LAB 6: Xác thực dot1x dùng kiểu FAST

Mô tả

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

Sơ đồ



Hình 100

Thực hiện

Cấu hình cơ bản trên router:

```
C2811#sh run
Building configuration...
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c2811
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
enable secret 5 $1$QgGG$mjteEFA5x1onr2X3kuDp50
!
aaa session-id common
L
!
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
1
interface FastEthernet0/0
ip address 10.10.10.1 255.255.255.0
duplex auto
 speed auto
1
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
1
interface Serial0/0/1
no ip address
shutdown
clock rate 2000000
!
interface wlan-controller1/0
no ip addresss
shutdown
!
!
control-plane
!
line con 0
!
scheduler allocate 20000 1000
!
End
```

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

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

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

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

Truy cập vào WLC module từ Router 2811. c2811#service-module wlan-controller 1/0 session

```
Trying 192.168.99.254, 2066 ... Open
```

Cấu hình WLC từ chế độ SETUP MODE như hình 101.

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

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

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

Trying 192.168.99.254, 2066 ... Open

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

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

C2811#conf t

C2811(config)#ntp master 2

Cisco Controller

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup System Name [Cisco ff:f6:a0]: NMWLC Enter Administrative User Name (24 characters max): cisco Enter Administrative Password (24 characters max): cisco Management Interface IP Address: 192.168.99.24 Management Interface Netmask: 255.255.255.0 Management Interface Default Router: 192.168.99.254 Management Interface VLAN Identifier (0 = untagged): 0 Management Interface Port Num [1]: 1 Management Interface DHCP Server IP Address: 192.168.99.24 AP Manager Interface IP Address: 192.168.99.25 AP-Manager is on Management subnet, using same values AP Manager Interface DHCP Server (192.168.99.24): 192.168.99.24 Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: mg1 Network Name (SSID): 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 101

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

	Cisco Controller			
	User name:	🖸 cisco	~	
Wireless LAN Contr	Password:	•••••	d	
				Logir
		ОК	Cancel	

Hình 102

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

Cinco Stattung							Save Co	nfiguration A	Ping Logout Refresh	
A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Controller	General								Apply	
General	802.3x Flo	ow Contro	ol Mode	Disabled 💌						
Interfaces	LWAPP Transport Mode			Layer 3 🛩 (Current Operating Mode is Layer3)						
Internal DHCP Server Mobility Management	Ethernet Multicast Mode			Disabled 💌	bled v					
Mobility Groups Mobility Statistics	Aggressiv	e Load B	alancing	Enabled 💌						
Ports Master Controller Mode	Peer to Pe	er Blocki	ng Mode	Disabled 💌						
Network Time Protocol	Over The	Air Provis	ioning of AP	Enabled 💌						
Qu's Promes	AP Fallbac	*		Enabled 💌						
	Fast SSID	change		Disabled 💌						
	Default Me	obility Do	main Name	mg1						
	RF-Netwo	rk Name		mg1						
	User Idle	Timeout ((seconds)	300						
	ARP Times	out (seco	nds)	300						
	Web Radio	is Auther	ntication	PAP 💌						
https://192.168.99.24/screens/b	ase/ntpserver_lis	t.html						۵	Internet	

Hình 103

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



Hình 105

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

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

🗿 Cisco - Microsoft Internet I	Explorer						E 🗗 🔀
File Edit View Favorites To	ools Help						
🔇 Back 🔹 🕥 - 💌 🙎	👔 🏠 🔎 Search 👷 Favorit	es 🚱 🔗 🌺 🛙	- 🛄 🛍	28			
Address 1/192.168.99.24	screens/frameset.html					~	🔁 Go Links 🎽
Cisco Systems	MONITOR WLANS CONT		SECURITY M	ANAGEMENT COM	Save Configurat IMANDS HELF	tion Ping)	Logout Refresh
Wireless	All APs	\sim					
Access Points All APs 802.11a Radios	Search by Ethernet MAC		Search				
Bridging	AP Name	AP ID Et	hernet MAC	Admin Status	Operational Status	Port	
Rogues Rogue APs Known Rogue APs Rogue Clients	AP001d.a27f.a562	3 00	:1d:a2:7f:a5:62	Enable	REG	1	Detail
Adhoc Rogues							
Clients Global RF 802.11a Network 802.11b/g Network 802.11h							
Country							
Timers							
		Hình	106.				
Cấu hình cá	ia thông cấ aha	Winalaga Cl	iont (lain	h 107)			
Cau ninn ca	ac thong so cho	wireless CI	ient (nin	n 107).			
Chan C	mtuollon > Int	-					
- Chọn Cơ	ontroller > Inte	erfaces > ne	ew.				
Casta Statem					Save Configuration	ons Ping 1	Logout Refresh
A.A.	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY M	NAGEMENT COM	MANDS HELP		
Controller	Interfaces						New
General	Interface Name	VIAN Identifier	IP Address	Interface Type			
Inventory	ap-manager	untegged	192.168.99.25	Static	Edit		
Interfaces	management	untagged	192.168.99.24	Static	Edt		
Internal DHCP Server	virtual	N/A	1.1.1.1	Static	Edit		
Mobility Management Mobility Groups Mobility Statistics							
Ports							
Master Controller Mode							
Network Time Protocol							

Hình 107

QoS Profiles

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

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

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

Cases Statutes						Save Co	ofiguration Pin	g Logout i Refresh		
h h	MONITOR WEARS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Controller	Interfaces > Edit						< liack	Apply		
General	General Information	n								
Inventory Interfaces	Interface Name	vlan2		10						
Internal DHCP Server	Interface Address									
Mobility Management Mobility Groups	VLAN Identifier	2	12	_						
Ports	IP Address	192.	168.2.1	dia chi cua	AP giao tiep voi cac v	vireless client				
Master Controller Mode	Netmask	255.	255.255.0	ip nay da	at cho sub int wian-cor	nbroi bren router				
Network Time Protocol QoS Profiles	Gateway	192.	168.2.254	client						
	Physical Informatio	n								
	Port Number 1									
	DHCP Information									
	Primary DHCP Server	192.	168.100.1	dia c	IN CUB DHCP (Rouber2)	k8 phaitoi dic CHICI	0			
	secondary once serv	0.0.1								
	Access Control List	Free								
	Note: Changing the Inter	face parameters	causes the WL	ANs to be						
	temporarily disabled and some clients.	thus may result	in loss of conne	ectivity for						
Date							A	Internet		
Ket qua tin	u duộc (mim	109).				Save Co	onfiguration Pic	ng Logout Refres		
A.A.	MONITOR WLANE	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Controller	Interfaces		Q					New		
preserve and a second s										
General	Interface Name	¥L.	AN Identifier	IP Address	Interface	Туре				
Inventory	ap-manager	unt	agged	192.168.99.2	25 Static	Edit				
Interfaces	management	unt	agged	192.168.99.3	24 Static	103				
Internal DHCP Server	virtual	N/3	k	1.1.1.1	Static	Edit				
Mobility Management Mobility Groups	vian2	2		192.168.2.1	Dynamic	Edd Ed	BX SCO			
Mobility Statistics							10			
Ports										
Master Controller Mode										
Network Time Protocol										
QoS Profiles										

- 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 110).

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

Cines Systems	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY	Save Co MANAGEMENT COMMANDS	vliguration Ping Logout Refre HELP				
WLANs	WLANs > Edit			< Back Apply				
WLANS WLANS	WLAN ID	2						
AP Groups VLAN	General Policies	vianz	Security Policies					
	Radio Policy Admin Status	All	Layer 2 Security	WPA				
	Session Timeout (secs)	1800		MAC Filtering				
	WMM Policy	Disabled	Layer 3 Security	Web Policy *				
	7920 Phone Support Broadcast SSID	Enabled	* Web Policy cannot b	e used in combination with IPsec				
	Allow AAA Override Client Exclusion	Enabled ** 60	and L2TP. ** When client exclus	and L2TP. ** When client exclusion is enabled, a timeout value of targe means infinity/will convice administrative override				
	DHCP Server DHCP Addr. Assignment	Override	to reset excluded clier	its)				
	Interface Name	vlan2						
	Radius Servers							
		Authentication Servers Accounting Servers						
	Server 1	IP:10.10.10.3, Port:1812 V none V						
Done				🔒 💣 Internet				

ĐÀO TẠO CHUYỆN GIẢ CHUYỆN GIẢ

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

```
R1(config)# interface wlan-controller1/0.2
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip address 192.168.2.254 255.255.0
```

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.

Chon Security \rightarrow New (hình 111).

Cinca Searcas			-		Save Configuration Ping Logout		
MONITOR WI	LANS CONTROLLER	WIRELESS	ECURITY	MANAGEMENT	COMMANDS	HELP	
Security RADIUS Auth	entication Servers					Apply	New
AAA Call Station I General RADBIS Authentication	D Type IP Address	*					
RADIUS Accounting Credentials C Local Net Users	Caching 🔲						
MAC Filtering Use AES Key Disabled Clients User Login Policies	Wrap						
AP Policies Network Man	agement Server	Server Address	Port	Admin	itatus		
Access Control Lists							
Web Auth Certificate							
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication							

Hình 111

LabPro Wireless

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

Cases Systems	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY	Save Co MANAGEMENT COMMANDS	nfiguration Ping Logo HELP
Security	RADIUS Authentication Ser	vers > New		< Back A
AAA General	Server Index (Priority)	2 💌		
RADIUS Authentication RADIUS Accounting Local Net Users	Server IPAddress	10.10.10.3	Picua Radius Server	
MAC Filtering Disabled Clients	Shared Secret Format	ASCII 💌		
User Login Policies AP Policies	Shared Secret			
Access Control Lists	Confirm Shared	Francisco		-
Web Auth Certificate	Secret	•••••		
Wireless Protection Policies	Key Wrap			
Rogue Policies Standard Signatures	Port Number	1812		
Custom Signatures Client Exclusion Policies AP Authentication	Server Status	Enabled 💌		
	Support for RFC 3576	Enabled 💌		
	Retransmit Timeout	2 seconds		
	Network User	Enable		

Hình 112

Chọn Apply (hình 113).

Einen Serren	MONITOR	WANS O		WIRELESS S	ECURITY	MANAGEMENT	Save Co	nfiguration P	ing Logout Refres
Security AAA General RADIUS Authenbication RADIUS Authenbication RADIUS Authenbication MAC Filtering Disabled Clients User Login Policies AP Policies AP Policies AP Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Client Exclusion Policies AP Authentication	RADIUS / Call Stati Credenti Use AES Network User	WLAS C Authentikation on ID Type als Caching Key Wrap Management	n Servers	Server Address	Port 1812	Admin t	itatus Edit	Remove Ping	New
Done								۵ (🕽 Internet

Hình 113

Cấu hình xác thực FAST.

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

	MONITO	R WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Save Co COMMANDS	HELP	Fing Lo	gout Ref
VLANs	WLANS	a							N	ew
WLANS WLANS AP Groups VLAN	WLAN ID	WLAN SSID			Admin Status	Security Polici	es			
	1	managemen	¢		Enabled	802.1X		Edd	Semove	Mobility Anchors
	2	vlan2			Enabled			Edit	Remove	Mobility Anchors
	* WLAN I	10s \$-16 will n	ot be pushed to 1	1130,1200 and	1240 AP model					

Hình 114

Chọn 802.1X trong phần Layer 2 security (hình 115). Trong phần server1 chọn 10.10.10.3 (hình 116).

🔏 Cisco - Windows Internet	Explorer		<u>_ 문 ×</u>
🕞 🗢 💌 https://192.	168.99.24/screens/frameset.html	🗾 😵 Certi	tificate Error 🛛 🔄 🍾 🕒 Bing 🖉 🖓
Eile Edit View Favorites	Tools Help 🛛 🗙 🐑 -		
🖕 Favorites 🛛 🚖 🏉 Sug	ggested Sites 🝷 🙋 Free Hotmail 🙋	My Yahoo! 🙋 WebLH1 🙋 WebLH2 🙋 Y	Yahoo! 🩋 Yahoo! Bookmarks 🤌 Yahoo! Mail 🧶 Web Slice Gallery 🔹
Cisco			🐴 • 🔝 - 🖃 🖶 • Page • Safety • Tools • 🕢 •
CISCO SYSTEMS			Save Configuration Ping Logout Refresh
	MONITOR WLANS CO	ONTROLLER WIRELESS SECURIT	TY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit		< Back Apply
WLANS	WI AN TO	2	
WLANs AR Groups MLAN	WLAN SSID	vlan2	
AP Groups VLAN			
	General Policies		Security Policies
	Radio Policy	All	laver 2 Security 802.1X
	Admin Status	Enabled	
	Session Timeout (secs)	1800	
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security None
	WMM Policy	Disabled 💌	Web Policy *
	7920 Phone Support	Client CAC Limit 🛛 AP CAC Lim	nit
	Broadcast SSID	Enabled	
	Allow AAA Override	Enabled	* Web Policy cannot be used in combination with IPsec and L2TP.
	Client Exclusion	Enabled ** 60	** When client exclusion is enabled, a timeout value of
	DHCP Server		to reset excluded clients)
	DHCP Addr. Assignment	Required	
	Interface Name	vlan2	
	Radius Servers		
		Authentication Servers Account Servers	ting s
Done	Concert .	WI W	
Durie			 Internet ₹ _ 100% ★

Hình 115

LabPro Wireless

Cisco - Windows Internet Exp	lorer			
🕒 🗢 🖉 https://192.168.	99.24/screens/frameset.html	🗾 😵 Certificate Error	🗟 😽 🗙 🔁 Bing	P -
	Tools Help 🛛 🗙 🐑 🗸			
🔶 Favorites 🛛 🚖 🏉 Sugges	sted Sites 👻 🙋 Free Hotmail 💋	My Yahoo! 🙋 WebLH1 🙋 WebLH2 🏉 Yahoo! 🥑 Yaho	oo! Bookmarks 🛯 🙋 Yahoo! Mail	💋 Web Slice Gallery 👻
Cisco			🔄 🗄 • 🗟 • 🛋 🖶	• Page • Safety • Tools • 🕢 • »
CISCO SYSTEMS			Save Confi	guration Ping Logout Refresh
	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY MANAGE	EMENT COMMANDS I	HELP
WLANs	Admin Status	✓ Enabled		MAC Filtering
	Session Timeout (secs)	1800		
WLANS WLANS	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None
AP Groups VLAN	WMM Policy	Disabled 💌		Web Policy *
	7920 Phone Support	Client CAC Limit CAP CAC Limit		
	Broadcast SSID	Enabled	* Web Policy cannot be	used in combination with IPsec
	Allow AAA Override	Enabled	and L2TP.	
	Client Exclusion	Enabled ** 60 Timeout Value (secs)	** When client exclusion zero means infinity(will	n is enabled, a timeout value of require administrative override
	DHCP Server	🗖 Override	to reset excluded clients	5)
	DHCP Addr. Assignment	Required		
	Interface Name	vlan2 💌		
	Radius Servers			
		Authentication Servers Accounting Servers		
	Server 1	IP:10.10.10.3, Port:1812		
	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 116

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

Quan sát kết quả (hình 117).

Cisco - Windows Internet Ex	plorer									_ 8 ×
📀 🗢 💌 https://192.168	8.99.24/screer	s/frameset.html			💌 😵 Certifica	te Error 🛛 🗟 😽	🗙 🗔 Bing			P -
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	Tools Help] × 🕲	*							
🖌 🙀 Favorites 🛛 🚖 🏈 Sugge	ested Sites 👻	🧉 Free Hotmai	🙋 My Yahoo! 🧧	WebLH1 🥭 V	VebLH2 🙋 Yaho	oo! 🙋 Yahoo! Book	marks 🙋 Yahoo! Mail 🍦	🦲 Web Slice	e Gallery 🔻	
6 Cisco			1]	🏠 • 🗟 • 🖃 🌧 •	• <u>P</u> age •	Safety -	T <u>o</u> ols • 🔞 • "
CISCO SYSTEMS								uration F	Ping Lo	gout Refresh
	MONITOR	R WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS HE	ELP		
WLANs	WLANs								N	ew
WLANs WLANs	WLAN ID	WLAN SSID			Admin Status	Security Polic	ies			
AP Groups VLAN	1	managemen	t		Enabled	802.1X		Edit	Remove	Mobility Anchors
	2	vlan2			Enabled	802.1X		Edit	Remove	Mobility Anchors
	* WLAN I	Ds 9-16 will n	ot be pushed to 1	.130,1200 and	1240 AP model	ls.				

Hình 117

Cấu hình trên ACS hỗ trợ xác thực bằng FAST.

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



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

< >- C ×	☆ http://127.0.0.1:1049/	☆ - Google
CISCO SYSTEMS	User Setup	
ամինուսմինու	Select	
Sery Sery	User: Find Add/Edit List users beginning with letter/number: A B C P D F C C H I J K L M N C P D R S T U V W K Y Z O 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 Databases Adding a User to the ACS Internal Databases Adding a User to the ACS Internal Databases Changing a Username in the ACS Internal Databases The Stup and Username in the ACS Internal Databases The Stup and Username in the ACS Internal Databases The Stup and Username in the ACS Internal Databases Second Databases Defore ACS can authenticate users with an external user database You must have the database up and running on the external server as the total second provide on the ACS internal Databases up and unuing on the external server be running and properly configured. You must have configured the applicable parameters in the Extern User Databases section. Note: User Setup configured to a varies in the ACS Internal Idatabase in a external user database. User a database is users for added security, authorization, a accounting purposes, User Setup keeps track of users who authenticate in a external user database is the Set of users who authenticate is an external user database. External user databases is track for users who authenticate and is external user databases. External user databases is track of users who authenticates in the ACS internal User Setup lets you on authenticate who authenticate
		[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 letters of the username in the User field, add an asterisk (*) as
		wildcard, and click Find. From the list of usernames displayed, clic
ôn I Jaart	etup.exe?action=make_r_fs8option=users8nav_seq=3 Hình 119	Widesro, and elice Hind , from the list of Userhames alphayed, elic the unername whore information way want to way or channel
âp Useri	etup.exe?action=make_r_fs8option=users8nav_seq=3 Hình 119 name: cisco (hình 120). -Mozilla Hirefox Higory Bookmarks Iools Help	Wideard, and click Hild , From the list of Userhames displayed, clic the unerosome whose information way and to view or obsore
âp Useri CiscoSecure ACS Ele Edt Yew C > C >	etup.exe?action=make_r_fs8option=users8nav_seq=3 Hinh 119 name: cisco (hinh 120). - Mozilla Firefox Higtory Bookmarks Tools Help	Widedro, and elick Hind, From the list or Userhame's diplayée, di the unerowne whore information was to view or channe.
âp Useri CiscoSecure ACS Ele Edt View Cisco System du du	Hinh 119 Hame: cisco (hinh 120). Mozilia Firefox Higory Bookmarks Tools Help Description: Description: Market State User Setup	Madard, and elick Hind , from the list or Userhame's displayee, die the unerowne where information wave barries or channe.
âp Userr CiscoSecure ACS Ele Edk ⊻Jew Cisco Status Cisco Status unilinuumilinu.	estup.exe?action=make_r_fs8option=users8nav_seq=3 Hinh 119 name: cisco (hinh 120). - Mozilla Firefox Higory Bookmarks Tools Help Comparison Tools Help User Setup Select	Middard, and click filled, from the list of userhames displayee, clic the unername whole information was the list of click and the unername whole information was the list of
âp Useri âp Useri CiscoSecure ACS Ele Edt Yew CiscoStruttin CiscoStruttin Strup Ele Edt Yew CiscoStruttin Strup Strup Strup Strup Strup CiscoStruttin CiscoStruttin CiscoStrup Strup Strup CiscoStruttin CiscoStrup Strup Strup CiscoStrup Strup Strup CiscoStrup Strup Strup Strup CiscoStrup Strup	Estup.exe?action=make_r_fs8option=users8nav_seq=3 Hinh 119 name: cisco (hinh 120). • Mozilla Firefox •	 Under Sature and External User Databases Ending a Specific User in the ACS Internal Database Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a Specific User in the ACS Internal Databases Ending a User Databases in the ACS Internal Databases Ending a User Database in the ACS Internal Databases Ending a User Databases up and running on the external server for example, if you are using to the polyholic polymenters in the External User Databases section. Note: User Setup configuration overrides Group Setup configuration Ending Databases section.



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

Hình 122

coSecure ACS - Mozilla Firef <u>- 8 ×</u> < 🔊 - C 🗙 🏠 📄 http://127.0.0.1:1049/ ☆ • 🖸 • Google ۶ ISCO SYSTEMS Network Configuration Select User Setup **%**Q AAA Clients ? Group Setup AAA Client Hostname AAA Client IP Authenticate Shared Profile Components Using Address Network Configuratio RADIUS (Cisco router 10.10.10.1 Airespace) System Configuratio RADIUS (Cisco Aironet) <u>WLC</u> 192.168.99.24 Interface Configuratio Maministrat Add Entry Search Di External | Databases This page changes depending your interface ration. If you are using Network Device Groups (NDGs), so ulck Network Configuration in the navigation bar, e Network Device Groups table and Proxy Distribution nformation appear. If you are not using NDGs, the AAA table and the AAA Servers table appear in place of the C Device Groups table. **%**Q BBBB Posture Validation ? AAA Servers Network Acce AAA Server AAA Server IP AAA Server Name Address Туре Seports and Activity CiscoSecure c0109 127.0.0.1 Network Device Groups ACS Documentati Network device groups are collections of AAA dients and AAA servers. You can assign AAA dients and AAA servers to the network device groups you create. AAA dients and AAA servers not assigned to a particular HDG 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 Adding a Network Device Group No Local (Default) c0109

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

Hình 123

Khai báo kiểu xác thực FAST trên ACS.

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

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



Hình 124

Chon Generate Self-Signed Certificate (hình 125).

🕲 CiscoSecure AC5 - M	ozilla Firefox	
Elle Edit View Higto	ry Bookmarks Tools Help	
Contraction Contraction	http://127.0.0.1:1868/	ରେ • 🖸 Google 🎤
🙋 Most Visited 🏾 P Getti	ng Started 🔊 Latest Headlines	
CISCO SYSTEMS	System Configuration	×
illinillin	Select	
User Setup	ACS Certificate Setup	Install ACS Certificate ACS Certification Authority Setup
Group Setup	Aco continuite octup	Edit Certificate Trust List Certificate Revocation Lists
Shared Profile	Install ACS Certificate	<u>Generate Certificate Signing Request</u> <u>Generate Self-Signed Certificate</u>
Network	ACS Certification Authority Setup Edit Certificate Trust List	
Configuration	Certificate Revocation Lists	Install ACS Certificate
Configuration	Generate Certificate Signing Request	Select to install a certificate from Windows certificate storage or from a file.
Configuration	Generate Self-Signed Certificate	[Back to Top]
Administration Control	Cancel	ACS Certification Authority Setup
External User		Select to add a third-party CA certificate into the ACS CA certificates list.
Dannell Posture	Pack to Help	[Back to Top]
Comm Validation		Edit Certificate Trust List
Profiles		You can specify which third-party certificate authorities (CAs)
Reports and Activity		ACS should trust when authenticating users with certificate-based protocol. If a user's certificate is from a CA that you have not specifically configured ACS to twict
Documentation		authentication fails.
		[Back to Top]
		Certificate Revocation Lists
		You can configure ACS to retrieve certificate revocation lists (CRLs) from CAs that are enabled on the Certificate Trust
		List
http://127.0.0.1:1868/set	up.exe?action=make_rb_fs&option=certificateGenerationInterface_paintRBFrameset	Back to Tool
🍠 Start 🛛 🞯 🥌 💋	* 🔤 E:\WINDOWS\syste 🔁 G:\ 🔤 document.doc - Micr	🕑 CiscoSecure ACS 🦉 4.3PG - Paint 🛛 🛃 😒 🛒 🌒 6:28 AM
File Edit View Hist	rozma Firelox	
<>- C ×	↑ http://127.0.0.1:3752/	Cr ⋅ Google
Cieco Sverene		X
	System Configuration	
adiiiiinaadiiiiina -	Edit	· · · ·
	Concrete Salf Signed Cortificate	
Setup	Generate Sen-Signed Certificate	<u>Certificate subject</u> Certificate file
Group Setup		Private key file Private key password
Shared Profile	Generate new self-signed certificate	Retype private key password Key length
Network	Certificate subject cn=cisco	Install generated certificate
Configuration	Certificate file c:\cisco.cer	
Configuration	Private key file c:\cisco.pvk	Use this page to generate a self-signed certificate. You have the option of having ACS automatically install the certificate
Interface Configuration	Private key password	do so, the certificate is added to local machine storage. Each time you generate a self-signed certificate, the certificate and
Administration Control	Retype private key	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
External User	Key length 2048 bits	server certificates and to end-user clients for use as certification authority certificates so that the end-user client will bruck OCE. If you certificates is to the termination of the second
Databases	Digest to sign with SHA1	win clust ACS. If you secure remote access to the web interface using HTTPS, you can also import the certificate into local storage on computers that run web proveers for access
Validation	Install generated certificate 🗵	to ACS.
Profiles	💡 Back to Help	Certificate subject
Reports and Activity		Type the subject for the certificate, prefixed with "cn=". We recommend using the ACS server name. For example,
Online Documentation		
		versize the full path and file name for the certificate file that
		you want to generate. For example, "ci\acs_server_cert \acs_server_cert.cer". When you submit this page, ACS
		creates the certificate file using the location and file name you specify.
	Submit Cancel	[Back to Top]
		Nuiusto kou filo

Hình 126

Xuất hiện thông báo sau (hình 127).

Edit View His		
	☆ http://127.0.0.1:3752/	숫 · Google
CISCO SYSTEMS	System Configuration	
միտմիտ	Solori	
Itematilities Image: Secure protection Image: Secure protection </td <td>System Conngutation Select ACS Certificate Setup ACS Certificate ACS Certificate Provention Setup Certificate Revocation Lists Certificate Revocation Lists Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only. Cancel</td> <td>Install ACS Certificate ACS Certificates ACS Certificate network list Certificate Revocation Lists Certificate Revocation Lists</td>	System Conngutation Select ACS Certificate Setup ACS Certificate ACS Certificate Provention Setup Certificate Revocation Lists Certificate Revocation Lists Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Central Certificate Signing Request Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only. Cancel	Install ACS Certificate ACS Certificates ACS Certificate network list 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
∕ào syst	Hinh 127 tem configuration> Service Cont	rol (hình 128).
7ào sysi	Hinh 127 tem configuration> Service Cont	rol (hình 128).
Zào sysi scosecure ACS Edit ⊻iew Hig	Hinh 127 tem configuration> Service Cont	rol (hình 128).
Tào syst scosecure ACS - Edit Yiew Hig S. C X	Hinh 127 tem configuration> Service Cont Mozilla Firefox tory Bookmarks Tools Help The http://127.0.0.11:3752/	rol (hình 128).
Tao syst Edit View Hig Co C X Sco Systems	Hinh 127 tem configuration> Service Cont MozIIIs Firefox Tools Leb Tools	rol (hình 128).
Vào sysi scosecure ACS - Edit View Hig >> C X isco Systems allinamatilina.	Hinh 127 tem configuration> Service Cont Mozilla Firefox tory Rookmarks Tools Help To Thep://127.0.0.1:3752/ System Configuration Stelest	rol (hình 128).
COSECUTE AES - Edit View Hig Cosecute AES - Edit View Hig Cosecute Cosecute Sec	Hinh 127 Term configuration> Service Cont	Service Control Cont
AD SYSS scoSecure ACS - Edk ylew Hg C X sco Systems sco Systems sco Systems sco Systems be be be be configuration c	Hinh 127 tem configuration> Service Cont	 Service Control Service Control Service Control Service Control Control Service Control Control Service Control Service Control Control Service Control Service Cont

LabPro Wireless

ent sol

🐸 CiscoSecure ACS - M	1ozilla Firefox			8×
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> t	ory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			12
<->- C ×	☆ http://127.0.0.1:3752/		☆ • Google	\mathbf{P}
CISCO SYSTEMS	System Configuration	-		×
User Setup Group Setup Shared Profile Components	CiscoSecure ACS on c0109		Starting and Stopping the ACS Services Services Log File Configuration Starting and Stopping the ACS Services	_
Network Configuration Sustem Configuration	Services Log File Configuration		To restart or stop the ACS reviews, click as appropriate the Restart or Stop button, located at the bottom of the page. This achieves the same result as starting and stopping all the services (excluding CSAdmin) from within Windove Control Panel. CSAdmin is the web server for the interfaces, and it is not restarted. It is left on to prevent remote administrators cSAdmin can be started or stopped from the Services ion in Windove Control Panel. However, it is best to allow ACS to handle the services because there are dependencies in the order in which the services are started.	
External User Databases Posture Validation	© Low © Full Generate New File © Every day		[Back to Top] Services Log File Configuration The options in this section control the parameters for the Service log file and directory.	
Reports and Activity	© Every week © Every month © When size is greater than 10240 KB		Level of detail Click one of the following options to determine the level of detail that appears in the log file:	
	☞ Manage Directory ⓒ Keep only the last ₃ofiles ⓒ Delete files older than 7days		None. No log file is generated. Low. Only start and stop actions are logged. Full. All services actions are logged. Generate New File To use solutional two as full fast avail of datall, disk as a of the	
Done	Restart Stop Cancel	-	n jou salected by Srian to Even for develop data in the one following options to configure when the new log file is generated. Note: To make sure your system is set to your local time, click Start: Settings: Control Panel: Regional Settings.	-

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

Hình 129

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

Cấu hình hỗ trợ cơ c<mark>hế</mark> xác thực theo FAST.

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

Image: Barried Profile Image: Barried	Ciscosecure ALS - Mozilla Firefox	_ 변 초
System Configuration System Configuration Stor Stor </th <th>Eile Edit View History Bookmarks Iools Help</th> <th></th>	Eile Edit View History Bookmarks Iools Help	
Litts Stritter System Configuration State Service Control Image: Service Control Image: Service Control Image: Service Control Date Format Control Image: Service Control Date Service Management Image: Service Management Date Service Management Image: Service Management ACS Certificate Setup Image: Service Management Service Control Service Management Service Management Image: Service Management Service Management	< >- C 💥 🏠 📋 http://127.0.0.1:3752/	्रि • Google 🔎
System Configuration State State Image: Service Control Select to open the page from which you can stop or rest	CISCO SYSTEMS System Configuration	×
State	ally ally	
day/month/year, for CSV files and Service Logs and in the GUI.	State State </th <th>Service Control Longing Service Control Longing Acts Revice Management Acts Internal Database Replication Acts Revice Management Acts Control Service Control Service Control Select to open the page from which you can stop or restart Cisco Secure ACS reports and customize the type of information that is logged. If act to Top! Date Format Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. If act to Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. If act to Top! Date Format Control Select to configure and Service Logs and in the</th>	Service Control Longing Service Control Longing Acts Revice Management Acts Internal Database Replication Acts Revice Management Acts Control Service Control Service Control Select to open the page from which you can stop or restart Cisco Secure ACS reports and customize the type of information that is logged. If act to Top! Date Format Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. If act to Control Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. If act to Top! Date Format Control Select to configure and Service Logs and in the

Hình 130

Chọn EAP – FAST Configuration (hình 131).

Hình 131

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

🐸 CiscoSecure ACS - M	lozilla Firefox		_ @ ×
Eile Edit View Histo	ory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
< 🔊 - C 🗙	☆ http://127.0.0.1:3752/		र्ट्र • 🔽 Google 🔎
CISCO SYSTEMS	System Configuration		X
antillinaantillina -	EAP-FAST Settin	gs 🔺	
User Stop Stop <t< th=""><th>EAP-FAST Ø Allow EAP-FAST Active master key TTL Retired master key TTL Tunnel PAC TTL Client initial message: Authority ID Info: Ø Allow anonymous in-band PAC Allow authenticated in-band P/ Accept client on authentica Require client certificate fo Allow Machine Authentication Machine PAC TTL Allow Stateless session resum Authorization PAC TTL Allowed inner methods Ø EAP-GTC Ø EAP-GTC Ø EAP-TLS Select one or more of the following comparison methods: © Certificate SAN comparison Submit Submit + Restart</th><th></th><th>Authentication configuration errors Number Error 1 To enable "Anonymous PAC provisioning" option, "EAP-MSCHAPv2" and "EAP-GTC" must be turned on.</th></t<>	EAP-FAST Ø Allow EAP-FAST Active master key TTL Retired master key TTL Tunnel PAC TTL Client initial message: Authority ID Info: Ø Allow anonymous in-band PAC Allow authenticated in-band P/ Accept client on authentica Require client certificate fo Allow Machine Authentication Machine PAC TTL Allow Stateless session resum Authorization PAC TTL Allowed inner methods Ø EAP-GTC Ø EAP-GTC Ø EAP-TLS Select one or more of the following comparison methods: © Certificate SAN comparison Submit Submit + Restart		Authentication configuration errors Number Error 1 To enable "Anonymous PAC provisioning" option, "EAP-MSCHAPv2" and "EAP-GTC" must be turned on.
00.10			

Hình 132

Cấu hình Wireless client hỗ trợ kiểu xác thực FAST.

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

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

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

🖹 Cisco Aironet Desktop Uti	lity - Current Profile: Default	? 🛛
<u>A</u> ction <u>O</u> ptions <u>H</u> elp		
Current Status Profile Manageme	nt Diagnostics	
Contract Con		<u>N</u> ew
User vlan3abc		Modify
		Remo <u>v</u> e
		Activate
← Details		
Network Type:	Infrastructure	Import
Security Mode:	Disabled	
Network Name 1 (SSID1):	<empty></empty>	<u>E</u> xport
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

Hình 133

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

Av	ailable Infrastructu	ire an	d Ad Hoc Networks			? 🗙
	Network Name (SSID) i chinh nguyen i management i management i Thuc Tap khong i vlan2 i vlan2	(2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2)	Signal-to-Noise Ratio (SNR) ?? 24 dB ?? 28 dB ?? 12 dB ?? 25 dB ?? 28 dB ?? 11 dB) Channel 11 6 36 1 6 36 36	Wireless Mode 2.4 GHz 54 Mbps 2.4 GHz 54 Mbps 5 GHz 54 Mbps 2.4 GHz 54 Mbps 2.4 GHz 54 Mbps 5 GHz 54 Mbps 5 GHz 54 Mbps	
l			Activate	Refresh	ОК	

Hình 134

Chọn vlan2 → OK (hình 135).

Profile Management		? ×
General Security Advance	d	
Profile Settings Profile Name:		
Client Name:	C0106	
Network Names		
SSID1:	vlan2	
SSID2:		
SSID3:		
This Device is controlled by Security and other settings f	the Windows Wireless Configuration Service. It may override Network Name, rom this profile.	
		ancel

Hình 135

V.	
Profile Management	? 🗙
General Security Advance	d
Profile Settings	
Profile Name:	test_FAST
Client Name:	C0106
Network Names	
SSID1:	vlan2
SSID2:	
SSID3:	
	OK Cancel

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

Hình 136

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

file Management	?
eneral Security Advanced	
- Set Security Options	
◯ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: LEAP
🔿 WPA/WPA2 Passphrase	
💿 802.1x	802.1x EAP Type: EAP-FAST
O Pre-Shared Key (Static WEP))
◯ None	
Configure	Allow Association to Mixed Cells Profile Locked
	📃 Limit Time for Finding Domain Controller To: 🕕 📚 sec
Group Policy Dela	y: 60 🔷 sec
	OK Cance
	Hình 137

EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Mashing Information for Domain Logan	

Hình 138

ΟK

Cancel

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

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

EAP-FAST Authentication Status	? _ 🗆 🗙
Card Name: Cisco Aironet 802.11a.	/b/g Wireless Adapter
Profile Name: test_FAST	
Steps	Status
1. Starting EAP-FAST 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 139

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

D:\WINDOWS\system32\cmd.exe	- 🗆 ×
Windows IP Configuration	_
Ethernet adapter Wireless Network Connection:	
Connection-specific DNS Suffix .: IP Address: 192.168.2.4 Subnet Mask: 255.255.255.0 IP Address	
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:	
Connection-specific DNS Suffix . : IP Address : fe80::5efe:192.168.2.4%2 Default Gateway :	
D:\>	-

Hình 140

Ping kiểm tra (hình 141).

Hình 141

