Cấu hình xác thực bằng RADIUS server



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

Mô tả yêu cầu:

• Cấu hình RADIUS server trên Win 2003, tạo user và password cho các client dự định tham gia vào mạng

• Bật tính năng xác thực EAP Authentication với RADIUS server trên AP Aironet (bằng webpage và CLI).

• Cho PC tham gia vào mạng, kiểm tra kết nối.

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

Các bước thực hiện :

1. Cấu hình RADIUS server trên win 2003:

• Cài đặt phần mềm Cisco Secure ACS v3.2 trên pc chạy win 2003 để làm server. Double click vào file setup.exe trong thư mục chứa phần mềm ACS để tiến hành cài đặt. Màn hình setup hiện ra :

Before You Begin				×
	BEFORE YOU E complete:	EGIN, the	following item	is must be
	🔽 End-user cli	ents can suc	cessfully connec	t to AAA clients
	🔽 This Windo	ws Server ca	in ping the AAA o	clients
	Any Cisco II 11.1 or later	OS AAA clier	nts are running Ci	sco IOS release
	Microsoft In installed	ternet Explor	er v6.0 SP1 or N	etscape v7.02 is
	When you have co and then click Nex	ompleted all c it.	of these items, ch	eck each one
	If these items h proceed with th Click Cancel an	ave not be e installati d complete	en completed, on of CiscoSe these items.	. do not cure ACS.
	<u>E</u> xplain >>	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

To successfully configure Cisco your first NAS, the following info NASes can be configured from installed.	oSecure ACS to communicate wi ormation is required. Additional within CiscoSecure ACS once
Authenticate Users Using:	RADIUS (Cisco Aironet)
Access <u>S</u> erver Name:	ap2
Access Server <u>I</u> P Address:	192 . 168 . 1 . 254
Windows Server IP Address:	192 . 168 . 1 . 1
TACACS+ or RADIUS Key:	123456789
< Back	Next > Cancel

Authenticate Users Using : chọn thiết bị tương ứng mà ta sử dụng. Ở đây do ta sử dung Access point là Aironet nên ta chọn là **RADIUS** (Cisco Aironet).

Access Server Name: tùy chọn đặt tên cho thiết bị. Ta nên đặt trùng tên với Access point mà ta muốn cấu hình để dễ phân biệt.

Access Server IP Address: Địa chỉ IP của AP mà ta cần cấu hình để PC server có thể truy cập tới AP. Trong trường hợp này địa chỉ của AP là 192.168.1.254

Windown Server IP Address: địa chỉ IP của Server làm RADIUS. Chẳng hạn như 192.168.1.1

TACACS + or RADIUS Key: đặt key cho RADIUS server phải trùng với key của AP. Nhấn **Next** để sang bước tiếp theo.

Image: Secure ALS user Interface. Image: User Level Network Access Restrictions Image: Group Level Network Access Restrictions Image: Network Access Restrictions
 Max Sessions Default Time of Day/Day of Week Specification Distributed System Settings Database Replication se advanced options along with other features that you may ose to display or hide from the user interface can also be cted from within CiscoSecure ACS after installation is plete.

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

• Tạo User và password :

Giao diện chính của ACS:



Click vào nút User Setup để tạo user

CiscoSecure ACS - Microsoft Internet Explorer	×
Ele Edit View Favorites Tools Help	N
🔾 Back • 🕤 • 🖹 🙎 🟠 🔎 Search 😚 Favorites 🚯 Media 🔗 🍰•	🦆 🖬 🞯
Address a http://127.0.0.1:1756/	💌 🄁 Go 🛛 Links 🏁
Cisco Systems User Setup	×
Select	Help
User Setup Setup Stared Profile Shared Profile Components Stared Profile List users beginning with letter number: A B C D E E G H I J C K L M N O E D C R S I U V M X Y Z O I 2 3 4 5 6 2 8 P Stared Profile List All Users	 User Setup and External User Databases Finding a Specific User in the CiscoSecure User Database Adding a User to the CiscoSecure User Database Listing Usernames that Begin with a Particular Character Listing All Usernames in the CiscoSecure User Database Changing a Username in the CiscoSecure User Database
Control over the second s	User Setup enables you to configure individual user information, add users, and delete users in the database.
 Applet appPing started 	Internet

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



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

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



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

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

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



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

+Thực hiện trên webpage:

• Đặt địa chỉ IP của PC trùng với địa chỉ của AP. Trường hợp này địa chỉ của AP là 192.168.1.254, ta đặt cho PC là 192.168.1.2

• Kết nối giữa PC với AP thông qua cáp thẳng

• Mở trình duyệt web lên, điền địa chỉ của AP là 192.168.1.254 vào thanh địa chỉ, màn hiện đăng nhập hiện ra yêu cầu nhập user name và password. mặc định user name là **Cisco**, Password là **Cisco**

Hinh đăng nhập user name và pass

• Giao diện chính của AP

Hình giao dien chính của AP

Chon muc EXPRESS SECURITY

Hinh trong muc EXPRESS SECURITY

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

+Cấu hình bằng CLI:

• Vào mode config bật tính năng AAA

ap(config)# aaa new-model

• Định nghĩa AAA Server Groups

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

• Cho phép xác thực trên RADIUS

ap(config)#aaa authentication login eap_methods group rad_eap

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

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

ap(config-ssid)#guest-mode

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

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

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

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

Cấu hình tham khảo:

```
ap#sh running-config
Building configuration...
```

```
Current configuration : 2430 bytes
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
١
hostname ap
enable secret 5 $1$EdQk$vBu/6AkF37mOFlG07co6i1
1
ip subnet-zero
aaa new-model
١
aaa group server radius rad eap
server 192.168.1.1 auth-port 1645 acct-port 1646
1
aaa authentication login eap methods group rad eap
aaa session-id common
```

```
dot11 ssid ap2
authentication open eap eap methods
authentication network-eap eap methods
guest-mode
power inline negotiation prestandard source
--More-- !
username Cisco password 7 047802150C2E
bridge irb
١
١
interface Dot11Radio0
no ip address
no ip route-cache
encryption mode wep mandatory
ssid ap2
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
--More-- bridge-group 1 spanning-disabled
1
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
interface FastEthernet0
no ip address
no ip route-cache
```

```
--More-- duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
hold-queue 160 in
1
interface BVI1
ip address 192.168.1.254 255.255.255.0
no ip route-cache
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779...onfig/help/eag
ip radius source-interface BVI1
radius-server host 10.0.0.2 auth-port 1645 acct-port 1646 key 7 1446405858517C
control-plane
bridge 1 route ip
--More-- !
1
١
line con 0
line vty 04
!
end
```

3. kiểm tra kết nối :

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

ssociation	Authentication	Connection
Select this wireless Et	option to provide hemet networks.	authenticated network access for
Enable	IEEE 802.1x aut	nentication for this network
EAP type:	Smart Card or o	other Certificate 😽
Authen	ticate as compute	er when computer information is available
Autheni Autheni Autheni unavai	ticate as compute ticate as guest w able	er when computer information is available

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

reless Networks	Link Status	Site Monitor	Diagnostics	Information		
Let this tool Show utility is Enable Radi	manage your v coni o	weless netwo	iks	e da result (Abrill		
Preferred network	k connections					
our computer a	utomatically or	onnects to the	first network th	at is within range	•	-
Add -	Edt Par		0	Options -		
Type Netwo	vik Name			Security		
	Click Ad	e bhe at b	network co	nnection to l	this list	
	Click Ad	d to add a	network co	nnection to I	this list.	

Click vào nút Add

Network name (SSID)	ap1	Select.	
This is an ad hoc network	Channel 1	141	
Network authentication:	902.1×	×	
CAP method	EAP method		
LEAP	ONE -		
🔲 Mataon Key 🔳 User Na	me/Password	ntty 🔲 Server Identity 📕 Options	
Prompt for user na	ame and password		
Prompt for user ru	ame and password		
Prompt for user nu	ame and password		
Prompt for user na	erre and password		
Prompt for user na	ane and password down domain from Name.		
Prompt for user nu	ene and password Sowe domain Prenover		
Prompt for user nu	ene and password Sowe domain Pressword password Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pressword Pre	n as 1 fger	

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

and an international	Link Status	Site Mor	nitor C	Nagnostics	Informatio	m		
Let this tool Show utility is Enable Radie	manage your con o	wveless rv	etworka					
Preferred network	k connections							
rour computer a	utomatically o	onnects to	the first	t network t	nat is within	range.		
· ·	Edd Ba	×	0	0	Ontons	•		
Type Netw	ork Name			- passer () i	- upsons		Security	
100							8	
	-							

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

"ap1"	
Domain/User Name:	vnpro1
Password:	
	OK Cancel

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

🐼 Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128 Reply from 192.168.1.1: bytes=32 time<1ms TTL=128 Reply from 192.168.1.1: bytes=32 time=2ms TTL=128 Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\>

=>ping thành công, kết nối hoàn tất

[Nguồn: VnPro biên soạn]