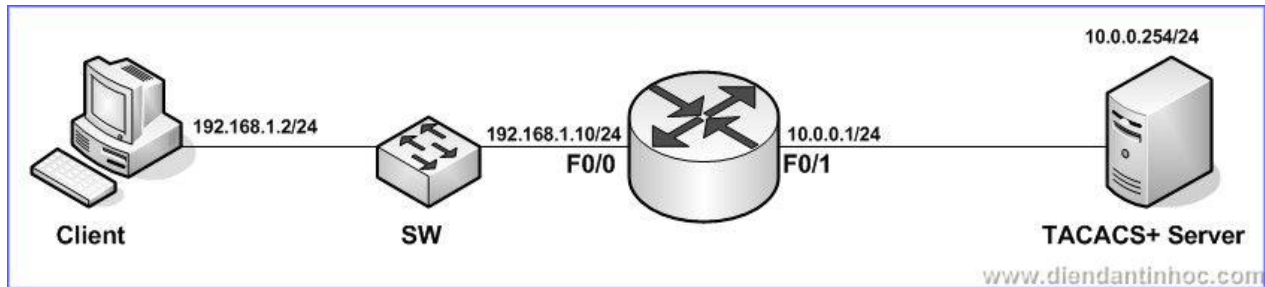


Quyền lý router bằng TACACS+ server kết hợp Privilege Levels



_TACACS+ và RADIUS server cung cấp cho bạn khả năng quản lý truy cập các thiết bị trong mạng một cách tập trung và hiệu quả tính năng bảo mật. privilege levels trong router Cisco là sự phân cấp quy định quyền sử dụng thiết bị. Bài viết này dựa vào ý tưởng kết hợp hai yếu tố trên cùng một giải pháp quản lý mạng để nâng cao tính an toàn cho hệ thống mạng. C TACACS+ và RADIUS là hai giao thức có liên quan đến nhau. Về câu hỏi thì trả lời là tại sao tác giả bài viết lại chọn TACACS+? trả lời câu hỏi thì ta hãy xem ưu điểm của TACACS+ trong quản lý router :

_RADIUS không cho phép kiểm soát hành động mà user thực hiện và không cho phép sử dụng trên router. TACACS+ thì làm được điều này và hạn chế hành động trong quản lý router như vào vì cung cấp 2 phương thức kiểm soát vì cấu hình (authentication) trên phiên đăng nhập user và group:

+ Gán hành động nào đó cho các thiết bị thông qua privilege levels và thông qua TACACS+ server áp dụng phân cấp quy định này cho user truy cập vào.

+ Xác định hành động nào đó có thể thực hiện trên router lên user hoặc group thông qua hành động cụ thể trên TACACS+ server.

A. Phần 1: Cấu hình Privilege Levels

Privilege Levels

_Mặc định trên router có sẵn 3 privilege levels:

.Privilege level 0: ít sử dụng. Gồm 5 lệnh: **disable, enable, exit, help** và **log out**

.Privilege level 1: non-privilege. Thường gọi là "router>"

.Privilege level 15: privilege – thường gọi là cấp cao nhất vào chế độ enable (router#)

_Levels từ 2-14 không có cấu hình mặc định nhưng ta có thể cấu hình chuyển đổi như những gì của các levels với nhau. Khi đang truy cập router ở level nào, ta gõ lệnh **show privilege**. Khi thấy những hành động nào có thể sử dụng trong level đang ở thì ta gõ ? khi đang truy cập level cần xác định.

Mô tả yêu cầu

_Cài đặt cấu hình chính xác và cấu hình cho user dựa vào privilege levels trên TACACS+ server

_Cấu hình AAA service trên router

_Dùng client với chế độ terminal kiểm tra kết quả.

Thi t b

_Router Cisco 2691

_M t PC cài Windows XP làm client

_1 máy tính Windows Server 2003 cài ch ãng tr ãnh Cisco Secure ACS. Link:

. http://rapidshare.com/files/117780965/Cisco_Secure_ACS_4.0.1.27_Full.rar

. <http://www.mediafire.com/?xwmggygf2f4>

Các b c th c hi n

1.Cài t và c u hình TACACS+ server:

a.Vi c cài t không khó, c n chú ý các v n sau:

+ Dùng Internet Explorer 6SP1 ho c Netscape 7 tr ã lên

+ Cài t Java. Link: www.java.com

+ Check t t c các ô.

Sau khi cài t xong. Click vào bi u t ãng ACS admin trên desktop truy c p vào server thông qua trình duy t web



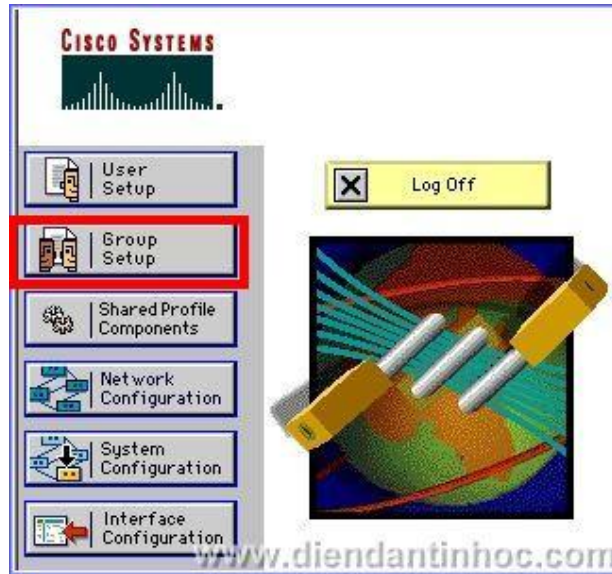
Hình 1: Giao di n chính c a ch ãng tr ãnh Cisco Secure ACS 4.0

b.C u hình trên TACACS+ Server:

B c 1: T o group

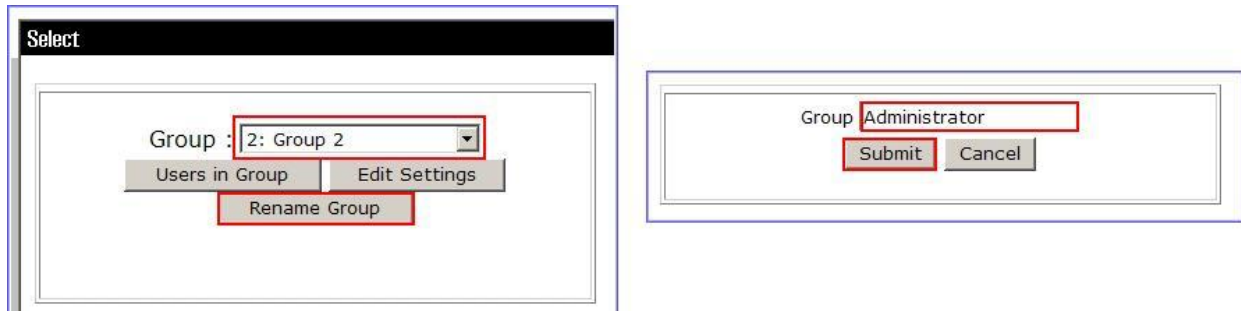
ây chúng ta s t o ra 2 nhóm. Nhóm m t l à Administrator có quy n privilege level 15 và nhóm guest có quy n privilege level 0.

. Vào Menu Group Setup



Hình 2: T o Group

.Ch n m t group b t k r i ch n Rename Group. Nh p vào Administrator r i click Submit.



Hình 3: T o Group mang tên Administrator

Làm t ng t t o ra thêm m t group n a tên Guest. Tì p n ta phân quy n cho 2 nhóm theo privilege level nh ã nói trên: Tr c h t ta phân quy n cho nhóm Administrator.

Ch n Group là Administrator r i sau ó ch n **Edit Settings**



Hình 4: C u hình cho t ng group

Trong c a s **Group Setup** tì p theo ta làm l n l t nh sau;

- . Ch n **TACACS+** trong m c Jump to
- . Check vào **Shell (exec)**
- . Check vào **Privilege Level** và nh p vào thông s **15**
- . Ch n **Submit + Restart**

Group Setup www.diendantinhoc.com

Jump To **TACACS+**

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing Enabled

Note: PPP LCP will be automatically enabled if this service is enabled

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify Enabled

No escape Enabled

No hangup Enabled

Privilege level

Submit Cancel

Hình 5: Cấu hình cho nhóm Admin mức Privilege Level 15

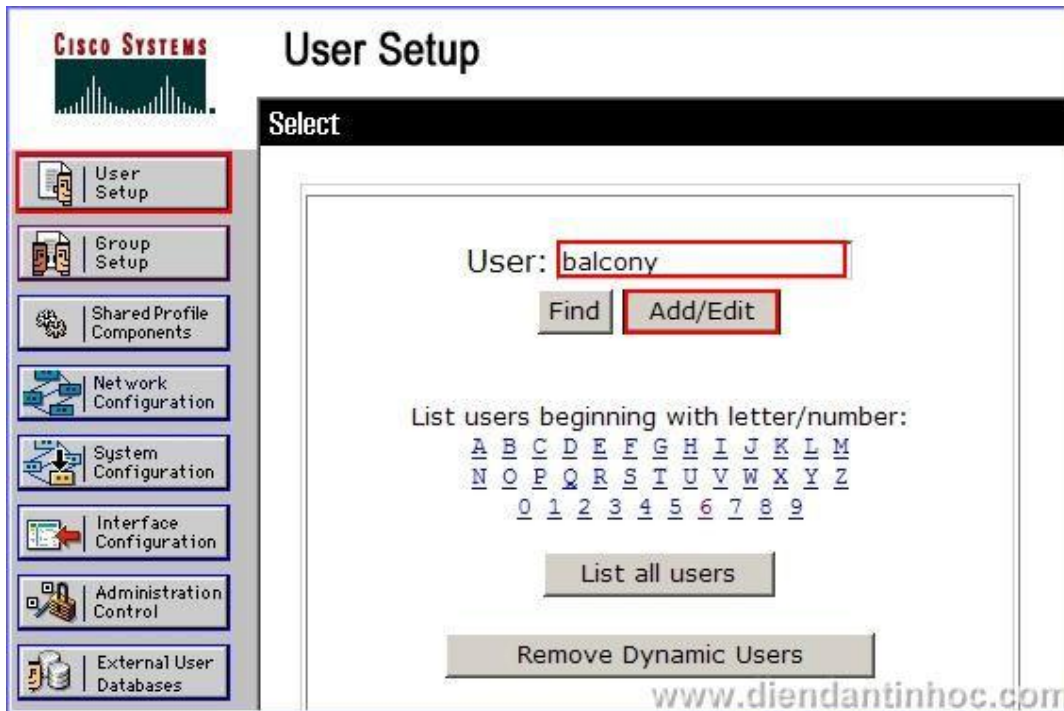
Như vậy, những user nào thuộc group Administrator khi kết nối vào router thông qua TACACS+ servers sẽ có quyền cấp 15.

Với cấu hình cho nhóm Guest Privilege Level 0 tương tự như vậy.

Bước 2: Tạo user và add user vào group

Chúng ta sẽ tạo user mang tên **balcony** thuộc group **Administrator** và user mang tên **Guest** thuộc nhóm **Guest**

Vào menu **User**, nhập vào tên **balcony**, chọn **Add/Edit**



Hình 6: Thêm user mang tên balcony

Trong màn hình **User Setup** tiếp theo ta cần nhập các thông số sau:

- + Password authentication: **ACS internet Database**
- + Password cho user **balcony**
- + Chọn nhóm cho user này là **Administrator**.

User Setup

User Setup ?

Password Authentication:

ACS Internal Database ▾

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

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Administrator ▾

www.dientanlinhoc.com

Hình 7: C u hình cho user **balcony**

Vi c t o và c u hình cho user Guest và group Guest ta làm t ãng t .

B c 3: C u hình AAA server và Client:

Vào menu Network Configuration. Tr c tiên ta c u hình AAA client. Click vào **Add Entry** trong ph ãn AAA Client

Hình 8: Ch n ph n c u hình AAA Client

Trong c a s t i p theo ta c n nh p các thông s sau:

+AAA Client hostname: hostname c a router (center)

+AAA IP address: a ch c a router 10.0.0.1

+Key: khoá th ng l ng gi a router và server (ta ch n tu ý và c n ph i kh p v i giá tr s nh p khi c u hình router)

+Authentication Using: T t nhiên là ch n TACACS+

Sau ó ta ch n **Submit** + **Apply**

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using: **TACACS+ (Cisco IOS)**

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

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Hình 9: Cấu hình cho AAA client

Tiếp theo ta sẽ cấu hình cho AAA Server:

Chọn **Add Entry** trong phần AAA server:

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type

Hình 10: Chọn cấu hình thêm mới AAA server.

Nhập vào các giá trị sau:

- + AAA server name: tùy ý
- + AAA server IP: địa chỉ IP của máy cài TACACS+
- + Key: khóa giao thức (trùng với khóa lúc này là 123456)
- + AAA server type: Chọn TACACS+

Chọn vào Submit + Apply

Hình 11: Cấu hình thông số cho AAA server

2. Cấu hình trên router:

Sau đây là những lệnh cấu hình chính: Chú ý là những lệnh này dùng cho Cisco IOS 12.05 trở về sau

```
center(config)#aaa new-model
center(config)#aaa authentication login default group tacacs+
center(config)#aaa authorization exec default group tacacs+
center(config)#tacacs-server host 10.0.0.254 //IP của TACACS+ server
center(config)#tacacs-server key 123456 //key nhập trên
```

Cấu hình nhìn chung thì cũng không có gì đáng nói. Đây là link download toàn bộ file cấu hình của router Center:

- . <http://www.box.net/shared/5cwvyi804k>
- . <http://www.mediafire.com/?tqfyhj4x9ux>

3. Kiểm tra hoạt động:

Sử dụng máy client chạy Windows XP và dùng command line telnet vào router Center kiểm tra cấu hình bằng hai tài khoản **balcony (admin)** và **Guest (guest)**

Trên client ta vào CMD và gõ lệnh **telnet 192.168.1.10**. Thông báo yêu cầu nhập username và password sẽ hiện lên. Ta nhập vào balcony và password tương ứng như đã cấu hình:

```

c:\ Telnet 192.168.1.10
Username: balcony
Password:
center#enable
center#conf t
Enter configuration commands, one per line. End with CNTL/Z.
center(config)#_

```

www.diendantinhoc.com

Hình 12: Truy cập vào router với tài khoản level 15

Ta thấy như hình, với level 15 khi login vào router sẽ cho privilege.

Tiếp theo ta thử login vào với tài khoản Guest:

```

c:\ Telnet 192.168.1.10
Username: Guest
Password:
center>enable
% Error in authentication.
center>?
Exec commands:
<1-99> Session number to resume
disable Turn off privileged commands
enable Turn on privileged commands
exit Exit from the EXEC
help Description of the interactive help system
logout Exit from the EXEC
center>_

```

www.diendantinhoc.com

Hình 13: Login bằng tài khoản Guest

Hình trên chứng tỏ user Guest với level 0 như ta thấy ở hình thì chỉ có thể sử dụng 5 lệnh như đã nêu ở bài

B. Phần 2: Kỹ thuật Privilege Levels và Command Authorization;

Như đã đề cập trên, sử dụng TACACS+ so với RADIUS đó là chức năng Command Authorization. Nói nôm na đó là xác định những lệnh mà user có thể hoặc không thể sử dụng khi truy cập vào.

Vậy lúc này thì những lệnh mà một user khi login vào thì họ có thể thực hiện chính là những lệnh nằm trong Privilege Levels của họ thì những lệnh mà chúng ta cấu hình trong Command Authorization.

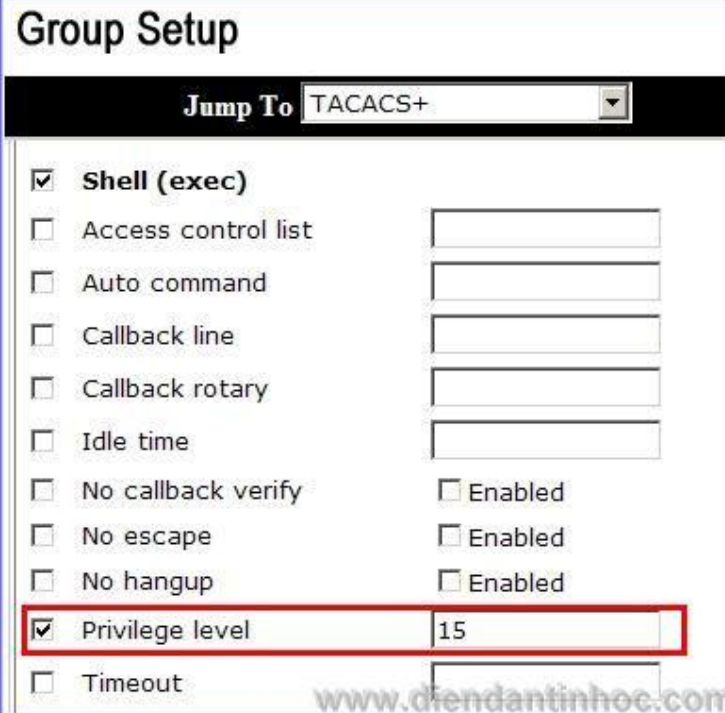
Mô tả yêu cầu:

Dựa trên hai groups có trên là Administrator ta cấu hình thêm như sau:

- + Administrator với Level 15 nhưng không thể xóa **startup-config**
- + Guest lúc này ta set lên level 15 luôn nhưng chỉ có phép sử dụng lệnh **Show**

Các bước thực hiện

Như đã nói trên, trình chúng ta set quyền của nhóm Guest mức 15. Vì chúng ta set lên Level 15 bây giờ có ý nghĩa đó là maximum Level. Trình chúng ta thu về Command Authorization mà bạn sẽ set sau này.



The screenshot shows the 'Group Setup' configuration page for TACACS+. The 'Jump To' dropdown is set to 'TACACS+'. The 'Privilege level' is set to 15 and is highlighted with a red box. Other options include Shell (exec), Access control list, Auto command, Callback line, Callback rotary, Idle time, No callback verify, No escape, No hangup, and Timeout.

Option	Value
<input checked="" type="checkbox"/> Shell (exec)	
<input type="checkbox"/> Access control list	
<input type="checkbox"/> Auto command	
<input type="checkbox"/> Callback line	
<input type="checkbox"/> Callback rotary	
<input type="checkbox"/> Idle time	
<input type="checkbox"/> No callback verify	<input type="checkbox"/> Enabled
<input type="checkbox"/> No escape	<input type="checkbox"/> Enabled
<input type="checkbox"/> No hangup	<input type="checkbox"/> Enabled
<input checked="" type="checkbox"/> Privilege level	15
<input type="checkbox"/> Timeout	

Hình 14: Chọn Level của group Guest lên 15

Bước 1: Tạo nhóm user **Command Authorization** – mức nhóm này chỉ có thể cho các thiết bị dành cho user.

Trước tiên chúng ta vào menu Shared Profile Components. Click vào **Shell Command Authorization Sets**

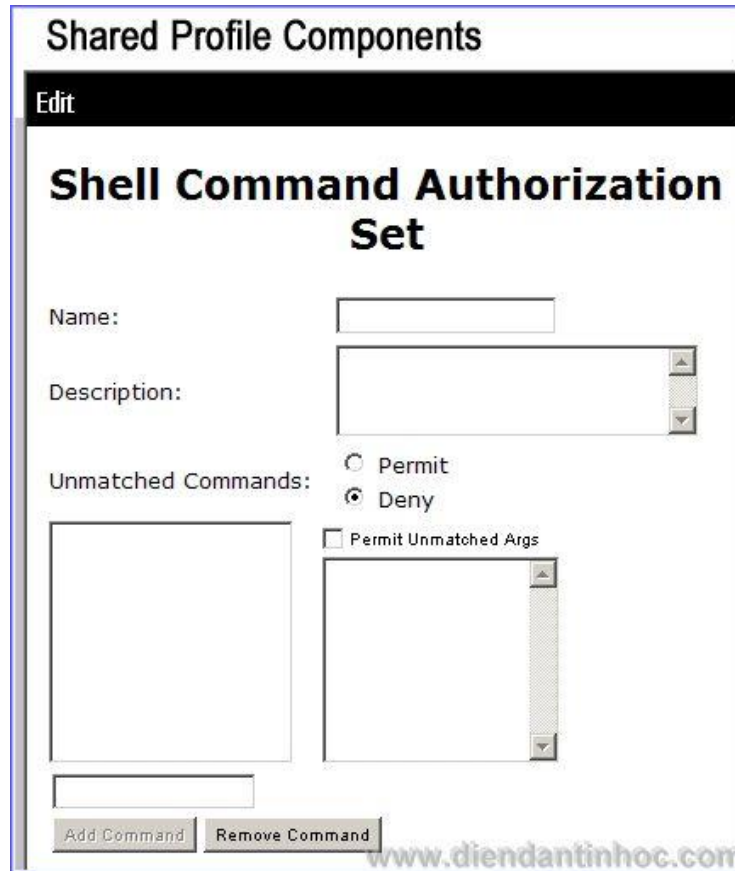


The screenshot shows the 'Shared Profile Components' configuration page. The 'Shared Profile Components' menu item is highlighted with a red box. The 'Shell Command Authorization Sets' option is also highlighted with a red box. Other options include Network Access Filtering, RADIUS Authorization Components, and PIX/ASA Command Authorization Sets.

www.diendantinhoc.com

Hình 15: Chọn chức năng cấu hình Command Authorization

Bấm vào nút **Add** thêm vào menu. Nội dung của hình gồm các phần với nghĩa như sau:



Hình 16: Khung cấu hình Command Authorization

.Name: Tên của menu cấu hình này.

.Unmatched Commands: Chọn cách mà server sẽ hiển thị những lệnh mà bạn không nhập bên dưới. (2 tùy chọn là Permit và Deny)

.Args: argument. Ví dụ **ip route, ip interface brief..** là args của lệnh **show**

.Permit Unmatched Args: Cho phép các args mà bạn không nhập vào. Nếu bạn không check vào thì máy sẽ hiển thị là Deny.

.Add Command: Thêm vào menu lệnh mới. Thêm vào menu lệnh thì bạn nhập vào và sau đó nhấn **Add Command**. Tiếp theo là bạn nhập thêm những args của lệnh đó với cú trúc: **permit/Deny arg.** Nếu bạn thêm một Arg thì bạn nhấn enter xuống dòng. Nếu hiển thị thì bạn nhập vào cấu hình như sau:

T o m u cho nhóm Admin: T o m u cho nhóm Admin. Nhóm Admin sẽ đăng nhập các lệnh Level 15 từ lệnh **erase startup-config**. Bạn làm như sau:

Nhập vào **Name** là **Admin**

.Unmatched commands: chọn permit – tức là cho phép tất cả các lệnh.

Nhập **erase** rồi nhấn **Add command**

Click vào **erase**, gõ vào khung bên phải deny **startup-config**

.Check vào **permit unmatched Args** nếu không máy sẽ cấm các Args khác của lệnh **erase**

Xong ta nh n **Submit**

Shared Profile Components

Edit

Shell Command Authorization Set

Name: Admin

Description:

Unmatched Commands: Permit Deny

Permit Unmatched Args

erase

deny starup-config

Add Command Remove Command

Submit Delete Cancel

Hình 17: t o m u command authorization cho group Admin

T o m u cho nhóm Guest:

Nhóm Guest hi n ang Level 15, t c là có y quy n h n c a Admin nên ta th c hi n theo ý t ng là **permit** m t s l nh, còn l i là **deny all**. C th là ch cho phép Guest th c hi n 2 l nh: show ip route và show ip interface brief

- .Nh p vào Name là Guest
- .**Unmatched commands:** Ch n Deny
- .Add command **Show**. Khung bên ph i nh p vào **deny run; permit ip route; permit ip interface brief**
- .Th c ra nh p vào **deny run** là th a b i vi c không check vào Permit unmatched Arg ã ng m th c hi n l nh này.
- .Click vào **Submit**.

Name:

Description:

Unmatched Commands: Permit Deny

Permit Unmatched Args

show

permit ip interface brief
permit ip route
deny run

www.dientaithoc.com

Hình 18: Tạo mới cho group Guest

Bước 2: Cấu hình Command Authorization cho từng group

Bước 1 ta đã cấu hình nhóm người dùng cho từng group, sang bước này ta sẽ áp dụng người dùng vào từng nhóm thích hợp.

Cấu hình cho nhóm Admin:

- + Vào menu **Group Setup**. Chọn group name là Administrator như đã cấu hình. Click vào **Edit Setting**
- + Kéo thanh cuộn xuống phần **Shell Command Authorization Sets** ta chọn **Assign Shell Command Authorization Set for any network devices**. Click vào và chọn **Admin** ngay bên dưới.
- + Click vào **Submit + Restart**

Group Setup www.diendantinhoc.com

Jump To TACACS+ ▼

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify Enabled

No escape Enabled

No hangup Enabled

Privilege level

Timeout

Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device

Per Group Command Authorization

Unmatched Cisco IOS commands

Permit

Submit Cancel

Hình 19: Cấu hình cho nhóm Admin.

Cấu hình cho nhóm Guest :

Ta làm tương tự :

www.diendantinhoc.com

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify Enabled

No escape Enabled

No hangup Enabled

Privilege level 15

Timeout

Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device

Guest

Per Group Command Authorization

Unmatched Cisco IOS commands

Permit

Submit Submit + Restart Cancel

Hình 20: Cấu hình cho nhóm Guest

Bước 3: Cấu hình trên router

```
center(config)#aaa new-model
center(config)#aaa authentication login default group tacacs +
center(config)#aaa authorization exec default group tacacs+
center(config)#aaa authorization commands 15 default group tacacs+
center(config)#tacacs-server host 10.0.0.254
center(config)#tacacs-server key 123456
```

Bước 4: Kiểm tra hoạt động

Trên PC, ta mở command line và telnet vào địa chỉ 192.168.1.10 của router:

Tài khoản Admin cho ta kết quả:

Như ta thấy hình bên dưới thì kết quả của lệnh **erase startup-config** là **authorization failed**

```

c:\ Telnet 192.168.1.10 www.diendantinhoc.com
Username: balcony
Password:
center#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
center(config)#exit
center#erase
center#erase startup-config
Command authorization failed.
^
% Invalid input detected at '^' marker.
center#

```

Hình 21: Login bằng tài khoản nhóm Admin

Tài khoản Guest:

```

c:\ Telnet 192.168.1.10 www.diendantinhoc.com
Username: Guest
Password:
center#conf t
Command authorization failed.
^
% Invalid input detected at '^' marker.
center#show ip interface brief
Interface IP-Address OK? Method Status
GigabitEthernet0/0 192.168.1.10 YES NVRAM up
FastEthernet0/1 10.0.0.1 YES NVRAM up
center#show run
Command authorization failed.
^
% Incomplete command.
center#

```

Hình 22: Login bằng tài khoản Guest

Hình trên cho ta thấy tài khoản Guest chỉ có thể sử dụng 2 lệnh nhúng cấu hình.

H ết Ch ết :

Do không có điều kiện thực hành trên thì tôi bắt đầu nên mình sử dụng 2 chương trình giả lập phần mềm là Dynamip và Microsoft Virtual PC 2007

Bài viết trên chỉ là hướng dẫn sử dụng. Các bạn khi sử dụng phần mềm thì phải phù hợp với yêu cầu của mình nhé.

