Assignment -8

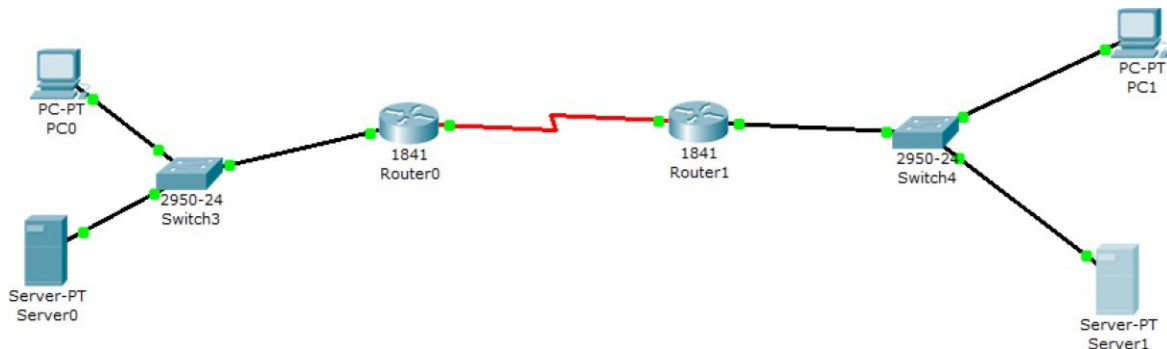## Performing an Initial Switch Configuration

David Bates

A. Topology Diagram

B. Objectives

➢ Perform an initial configuration of a Cisco Catalyst 2950 switch.

C. Tools, Commands & Settings

In this activity, you will configure these settings on the customer Cisco Catalyst 2950 switch:

➢ Host name
➢ Console password
➢ vty password
➢ Privileged EXEC mode password
➢ Privileged EXEC mode secret
➢ IP address on VLAN1 interface
➢ Default gateway

D. Implementations

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2950 switch.

b. Set the host name on the switch to **<Your Last Name>** using these commands.

Switch>**enable**
Switch#**configure terminal**

Switch(config)#**hostname <Your Last Name>**

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as <**your first name**>.

<Your Last Name>(config)#**enable password <your first name>**.

b. From global configuration mode, configure the secret as **cisco123**.

<Your Last Name>(config)#**enable secret cisco123**

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to configure the console line.

<Your Last Name>(config)#**line console 0**

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

<Your Last Name>(config-line)#**password cisco**
<Your Last Name>(config-line)#**login**
<Your Last Name>(config-line)#**exit**

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

<Your Last Name>(config)#**line vty 0 15**

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

<Your Last Name>(config-line)#**password cisco**
<Your Last Name>(config-line)#**login**
<Your Last Name>(config-line)#**exit**

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

<Your Last Name>(config)#**interface vlan 1**
<Your Last Name>(config-if)#**ip address 192.168.1.5 255.255.255.0**
<Your Last Name>(config-if)#**no shutdown**
<Your Last Name>(config-if)#**exit**

Step 6: Configure the default gateway.

    a.   From global configuration mode, assign the default gateway to 192.168.1.1.

            <Your Last Name>(config)#**ip default-gateway 192.168.1.1**

Reflection

a.   What is the significance of assigning the IP address to the VLAN1 interface instead of any of the Fast Ethernet interfaces?

b.   What command is necessary to enforce password authentication on the console and vty lines?
<Your Last Name>(config)#**line vty 0 15**

c.   How many gigabit ports are available on the Cisco Catalyst 2950 switch that you used in the activity?
24

E. Router Configurations Objectives

     •   Configure the router host name.

     •   Configure passwords.

     •   Configure banner messages.

     •   Verify the router configuration.

Step 1: Configure the router host name.

    a.   On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco 1841 ISR.

Set the host name on the router to **CustomerRouter** by using these commands.

        Router>**enable**
        Router#**configure terminal**
        Router(config)#**hostname CustomerRouter**

Step 2: Configure the privileged mode and secret passwords.

    a.   In global configuration mode, set the password to **cisco**.

        CustomerRouter(config)#**enable password cisco**

Set an encrypted privileged password to **cisco123** using the **secret** command.

        CustomerRouter(config)#**enable secret cisco123**

Step 3: Configure the console password.

    a.   In global configuration mode, switch to line configuration mode to specify the console line.

        CustomerRouter(config)#**line console 0**

Set the password to **cisco123**, require that the password be entered at login, and then exit line configuration mode.

CustomerRouter(config-line)#**password cisco123**
CustomerRouter(config-line)#**login**
CustomerRouter(config-line)#**exit**
CustomerRouter(config)#

Step 4: Configure the vty password to allow Telnet access to the router.

> a. In global configuration mode, switch to line configuration mode to specify the vty lines.

> CustomerRouter(config)#**line vty 0 4**

Set the password to **cisco123**, require that the password be entered at login, exit line configuration mode, and then **exit** the configuration session.

> CustomerRouter(config-line)#**password cisco123**
> CustomerRouter(config-line)#**login**
> CustomerRouter(config-line)#**exit**
> CustomerRouter(config)#

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

> a. Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the **show running-config** command.

> To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

> CustomerRouter(config)#**service password-encryption**

> Use the **show running-config** command again to verify that the passwords are encrypted.

To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

> CustomerRouter(config)#**banner motd $Authorized Access Only!$**

Test the banner and passwords. Log out of the router by typing the **exit** command twice. The banner displays before the prompt for a password. Enter the password to log back into the router.

You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the router pauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the **enable** command is mistyped.

> CustomerRouter>**emable**
> Translating "emable"...domain server (255.255.255.255)

> To prevent this from happening, use the following command to stop all DNS lookups from the router CLI.

> CustomerRouter(config)#**no ip domain-lookup**

Save the running configuration to the startup configuration.

> CustomerRouter(config)#**end**
> CustomerRouter#**copy run start**

Step 6: Verify the configuration.

    a.   Log out of your terminal session with the Cisco 1841 customer router.

    b.   Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.

    c.   Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.

    d.   Click the **Check Results** button at the bottom of this instruction window to check your work.

Reflection

Which Cisco IOS CLI commands did you use most?
CustomerRouter(config-line)#**password**
CustomerRouter(config-line)#**exit**
How can you make the customer router passwords more secure?
You can do this by creating an encrypted password and only accessable by certain people/users

➢ Adding routes using the command :
      o ip route 0.0.0.0 0.0.0.0 192.168.1.2

      in class you had said you did not need a full on lab report for this so I will just hand in the lab sheet with the questions finished
      here is proof that the lab was done: