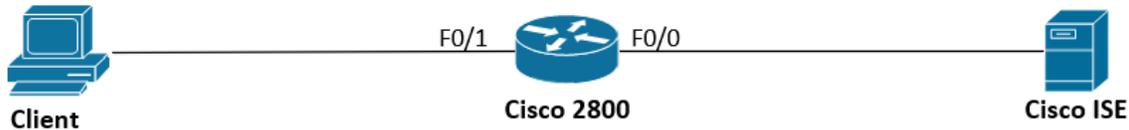


Authentication, Authorization, Accounting

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

I. Sơ đồ:



Hình 1: Sơ đồ bài lab.

Ta có bảng thông tin như sau:

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 cho Router

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

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

Cấu hình NAT cho Router:

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

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

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

Trên Router, ta dùng các lệnh sau:

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

Router(config)#aaa authentication login VTY group ISESRV local
Router(config)#aaa authorization console
Router(config)#aaa authorization exec CON none
Router(config)#aaa authorization exec VTY group ISESRV local if-authenticated
```

```
Router(config)#aaa accounting exec default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting commands 1 default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting commands 15 default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting network default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting connection default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
Router(cfg-acct-mlist)#exit

Router(config)#aaa accounting system default
Router(cfg-acct-mlist)#action-type start-stop
Router(cfg-acct-mlist)#group ISESRV
```

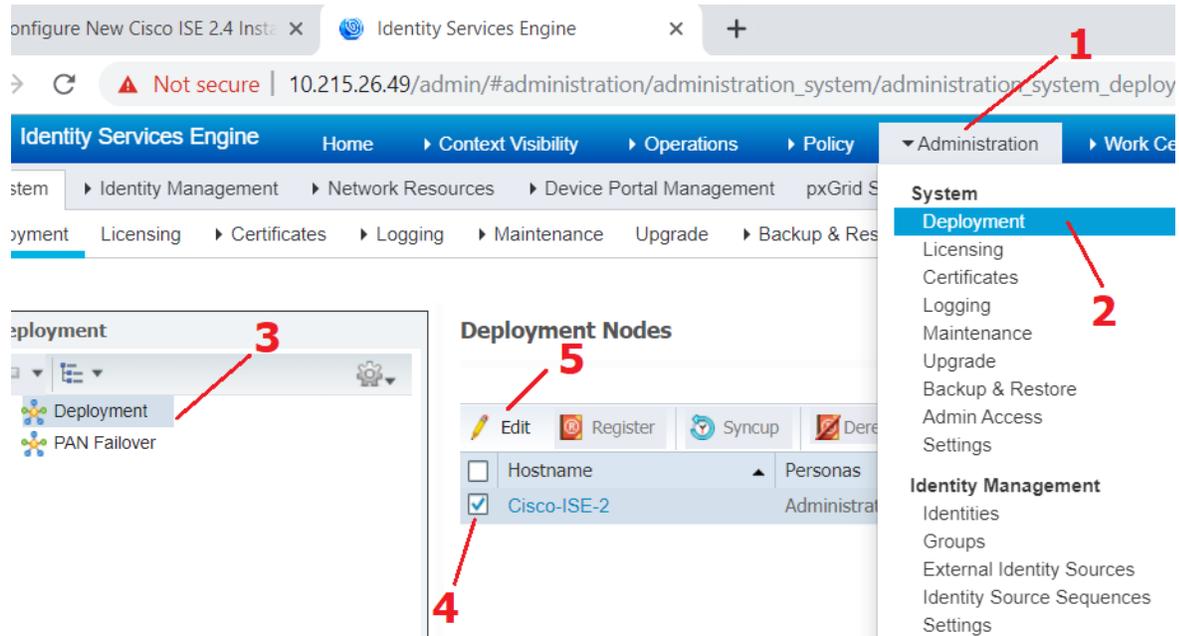
Cấu hình telnet cho Router:

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

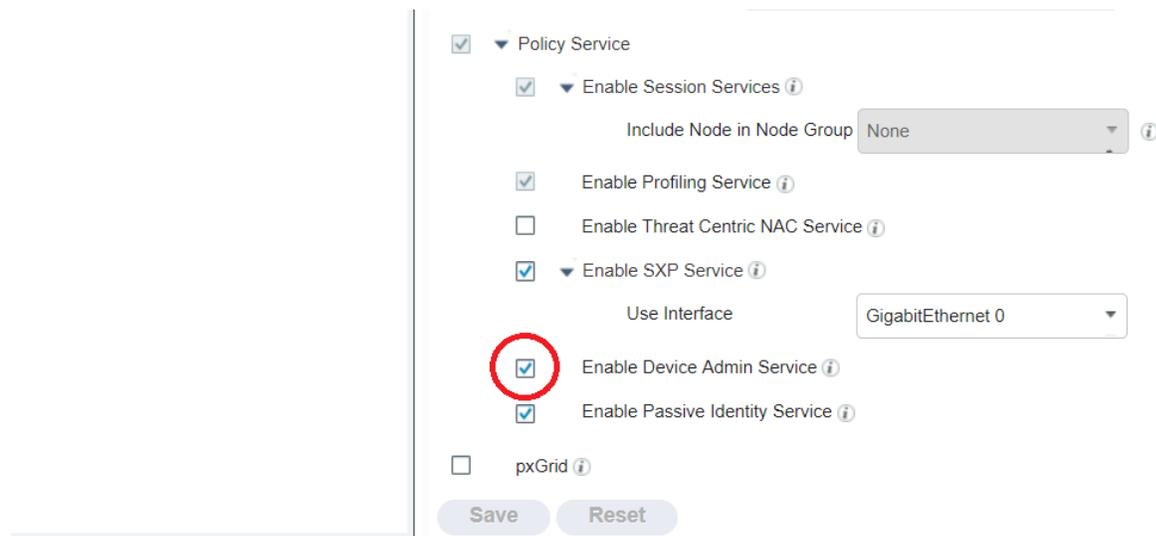
Bật tính năng TACACS+ trên ISE:

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:

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices

Network Devices List > **New Network Device**

* Name Router

Description

IP Address * IP: 192.168.3.135 / 24

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

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret Show

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Submit Cancel

Sau đó bấm submit.

Cấu hình xác thực/phân quyền bằng TACACS+:

Vào Work Center → Device Admin Policy Sets:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

- TrustSec
 - Overview
 - Components
 - TrustSec Policy
 - Policy Sets
 - SXP
 - Troubleshoot
 - Reports
 - Settings
- BYOD
- Profiler
 - Overview
 - Ext Id Sources
 - Network Devices
 - Endpoint Classification
 - Node Config
 - Feeds
 - Manual Scans
 - Policy Elements
 - Profiling Policies
 - Policy Sets
- Device Administration
 - Overview
 - Identities
 - User Identity Groups
 - Ext Id Sources
 - Network Resources
 - Policy Elements
 - Device Admin Policy Sets**
 - Reports
 - Settings

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

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 Report

TACACS Command Sets

0 Selected

Refresh Add Duplicate Trash Edit Import Export

Name	Description
DenyAllCommands	Default Comn

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

TACACS Command Sets > CommandSet1

Command Set

Name CommandSet15

Description Full Privilege for Admin

Commands

Permit any command that is not listed below

+ Add Trash Edit Move Up Move Down

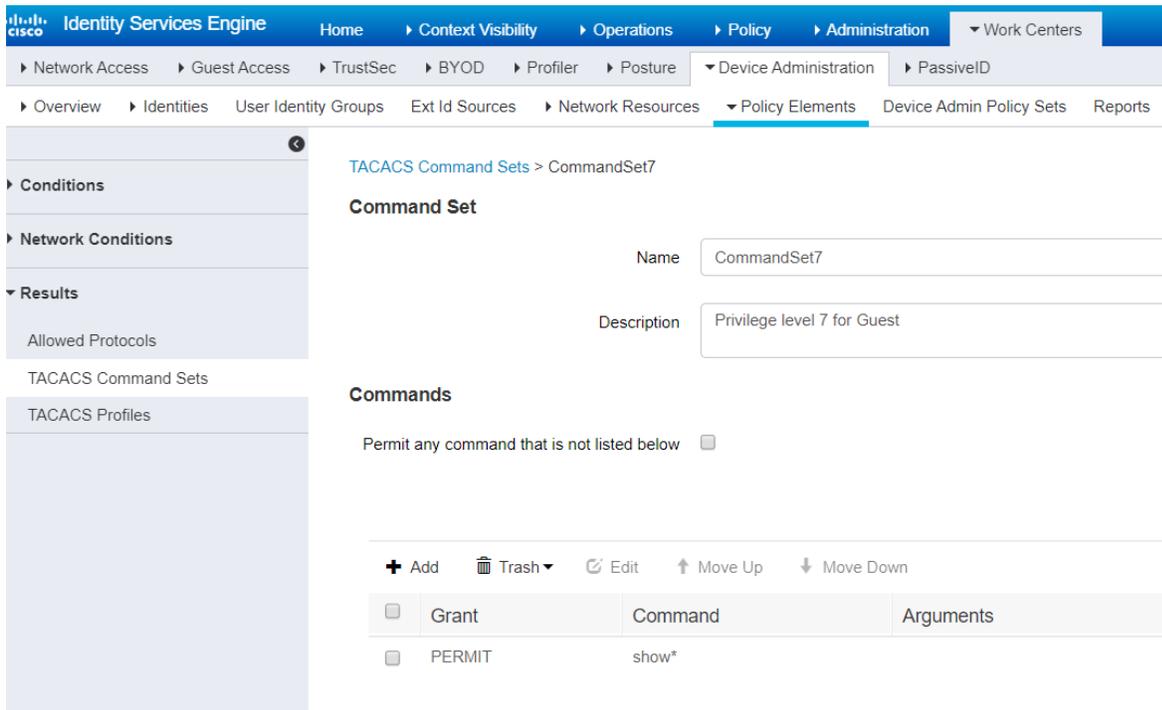
Grant	Command	Arguments
No data found.		

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*:



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: TACACS Command Sets > CommandSet7. The page is titled "Command Set" and contains the following fields:

- Name:** CommandSet7
- Description:** Privilege level 7 for Guest

Below the fields is a section for "Commands" with a checkbox "Permit any command that is not listed below" which is unchecked. At the bottom, there is a table with columns for "Grant", "Command", and "Arguments".

Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	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:

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

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: VnPro@123

Re-Enter Password: VnPro@123

* Login Password: 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:

Password Type: Internal Users

Password: VnPro@123

Re-Enter Password: VnPro@123

* Login Password: Enable Password:

User Information | Account Options | Account Disable Policy

User Groups

Group_Admin

Submit Cancel

▼ User Groups

Kết quả:

The screenshot shows the 'Network Access Users' page in the Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access Users. The page title is 'Network Access Users'. On the left, there is a sidebar with 'Users' and 'Latest Manual Network Scan Results'. The main content area has a toolbar with 'Edit', '+ Add', 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate'. Below the toolbar is a table with columns: Status, Name, De..., F., Last Na..., E..., and User Identity Groups. The table contains two rows: one for 'adminvnpro' with status 'Enabled' and group 'Group_Admin', and one for 'guest' with status 'Enabled' and group 'Group_Guest'.

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

The screenshot shows the 'Device Admin Policy Sets' page in the Identity Services Engine. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets. The page title is 'Device Admin Policy Sets'. The main content area has a search bar and a table with columns: Status, Policy Set Name, Description, and Conditions. The table contains two rows: one for 'Policy for Tacacs' with status 'Enabled' and a plus sign in the Conditions column, and one for 'Default' with status 'Enabled' and description 'Tacacs Default policy set'.

Policy Sets **1**

	Status	Policy Set Name	Description	Conditions
<input type="button" value="+"/>	<input checked="" type="checkbox"/>	Policy for Tacacs 2 <i>Đặt tên cho policy</i>		<input checked="" type="checkbox"/> 3
<input type="button" value="✎"/>	<input checked="" type="checkbox"/>	Default	Tacacs Default policy set	

Tạo policy như sau:

idio

1. Click vào chọn **DEVICE: Device Type**

Editor

Click to add an attribute

Equals Attribute value

2. Click vào chọn **All Device Types**

3

New AND OR

Sau khi click “AND” ta chọn “New” và thiết lập như sau:

DEVICE: Device Type

Equals All Device Types

Network Access: Protocol

Equals TACACS+

AND

New AND OR

New AND OR

Set to 'Is not'

Duplicate Save

Close Use

Sau đó bấm “Use”, ta được kết quả:

Policy Sets

Click vào chọn "Default Device Admin"

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

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	0		
Default Device Admin	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**:

Authorization Policy (2)

	Status	Rule Name	Conditions
		Admin Privilege 15	
		Default	

1 (points to Add icon)
2 Đặt tên (points to Rule Name)
3 (points to Add icon in Conditions column)

Cấu hình conditions như sau:

Conditions Studio

Library

Search by Name

- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- Network_Access_Authentication_Passed

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	Results	
				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**:

IdentityGroup Name

Equals

Set to 'Is not' Duplicate Save

+ New AND OR

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
	✔	Guest Privilege 7	IdentityGroup Name EQUALS User Identity Groups:Group_Guest	<input type="text" value="CommandSet7"/>	<input type="text" value="Shell 7"/>		⚙
	✔	Admin Privilege 15	IdentityGroup Name EQUALS User Identity Groups:Group_Admin	<input type="text" value="CommandSet15"/>	<input type="text" value="Shell 15"/>	0	⚙
	✔	Default		<input type="text" value="DenyAllCommands"/>	<input type="text" value="Deny All Shell Profile"/>	0	⚙

Reset Save

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:

```
C:\Windows\system32\cmd.exe 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:

```
Ctrl. Te net 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:

```
Router(config)#privilege exec level 7 show
Router(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**:

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

```
C:\> 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.



CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P. Thanh Mỹ Tây, Tp. Hồ Chí Minh
ĐT: (028) 35124257 | **Hotline:** 0933427079 **Email:** vnpro@vnpro.org
