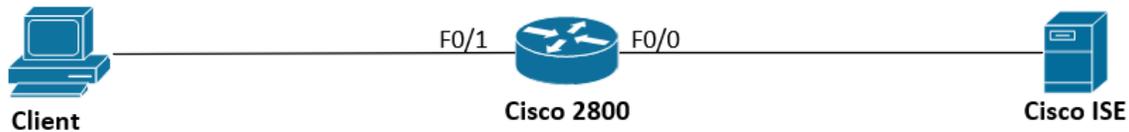


Lab – Xác thực và phân quyền login bằng giao thức TACAS+ sử dụng Cisco ISE

I. Sơ đồ:



Hình 1: Sơ đồ bài lab.

Mô tả:

Sơ đồ gồm 1 Router Cisco 2811 và 1 PC được đấu nối với nhau như trên hình 1. Router được đấu nối ra hệ thống mạng có kết nối tới Server Cisco ISE. Bài lab này có thể được thực hiện trên LAB giả lập sử dụng các IOL Router L3-ADVENTERPRISEK9-M-15.4-2T, qemu Windows 7 win-7-x86-IPCC.

PC Windows 7 vừa là Client để telnet tới Router test việc xác thực vừa để cấu hình Cisco ISE. Nếu đã có thiết bị cấu hình Cisco ISE thì có thể thay thế PC thành Router để test telnet.

Bảng quy hoạch IP:

Tên thiết bị	Interface	IP/Netmask	Gateway
Cisco ISE	NIC	10.215.26.49	-
Router	F0/0	DHCP	-
	F0/1	192.168.99.1/24	-
Client	NIC	192.168.99.99/24	192.168.99.1

II. Yêu cầu:

1. Cấu hình ban đầu

- Thực hiện cấu hình IP cho PC, Router, thực hiện NAT sao cho PC có thể ping thấy ISE server.

2. Cấu hình TACACS+:

- Tiến hành xác thực và phân quyền privilege cho các user truy cập telnet đến Router như sau (việc xác thực/phân quyền phải do Cisco ISE kiểm soát):

- Username: **guest**, password **VnPro@123**, privilege 7
- Username: **adminvnpro**, password **VnPro@123**, privilege 15

- Cấu hình xác thực local với privilege cho các user như trên để khi hoạt động xác thực với Cisco ISE không thành công, chuyển sang phương thức xác thực/phân quyền local.

III. Hướng dẫn:

Cấu hình IP cho Router

```
Router(config)#hostname R
R(config)#int f0/0
R(config-if)#ip address dhcp
R(config-if)#no shutdown

R(config)#int f0/1
R(config-if)#ip address 192.168.99.1 255.255.255.0
R(config-if)#no shutdown
```

Cấu hình NAT cho Router:

```
R(config)#access-list 1 permit 192.168.99.0 0.0.0.255
R(config)#ip nat inside source list 1 interface f0/0 overload
R(config)#int f0/0
R(config-if)#ip nat outside
R(config)#int f0/1
R(config)#ip nat inside
```

Kết nối PC với Router, đặt IP và Gateway. Kiểm tra kết nối tới ISE Server:

```
C:\Users\hoang>ping 10.215.26.49

Pinging 10.215.26.49 with 32 bytes of data:
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=1ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
```

Chỉ định TACACS+ Server cho Router: chỉ định địa chỉ IP của cisco ISE và key dùng chung
123abc

```
R(config)#tacacs-server host 10.215.26.49
R(config)#tacacs-server key 123abc
```

Cấu hình Router xác thực với ISE bằng giao thức TACACS+:

Tạo group server tên ISESRV để gán vào phương thức xác thực và phân quyền. Trong server group có thể chỉ định nhiều server và sẽ sử dụng các server theo thứ tự được chỉ định, nếu server đầu tiên thất bại thì server thứ hai sẽ thực hiện công việc xác thực, phân quyền

```
R(config)#aaa new-model
R(config)#aaa group server tacacs+ ISESRV
R(config-sg-tacacs+)#server 10.215.26.49
```

```
R(config-sg-tacacs+)#exit
```

Tạo phương thức xác thực đăng nhập tên là VTY do group server ISESRV thực hiện, sử dụng thông tin đăng nhập nội bộ nếu kết nối fail

```
R(config)#aaa authentication login VTY group ISESRV local
```

Tạo phương thức phân quyền cho User EXEC terminal tên là VTY do group server ISESRV thực hiện, nếu server bị ngắt, router sẽ làm luôn việc phân quyền sử dụng thông tin đăng nhập nội bộ

```
R(config)#aaa authorization exec VTY group ISESRV local if-authenticated
```

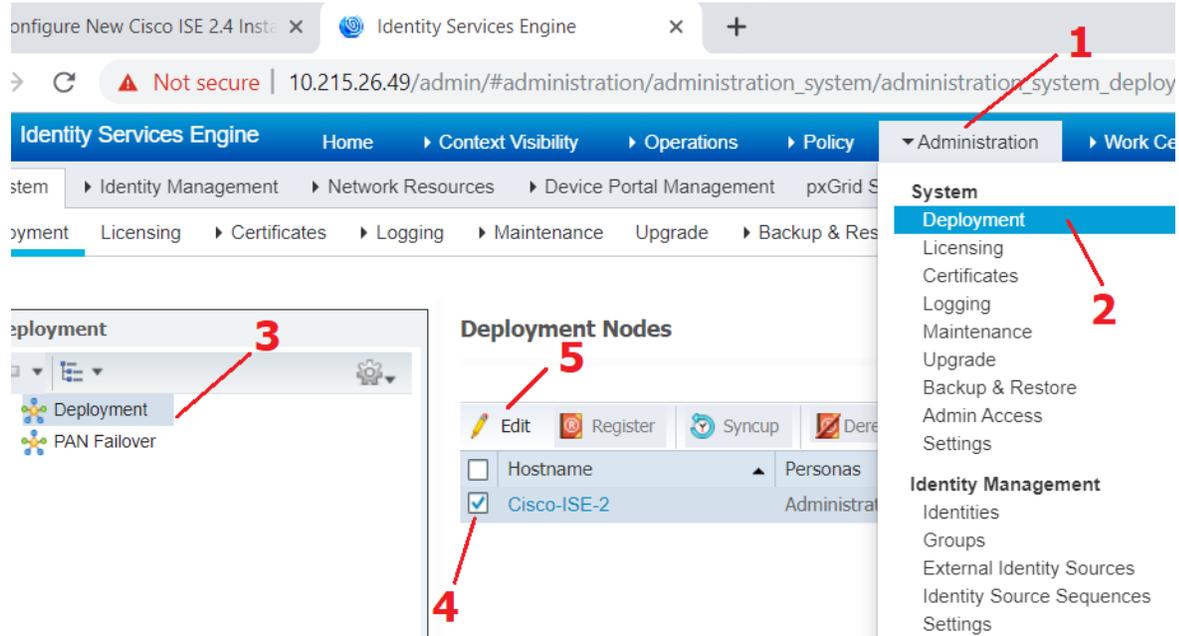
Cấu hình telnet cho Router:

```
Router(config)#line vty 0 4  
Router(config-line)#login authentication VTY  
Router(config-line)#authorization exec VTY  
Router(config-line)#exit
```

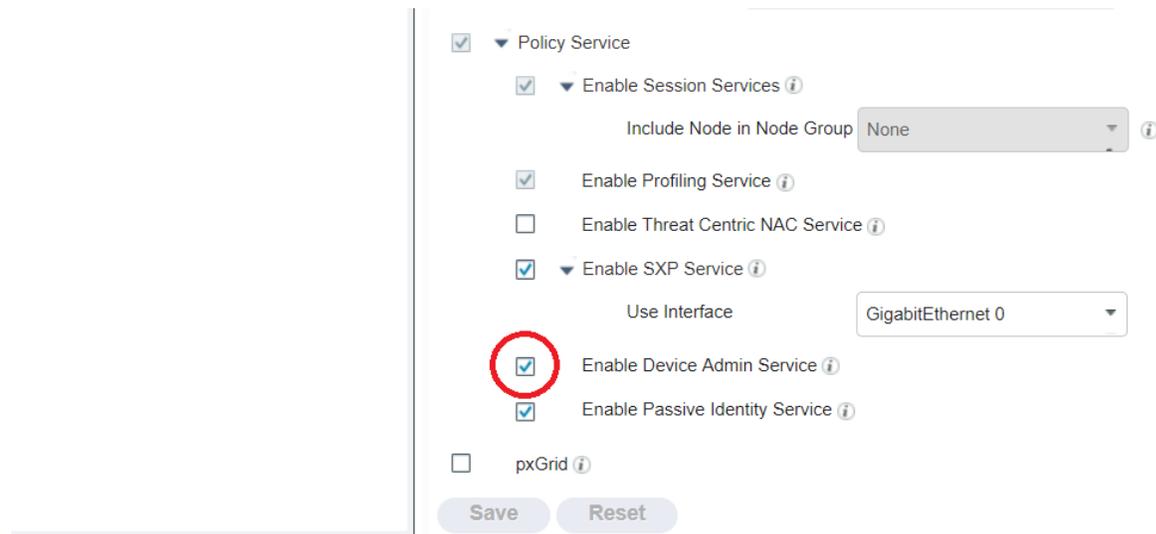
Bật tính năng TACACS+ trên ISE:

Đầu tiên, ta mở trình duyệt và truy cập vào IP 10.215.26.49 (IP của ISE Server). Đăng nhập bằng username và password được cung cấp.

Vào **Administration** → **Deployment** → Tích chọn hostname của Cisco ISE → **Edit**:



Ở phần Policy Service, chọn **Enable Device Admin Service** và Save lại:



Thêm Router vào ISE:

Vào **Work Centers** → **Device Administration** → **Network Resources** → **Network Devices** → **Add**:

Nhập tên, và IP của Router ta muốn thêm:

Name	IP/Mask	Profile Name	Location
------	---------	--------------	----------

* Name: Router
Description:
IP Address: 192.168.3.135 / 24

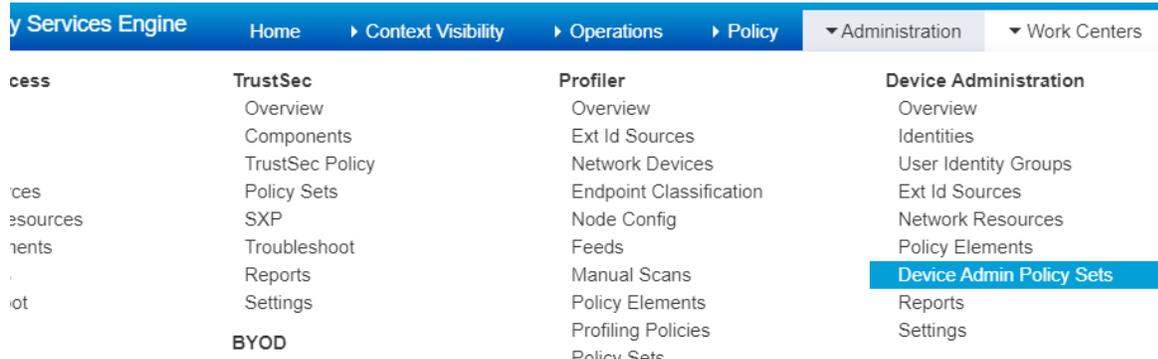
Ở phần **TACACS Authentication Settings** ta chỉ định chuỗi “**Shared Secret**” để Router và ISE giao tiếp với nhau.

Shared Secret: 123abc
Enable Single Connect Mode:
 Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

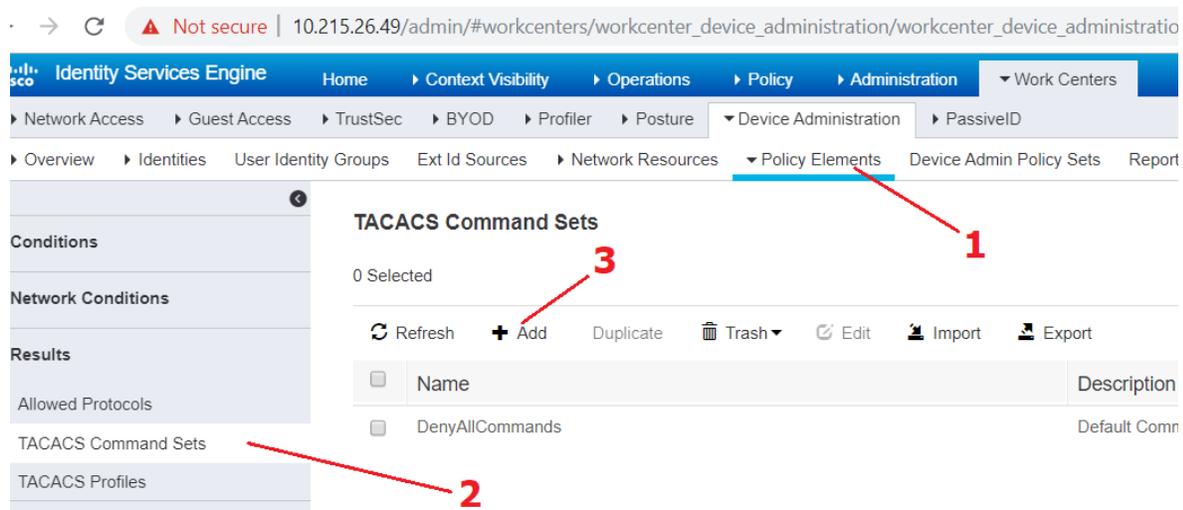
Sau đó bấm submit.

Cấu hình xác thực/phân quyền bằng TACACS+:

Vào Work Center → Device Admin Policy Sets:



Chọn Policy Elements → Result → TACACS Command Sets → Add:



Tạo command set cho user *adminvnpro* có thể dùng đầy đủ các lệnh khi telnet:

TACACS Command Sets > CommandSet1

Command Set

Name

Description

Commands

Permit any command that is not listed below

+ Add Trash ▼ Edit ↑ Move Up ↓ Move Down ⚙

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

Cancel Save

Tích chọn **“Permit any command that is not listed below”** và bấm Save.

Ta cũng tạo thêm command set cho user *guest* có privilege là 7, khi user này telnet vào router chỉ dùng được lệnh các lệnh *show*:

Sau đó bấm **Submit**.

Tiếp theo, ta vào **TACACS Profiles** → **Add**:

TACACS Profiles

0 Selected

Refresh + Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Tạo

profile cho **adminvnpro** với privilege 15:

TACACS Profiles > New

TACACS Profile

Name: Shell 15

Description: Shell for user admin, privilege 15

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

Default Privilege: 15 (Select 0 to 15)

Maximum Privilege: 15 (Select 0 to 15)

Profile cho **guest** với privilege 7:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Center

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy S

TACACS Profiles > New

TACACS Profile

Name: Shell 7

Description: Shell for user Guest

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

Default Privilege: 7 (Select 0 to 15)

Maximum Privilege: 7 (Select 0 to 15)

Access Control List

Vào **Administration** → **Groups** → **User Identify Groups** → **Add**:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Center

Identity Management Network Resources Device Portal Management pxGrid S

Groups External Identity Sources Identity Source Sequences Settings

System

- Deployment
- Licensing
- Certificates
- Logging
- Maintenance
- Upgrade
- Backup & Restore
- Admin Access
- Settings

Identity Management

- Identities
- Groups**
- External Identity Sources
- Identity Source Sequences
- Settings

Identity Groups

User Identity Groups

Edit Add Delete Import

Name
<input type="checkbox"/> Admin7
<input type="checkbox"/> ALL_ACCOUNTS (default)
<input type="checkbox"/> Employee
<input type="checkbox"/> GROUP_ACCOUNTS (default)
<input type="checkbox"/> GroupAdmin

Tạo 2 group cho user *adminvnpro* và user *guest*:

Identity Groups

- Endpoint Identity Groups
- User Identity Groups
 - ADmin7
 - ALL_ACCOUNTS (default)

User Identity Groups > **New User Identity Group**

Identity Group

* Name

Description

Identity Groups

- Endpoint Identity Groups
- User Identity Groups
 - ADmin7
 - ALL_ACCOUNTS (default)

User Identity Groups > **New User Identity Group**

Identity Group

* Name

Description

Vào **Identities** → **Add** → Tạo user **adminvnpro**:

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Network Access Users List > New Network Access User

Network Access User

* Name: adminvnpro

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: * Login Password: VnPro@123

Re-Enter Password: VnPro@123

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

Group_Admin

Submit Cancel

Trong đó:

- **Password Type:** Internal Users
- **User Group:** Group_Admin

Tương tự, ta cũng tạo thêm user **guest** với **User Groups** là Group_Guest:

Network Access User

* Name: guest

Status: Enabled

Email:

User Groups

Group_Admin

Submit Cancel

▼ User Groups

Group_Guest

Submit Cancel

Kết quả:

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Network Resources > Device Portal Management > pxGrid Services > Feed Service

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	De...	F..	Last Na...	E...	User Identity Groups
<input type="checkbox"/> <input checked="" type="checkbox"/>	adminvnpro					Group_Admin
<input type="checkbox"/> <input checked="" type="checkbox"/>	guest					Group_Guest

Tiếp theo, ta vào **Work Center** → **Device Admin Policy Sets** → **bấm (+)**:

Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassivelD

Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > R

Policy Sets

+ Status Policy Set Name Description Conditions

Search

	<input checked="" type="checkbox"/>	Policy for Tacacs	2 Đặt tên cho policy		3 +
	<input checked="" type="checkbox"/>	Default	Tacacs Default policy set		

Tạo policy như sau:

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
		Policy for Tacacs	AND DEVICE: Device Type EQUALS All Device Types Network Access: Protocol EQUALS TACACS+	Select from list +
	Default	Tacacs Default policy set		Default Device Admin x +

Click vào chọn "Default Device Admin"

Sau đó save lại.

Sau đó, ta click vào mũi tên qua phải của policy vừa mới tạo:

Allowed Protocols / Server Sequence	Hits	Actions	View
Default Device Admin x +	0		
Default Device Admin x +	0		

Ở phần "Authentication Policy" ta chọn Use: Internal Users:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Policy Sets → Policy for Tacacs

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
	Policy for Tacacs		AND DEVICE: Device Type EQUALS All Device Types Network Access: Protocol EQUALS TACACS+	Default Device Admin

▼ Authentication Policy (1)

Status	Rule Name	Conditions	Use
		Default	Internal Users Options

Tiếp theo, ta cấu hình phần **Authorization Policy**:

Status	Rule Name	Conditions
+		
✓	Admin Privilege 15	
✓	Default	

Cấu hình conditions như sau:

Conditions Studio
Library

Search by Name

Editor

IdentityGroup-Name

Equals

× User Identity Groups:Group_Admin

Set to 'Is not'

Duplicate Save

+ New AND OR

Close Use

Sau đó bấm “Use” để quay lại mục **Authorization Policy**, ở mục bên phải, ta chọn command set là “**CommandSet15**” và shell profile là “**Shell 15**”.

Status	Rule Name	Conditions	Command Sets	Shell Profiles
+				
✓	Admin Privilege 15	IdentityGroup-Name EQUALS User Identity Groups:Group_Admin	× CommandSet15	Shell 15
✓	Default		× DenyAllCommands	Deny All Shell Profile

Tương tự vậy, ta cũng tạo **Authorization Policy** cho account **guest**:

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
	✔	Guest Privilege 7	IdentityGroup Name EQUALS User Identity Groups:Group_Guest	× CommandSet7	Shell 7		⚙
	✔	Admin Privilege 15	IdentityGroup Name EQUALS User Identity Groups:Group_Admin	× CommandSet15	Shell 15	0	⚙
	✔	Default		× DenyAllCommands	Deny All Shell Profile	0	⚙

Sau đó ta save lại.

Ta dùng PC telnet vào Router với username là *adminvnpro* password là *VnPro@123*:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\hoang>telnet 192.168.99.1
```

Kết quả: Telet thành công:

```
Telnet 192.168.99.1
Username:adminvnpro
Password:
Router#
```

Gõ “?” để kiểm tra các lệnh user này có thể sử dụng, ta thấy user *adminvnpro* có thể dùng tất cả các lệnh:

```
telnet 192.168.99.1
```

```
Username: adminvnpro
```

```
Password:
```

```
Router#?
```

```
Exec commands:
```

```
<1-99>          Session number to resume
access-enable    Create a temporary Access-List entry
access-profile   Apply user-profile to interface
access-template  Create a temporary Access-List entry
alps             ALPS exec commands
archive          manage archive files
audio-prompt     load ivr prompt
auto            Exec level Automation
beep            Blocks Extensible Exchange Protocol commands
bert           Bit Error Rate Testing
bfe            For manual emergency modes setting
calendar        Manage the hardware calendar
call           Voice call
ccm-manager     Call Manager Application exec commands
cd             Change current directory
clear          Reset functions
clock          Manage the system clock
cns           CNS agents
configure      Enter configuration mode
connect        Open a terminal connection
copy          Copy from one file to another
credential     load the credential info from file system
crypto        Encryption related commands.
debug         Debugging functions (see also 'undebug')
delete        Delete a file
dir           List files on a filesystem
disable       Turn off privileged commands
disconnect    Disconnect an existing network connection
--More--
```

```
Router#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#_
```

Thử lại với account *guest* ta thấy account này được sử dụng rất ít lệnh và chỉ sử dụng được các lệnh *show*:

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

C    192.168.99.0/24 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 192.168.3.1
Router#conf t
      ^
% Invalid input detected at '^' marker.
Router#_
```

Không dùng được lệnh "Configure terminal"

Shutdown cổng F0/0 của Router. Ta sẽ không còn telnet vào Router được nữa vì đã mất kết nối đến ISE server:

```
User Access Verification

Username: adminvnpro
Password:

% Authentication failed

Username: adminvnpro
Password:

% Authentication failed

Username:
% Username: timeout expired!

Connection to host lost.

C:\Users\hoang>
```

Cấu hình xác thực/phân quyền local:

Kết nối vào cổng console của Router, ta dùng các lệnh sau:

```
R(config)#privilege exec level 7 show
```

```
R(config)#username adminvnpro privilege 15 password VnPro@123
```

Telnet lại vào Router, sử dụng account **adminvnpro**, ta thấy telnet thành công:

```
C:\ Telnet 192.168.99.1

User Access Verification

Username: adminvnpro
Password:

Router#show privilege
Current privilege level is 15
Router#_
```

Sử dụng account **guest** ta vẫn không kết nối được do không kết nối được với ISE và ta chưa tạo account **guest** trong local:

```
User Access Verification

Username: guest
Password:

% Authentication failed

Username:
% Username: timeout expired!

Connection to host lost.

C:\Users\hoang>
```

Bật trở lại cổng F0/0 của router, ta telnet lại lần nữa với account **guest**:

```
R(config)#int f0/0
R(config-if)#no shutdown
```

Telnet 192.168.99.1

```
Username: guest
Password:
Router#
```

Telnet thành công do kết nối được với ISE và dùng user guest trên ISE.

***Chú ý:** Do sử dụng giao thức DHCP nên khi bật lại cổng F0/0 của Router có thể IP sẽ bị thay đổi, có thể ta sẽ phải add lại thiết bị trên ISE Server.