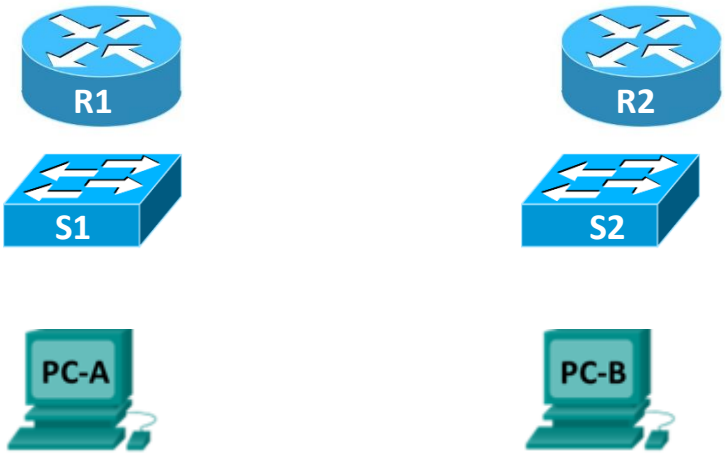
Lab – Password Recovery on a Cisco Router & Switch

Topology



Objectives

Part 1: Configure Console Passwords on Router & Switch

Part 2: Perform Password Recovery on Router

Part 3: Perform Password Recovery on Switch

Background / Scenario

Quite often, in a lab environment, students will need to gain console/privileged access to Cisco routers or switches but are unable to do so due to unknown passwords being preconfigured on the devices. In normal circumstances, students should always erase their configuration at the end of the lab to avoid this issue but occasionally this does not happen.

In this lab, you will recover a password protected router and switch.

This lab will also demonstrate how easy it is to get configuration access to network devices, even if they are password protected, once you have physical access to the devices. This underlines the importance for companies to restrict access to physical communication devices and to implement physical security strategies.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1: Configure Console Passwords on Router & Switch

Working in groups of 2, each student should configure their own switch and router with a password. They should then swap and in part 2 & 3 attempt to get access to the other members devices.

Step 1: Configure Console Password on Switch

a. Assign ***yourStudentNumber*** for the console password and enable login.

Step 2: Configure Console Password on Router

a. Assign ***yourStudentNumber*** for the console password and enable login.

Part 2: Perform Password Recovery on Router

Once each student has configured the console passwords on their devices, they should swap with their group member and attempt to recover their devices.

Step 1: Password Recover Router

a. Ensure the PC is connected to the console port of the router and has the terminal emulation (e.g. TeraTerm or HyperTerminal) open.

b. Use the power switch in order to turn off the router, and then turn the router back on.

c. If using TeraTerm, press the **Alt+B keys** on the terminal keyboard within 60 seconds of power up in order to put the router into ROMmon mode.

   If using HyperTerminal try the Pause key or the Ctrl+Break keys instead.

d. Type **confreg 0x2142** at the rommon 1> prompt in order to boot from Flash. This step bypasses the startup configuration where the passwords are stored.

e. Type **reset** at the rommon 2> prompt

f. The router reboots, but ignores the saved configuration.

g. Type no after each setup question, or press Ctrl-C in order to skip the initial setup procedure.

h. Once at the router prompt, go to global configuration mode.

i. Type **config-register 0x2102**

   Router(config)#config-register 0x2102

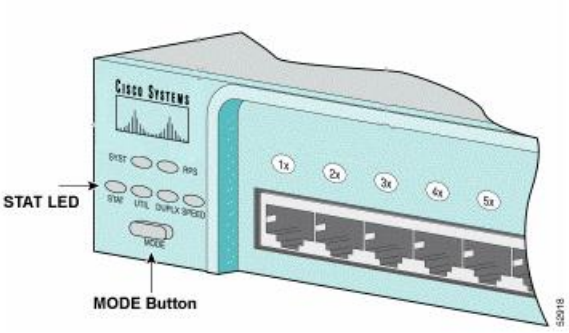
j. Perform a reload on the device and, when asked if you wish to save changes, type **y** for yes. Once the device reloads you should now have full configuration access to it without any passwords.

Part 3: Perform Password Recovery on Switch

Step 1: Password Recover Switch

a. Ensure the PC is connected to the console port of the switch and has the terminal emulation (e.g. TeraTerm or HyperTerminal) open.
b. Unplug the power cable.
c. Power the switch and bring it to the switch: prompt by doing the following:

   1) Hold down the mode button located on the left side of the front panel for a few seconfs, while you reconnect the power cable to the switch



d. Issue the **flash_init** command.

   switch: flash_init

e. Issue the **dir flash:** command.

   switch: dir flash:

f. Type **rename flash:config.text flash:config.old** to rename the configuration file.

   switch: rename flash:config.text flash:config.old

g. Issue the **boot** command to boot the system

   switch: boot

h. Enter "n" at the prompt to abort the initial configuration dialog.
i. At the switch prompt, enter enable mode.
j. Type **rename flash:config.old flash:config.text** to rename the configuration file with its original name.

   Switch#rename flash:config.old flash:config.text

k. Copy the configuration file into memory

   Switch#**copy flash:config.text system:running-config**

l. Perform a reload on the device and, when asked if you wish to save changes, type **y** for yes. Once the device reloads you should now have full configuration access to it without any passwords.