List ALEB Reg Wrop Interes Interes Admin Status MAA General R Policies R Marcellines List AP Policies R Marcellines R Marcellines R Marcellines R Marcellines R Marellines R Marellines R Marcellines R Marcellines R Mare	AAA General	Server Index (Priority)	2 💌		
MAC Shared Secret Format ASCII * Disable Clears Shared Secret * ************************************	RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	10.10.10.3	P cus Radius Server	
AP Policies Shared Secret	MAC Filtering Disabled Clients User Login Policies	Shared Secret Format	ASCII 💌		
Access Control Lists Web Auth Certificate Wireless Protection Policies Regue Poli	AP Policies	Shared Secret			
Web Auth Certificate Secret Wireless Protection Regue Policies Key Wrop Trusted AP Policies Port Number Standard Signatures Clear Exclusion Policies Port Number Support for RFC 3576 Enabled V Retransmit Timeout 2 Seconds Network User Windless From User Enabled V AP Authentication Server Status Enable Seconds Network User Enable Montrok WLAus Control Signatures Control Control Control Clear Security RADUIS Authentication Servers AA Cell Station 10 Type General References Credentials Caching User Log Policies AP Policies Luse AES Key Wrop Wacht Certificate Vietwork Management Server Server Address Port Admin Status Wireless Protection Policies It 10:10:10:3 10:12 Enabled	Access Control Lists	Confirm Shared			1
Writess Protection Policies Standard Signatures Cleme Exclusion Policies AP Authentication Fort Number 1832 Standard Signatures Cleme Exclusion Policies AP Authentication Server Status Enabled Support for RFC 3576 Enabled Retransmit Timeout 2 Security MONITOR WLANS Control Lists MONITOR WLANS Security RADUIS Authentication PACUSS Accounting Control Lists Server Status Cell Station 1D Type IP Address Server Status Security Cell Station 1D Type IP Address AAA Ceses Control Lists Cedentials Caching List Light Times Server Server Address Port Admin Status Macriteria RADUIS Authentication Brobios AP Folicies Standard Signatures Control Status Interer's hanagement Server Server Server Address Port Admin Status Write List Protection Picicies Standard Signatures I 10.00.00.3 1932 Enabled	Web Auth Certificate	Secret			-
Regue Policies Standard Signatures Custom Signatures Custom Signatures AP Authentication Port Number 1812 Server Status Enabled AP Authentication Support for RFC 3576 Retransmit Timeout 2 2 seconds Network User Enabled Hinh 155 Bare Configuration Security MONITOR RADUS Authentication Server Status Security RADIUS Authentication Servers AA Cell Station 1D Type General RADUS Autoencides AP Notes Server Server Address Port AAC Credentials Caching Local Ket User Server Server Address Port Admin Status Wireless Protection Protection Trackd AP Policies Standard Signatures Contor Signatures	Policies Trusted AP Policies	Key Wrap			
Clent Exclusion Policies AP Authentication AP Authentication AP Authentication AP Authentication Retransmit Timeout E seconds Network User Enable Hinh 155 Control User Control VALANS CONTROLLER WIRELESS BECURITY MANAGEMENT COMMANOS HELD Security ANA General RADIUS Authentication Servers AC all Station ID Type IP Address ACCess Control Lists We Auth Certificate Wireless Protection Tracked AP Policies Applicities Tracked AP Policies Standard Signatures Control Signatures Standard Signatures	Rogue Policies Standard Signatures Custom Signatures	Port Number	1812		
Support for RFC 3576 Enabled Retransmit Timeout 2 seconds Network User Enable Hinh 155 Save Configuration Pring Logout Refre NONTOR WLAYS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANOS HELP Security RADIUS Authentication Servers Address Security Management Commanue Help Call Station ID Type IP Address AAA Call Station ID Type IP Address ACCESS Control Lists Web Auth Certificate Authentication Disciple Policies AP Policies Access Control Lists Web Auth Certificate Network Hanagement Server Address Port Admin Status Network Hanagement Server Server Address Port Admin Status	Client Exclusion Policies AP Authentication	Server Status	Enabled 💌		
Retransmit Timeout 2 Network User Enable Hinh 155 Rick Sense Save Configuration MONITOR WLANS Control MAN Security RADIUS Authentication Servers AAA Call Station ID Type General RADIUS Authentication Servers AAA Credentials Caching User Logn Neticies Use AES Key Wrop User Logn Neticies Network Nanagement Security Network Nanagement Security Network Nanagement Security Ise AES Key Wrop User Logn Neticies 1 Notes Protectione 1 Vieles Sprotectione 1 Sourd Signatures Enabled		Support for RFC 3576	Enabled 💌		
Network User Hinh 155 Arts Smart Security MONITOR MONITOR MANY Controller MONITOR MONITOR MANY Controller MONITOR MONITOR MANY Controller MONITOR MONITOR MANY Controller MONITOR MONITOR MILLING Security AAA General RADIUS Accounting Local Station ID Type P Address ACerestoria Accounting Local Net Users ACerestoria AP Policios AP Policios AP Policios Access Control Lists Web Auth Certificate Wireless Protection Disciel AP Policios Roppue Policies Roppue Policies Standard Staphaners Controller Standard Staphaners		Retransmit Timeout	2 seconds		
Hinh 155 Security Security Security Security MAN Call Station ID Type IP Address Security Manuel Station ID Type IP Address AAA Call Station ID Type IP Address IP Address Credentials Caching IP New Disabled Cleinsts Use AES Key Wrap III IIII IIIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Network User	Enable		
Security RADIUS Authentication Servers Apply AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies AP Policies Regue Policies Regue Policies Standard Signatures Call Station ID Type IP Address Vier Login Policies Regue Policies Standard Signatures Network Management Index Server Address Port Index Admin Status	Linco Berrina	MONITOR WLANS CONTROLLE	R WIRELESS SECURITY MAN		Fing Logout Refresh
AAA Call Station ID Type IP Address General RADIUS Authenbication RADIUS Authenbication Credentials Caching Local Net Users Use AES Key Wrap Disabled Clients Use AES Key Wrap Disabled Clients Use AES Key Wrap Access Control Lists Network Management Server Server Address Port Admin Status Wieless Protection I 10.10.10.3 1812 Enabled Edit Remoure Eing Policies Trusted AP Policies Standard Signatures Edit Remoure Eing Edit Remoure Eing	Security	RADIUS Authentication Servers		App	ly New
RADIUS Authentication Credentials Caching SADIUS Authentication Users MAC Filtering Use AES Key Wrop Disabled Clents User AES Key Wrop User Login Policies Network AP Policies Network Web Auth Certificate Image: Certificate Wireless Protection Image: Certificate Policies Image: Certificate Standard Signatures Certificate Custom Signatures Certificate	AAA General	Call Station ID Type IP Address	x		
Mac Use AES Key Wrap Disabled Clients Use AES Key Wrap Uier Login Policies Network Management Server Index AP Policies Network Management Index Web Auth Certificate Imagement Index Wireless Protection Policies 1 Policies 1 Standard Signatures	RADIUS Authentication RADIUS Accounting Local Net Users	Credentials Caching			
Access Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Custom Signatures	MAC Filtering Disabled Clients User Login Policies	Use AES Key Wrap 🔲			
Web Auth Certificate Image: 1 10.10.10.3 1812 Enabled Edst Remove Eina Wireless Protection Policies Trusted AP Policies Trusted AP Policies Standard Signatures Standard Signatures	AP Policies	User Management Index	Server Address Port	Admin Status	
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures	Web Auth Certificate		10.10.10.3 1812	Enabled Edit Remove I	Ping
AP Authentication	Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication				

Done

Hình 156

🙆 🔮 Internet

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).

A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	20	
VLANs	WLANs	-							N	ew
VLANS WLANS	WLAN ID	WLAN SSIE			Admin Status	Security Polici	es			
AP Groups VLAN	1	managemen	¢		Enabled	802.1X		Edit	Remove	Mobility Anchors
	2	vlan2			Enabled			Edit	Remove	Mobility
	* WLAN I	Ds 9-16 will n	ot be pushed to 1	130,1200 and 1	1240 AP model	e.				

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.

A ANK		ET a un d		Layer 2 Security	WPA 💌
il Ana	Admin Status	Enabled			MAC Filtering
LANS	Session Timeout (secs)	1800			and the second se
NP Groups VLAN	Quality of Service (QoS)	Silver (best effort)		Layer 3 Security	None Y
	WMM Policy	Disabled M			Web Policy *
	7920 Phone Support	Client CAC Limit	AP CAC Limit		
	Broadcast SSID	Enabled		* Wah Policy cannot	he used in combination with IPsec
	Allow AAA Override	Enabled	1.011	and L2TP.	of over in commission must be see
	Client Exclusion	Enabled ** 60		** When client exclusion	sion is enabled, a timeout value of
	DHCP Server	Timeou D Override	A Value (secs)	to reset excluded clie	vill require administrative override ints)
	DHCP Addr. Accimment	Remired			
	Interface Name	(ulas2			
	processore marine	Trance Call			
	Radius Servers				
	Radius Servers	Authentication Servers	Accounting		
	Radius Servers	Authentication Servers	Accounting Servers	>	
	Radius Servers Server 1	Authentication Servers	Accounting Servers	>	
	Radius Servers Server 1	Authentication Servers	Accounting Servers	>	
	Radius Servers Server 1 Server 2 Server 3	Authentication Servers	Accounting Servers	>	
	Radius Servers Server 1 Server 2 Server 3 WPA Parameters	Authentication Servers	Accounting Servers V none V V none V	>	
	Radius Servers Server 1 Server 2 Server 3 WPA Parameters 802.11 Data Encryption	Authentication Servers E031010.00.0.Postrass none TKIP-MIC	Accounting Servers	>	

Hình 158

Cấu hình trên ACS hỗ trợ xác thực bằng PEAP.

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



Hình 160

Nhập Username: cisco (hình 161).

CiscoSecure ACS - I	Mozilla Firefox	
	tory gookmans toos help	∽ · G• Google
CISCO SYSTEMS	llser Setun	
Userp Setup Setup Setup Components Setup Components Setup Ret york Outputton Setup Interface Control Setup Interface Control Setup Setup Control Setup	User: cisco Find Add/Edit List users beginning with letter/number: <u>A B C D E F C H I J K L H</u> <u>N O F Q B S T U V V X Y Z</u> <u>O I 2 3 1 5 6 7 8 9</u> List all users Remove Dynamic Users Back to Help	 User Setup and External User Databases Finding a Specific User in the ACS Internal Database Using User to the ACS Internal Database Database Internal Database Using User Database Internal Database Database Internal Database Databases In
		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 dick Find. From the list of usernames displayed, dick the username whose information you want to view or change
Nhập Pa CiscoSecure ACS -	Issword: cisco123 → chọn submit (Mazilla Firefox	(hình 162).
	Story Bootmans Tools Tep http://127.0.0.1:1049/ 1	√ • G• Google
CISCO SYSTEMS	User Setup	X
User Setup Setup Setup Setup Setup Compounds Confouration Confouration Wetwork Network Suffiguration Confoura		Help • Account Disabled • Debting a Username • Debting a Username • Debting a Username • Debting a Username • Call and the User is assigned • Dependent Access is built from the User is account • Call and the User is account • Call and the User is account • Call and the Access is for the User is account • Call and the Access is for the User is account • Call and the Access is for the User is account • Call and the Access is for the account. • Call and the Access is the User is account • Call and the Access is the User is account.

Hình 162

😻 CiscoSecure ACS - Mozilla Firefox <u>- 8 ×</u> Eile Edit View History Bookmarks Iools Help ☆・ Google 🔇 🔊 - C 🗶 🏠 📄 http://127.0.0.1:1049/ × CISCO SYSTEMS **Network Configuration**Illin. ..միհ Frlit User Setup AAA Client Hostname AAA Client IP Address Network Device Group Group | Group **Add AAA Client** Authenticate Using Single Connect TACACS+ AAA Client Log Update/Watchdog Packets from Shared Profile Components og Update/Watchdog Packets og RADIUS Tunneling Packets teplace RADIUS Port info with from this AAA Client AAA Client WLC Network Configuration Hostname 192.168.99.24 System Configuration AAA Client AAA Client Hostname IP Address Interface Configuratio The AAA Client Hostname is the name assigned to the AAA client. Administrat Kev cisco [Back to Top] 🙀 | External User Databases AAA Client IP Address Authenticate RADIUS (Cisco Aironet) -BBBB Posture Validation The AAA Client IP Address is the IP address assigned to the AAA client. \square Single Connect TACACS+ AAA Client (Record stop in accounting on failure). 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**. Network Acce □ Log Update/Watchdog Packets from this AAA Client Reports and Activity 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. Class C network to be represented by a single AAA client entry, enter 192:168:13.* in the AAA Client IP Address box. Documentatio \square Log RADIUS Tunneling Packets from this AAA Client $\hfill\square$ Replace RADIUS Port info with Username from this AAA Client 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 diant lentry, enter 192.168.13.12-221 in the Adlent IP Address box. Submit Submit + Apply Cancel [Back to Top] Hình 163 Chọn Submit + Apply và xem kết quả (hình 164). 😂 CiscoSecure ACS - Mozilla Firefox - 8 × Edit View History Bookmarks ☆ • 💽 • Google C X 🏠 http://127.0.0.1:1049/ × CISCO SYSTEMS **Network Configuration** ավիս ...dh. Select User Setup **%**Q AAA Clients ? Group | Group AAA Client IP AAA Client Authenticate Shared P Compone Address Hostname Using Network Configuration RADIUS (Cisco router 10.10.10.1 Airespace) System Configuration RADIUS (Cisco <u>WLC</u> 192.168.99.24 Aironet) Configuration Administrati Add Entry Search Databases Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you dick 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 stable. Bana Posture Validation **%**0 ? AAA Servers Network Acces AAA Server AAA Server IP AAA Server Address Name Type Reports and Activity CiscoSecure c0109 127.0.0.1 Network Device Groups ACS Documenta 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 creats. AAA diants and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG. Add Entry Search To view the AAA Client and AAA Servers tables for a particular NDG, click the name of the NDG. Proxy Distribution Table ? [Back to Top] Character String AAA Servers Strip Account

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

Hình 164

No Local

(Default)

c0109

Adding a Network Device Group

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).

	A 15
→→ C × 🔬 🗋 http://127.0.0.1:1868/	は、・ Google
1ost Visited 🌪 Getting Started 🔝 Latest Headlines	
disco System Configuration	
Select	
 Service Control Logging Date Format Control Local Password Management ACS Internal Database Replication ACS Restore ACS Restore ACS Service Management ACS Certificate Setup Slobal Authentication Setup Back to Help 	Service Control Longing Pate Format Control Control Control Control Control Control Control Service Control Service Control Service Control Service Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. IBack to Top

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

SiscoSecure ACS - Mozilla Firefox	
Eile Edit View Higtory Bookmarks Iools Help	
C 🗙 🕜 🚺 http://127.0.0.1:1868/	රු · Google 🔎
🖻 Most Visited 🐢 Getting Started 🔝 Latest Headlines	
CISCO STSTEMS and the metalline System Configuration Select	×
	 Install ACS Certificate AcS Certificate Install Acts Edit Certificate Install Acts Edit Certificate Install Acts Edit Certificate Signal Request Cenerate Certificate Signal Request Cenerate Certificate Signal Request Cenerate Certificate Signal Certificate Install ACS Certificate Select to install a certificate from Windows certificate storage or from a file. Back to Top] ACS Certificates Inst. Back to Top] Edit Certificate Number of Certificate into the ACS CA certificates ist. Back to Top] Edit Certificate Number of the Certificate suborties (CAs) Acts of the sub-third bind party certificate suborties (CAs) Acts out by which sub-third bind guest with from a CA that you have and subortification guest with from a CA that you have and subortification acts output of ACS to trust. Back to Top] Back to Top] Back to Top]

Hình 166

- 8 × 😂 CiscoSecure ACS - Mozilla Firefox Eile Edit View History Bookmarks Tools Help ☆・ G• Google 🔇 🔊 - 😋 🗶 🏠 📘 http://127.0.0.1:3752/ × Cisco Systems System Configuration ath alh Edit Generate Self-Signed Certificate 🛛 📑 🛛 User Setup Certificate subject Certificate file Private key file Private key password Retype private key password Key length Digest to sign with Install generated certificate Group Setup Generate new self-signed certificate ? Shared Profile Components cn=cisco Certificate subject Network Configuration Certificate file c:\cisco.cer Use this page to generate a self-signed certificate. You have the option of having ACS automatically install the certificate when you submit the certificate generation request. When you time you generate a self-signed certificate, the certificate and private key files are written to the file system in the locations you specify. You can copy these files to other ACSs for use as server certificates and to end-user clients for use as server certificates and to end-user clients for use as certification automytic certificates so that the end-user client interface using HTTPS, you can also import the certificate into local storage on computers that run web browsers for access to ACS. System Configuration Private key file c:\cisco.pvk Private key password Configuration Retype private key password Administration ****** Key length 2048 bits 💌 💏 | External User Databases Digest to sign with SHA1 💌 BBBB Posture Validation Install generated certificate 🗵 Network Acces: Profiles Certificate subject 💡 🛛 Back to Help Type the subject for the certificate, prefixed with "cn=". We recommend using the ACS server name. For example, "cn=ACS11". Reports and Activity Documentation [Back to Top] Certificate file Type the full path and file name for the certificate file that you want to generate. For example, "cilacs_server_cert (acs_erver_cert.cer". When you submit this page, ACS creates the certificate file using the location and file name you specify. [Back to Top] Submit Cancel Hình 167 Xuất hiện thông báo sau (hình 168) 💛 CiscoSecure ACS - Mozilla Firefox _ 8 × View History Book narks <u>T</u>ools <u>H</u>elp Edit < 🔊 - 😋 💥 🏠 📑 http://127.0.0.1:3752/ ☆ • 🖸 Google \$ × CISCO SYSTEMS System Configuration alli. Select Install ACS Certificate ACS Certification Authority Setup Edit Certificate Trust List Certificate Revocation Liste Generate Certificate Signing Request Generate Self-Signed Certificate User Setup **ACS Certificate Setup** Group | Group 📧 Install ACS Certificate Shared Profile Components Z ACS Certification Authority Setup Network Configuration Edit Certificate Trust List Install ACS Certificate Certificate Revocation Lists System Configuration Select to install a certificate from Windows certificate storage or from a file. 🛛 Generate Certificate Signing Request Configuration Generate Self-Signed Certificate [Back to Top] Maministratic ACS Certification Authority Setup The current configuration has been Select to add a third-party CA certificate into the ACS CA certificates list. changed. Restart ACS in "System Databases Configuration:Service Control" to [Back to Top] Posture Validation adopt the new settings for EAP-TLS Edit Certificate Trust List Profiles or PEAP support only. You can specify which third-party certificate authorities (CAs) ACS should trust when authenticating users with carificate-based protocol. If a user's carificate is from a CA that you have not specifically configured ACS to trust, authentication fails. Reports and Activity Cancel Docume [Back to Top] 💡 Back to Help Certificate Revocation Lists You can configure ACS to retrieve certificate revocation lists (CRLs) from CAs that are enabled on the Certificate Trust List. [Back to Top] Generate Certificate Signing Request

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

Hình 168



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

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).



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).

Certificate Info	rmation		
This CA Root certificat install this certificate i Authorities store.	e is not trusted. To e in the Trusted Root C	nable trust, ertification	
Issued to: cisco			-
Issued by: cisco			
Valid from 7/30/20	009 to 7/30/2010		
(Install Certificate) Issuer Statem	ent

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

etwork Tasks	🞍 Wireless Network Connection Properties 👘 🔗 🔀	
Refresh network list	General Wireless Networks Advanced	ange or to get more
Set up a wireless net for a home or small of	Use Windows to configure my wireless network settings	Validating identity 🔮
elated Tasks	To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.	6000
Learn about wireless	View Wireless Networks	008e
Change the order of preferred networks	Preferred networks: Automatically connect to available networks in the order listed below:	006e
Change advanced settings	VCw_PROLINK (Automatic) Innotel-Branch-02 (Automatic) Move down	
	Add Remove Properties	
	Learn about setting up wireless network Advanced	

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.

Association	Authentication	Connection
Network na	ame (SSID):	vlan2
Wireless	network key	
This netv	vork requires a ke	ey for the following:
Network	Authentication:	WPA
Data en	cryption:	ТКІР
Network	key:	
Confirm r	network key:	
Key inde	x (advanced);	1
☑ The k	cey is provided fo	r me automatically
This is access	a computer-to-cor points are not us	mputer (ad hoc) network; wireless ed

DAOTAO CHUYÊN GIA Hình 175 TRI MANG QUỐC TẾ

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).

Association	Authentication	Connection
Select this wireless Eth	option to provide hernet networks.	authenticated network access for
<u> </u>	IEEE 802.1x aut	nentication for this network
EAP type	Protected EAP	(PEAP)
C	Smart Card or o	ther Certificate
	icate as compute	ar when computer information is available
Addient	icale as <u>c</u> ompute	
Authent unavaila	icate as guest wi able	hen user or computer information is

DAOTAO CHUYEN GIA Hình 176

LabPro Wireless

Protected EAP Properties	? 🗙
When connecting: Validate server certificate Connect to these servers:	
Trusted Root Certification Authorities:	
Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4 Certisign Autoridade Certificadora AC15 Certisign Autoridade Certificadora AC35 certisign Autoridade Certificadora AC35 cisco	
Do not grompt user to authorize new servers or trusted certification authorities.	
Select Authentication Method:	
Secured password (EAP-MSCHAP v2)	re
Enable Fast Reconnect	cel

Hình 177

	(interest (interest)	
	S	50
User name:	vnpro	
User name: Password:	vnpro •••••	
User name: Password: Logon domain:	vnpro	

Hình 178

LabPro Wireless

