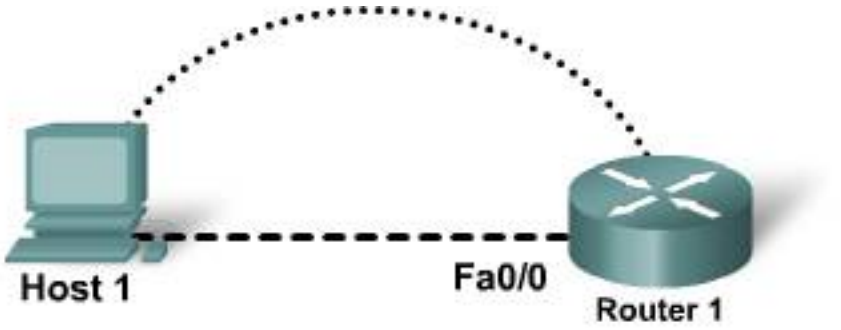
Lab 1.4.6A Gaining Physical Access to the Network

Topology 1



Device Designation	Device Name	Fast Ethernet Address	Subnet Mask
R1	FC-CPE-1	10.0.0.1	255.255.255.0
PC	PC1	10.0.0.254	255.255.255.0

Objectives

- Gain access to a router with unknown login and privileged mode passwords.
- Demonstrate the necessity and importance of physical security for network devices.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Implement basic router security.
- Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats.
- Explain general methods to mitigate common security threats to network devices, hosts, and applications.
- Describe the functions of common security appliances and applications.
- Describe recommended security practices, including initial steps to secure network devices.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

_____

_____

_____

How is an understanding of network device access useful in network administration?

_____

_____

_____

How will a network administrator know if the device's physical access is configured correctly?

_____

_____

_____

Background / Preparation

This lab demonstrates that physical access is required to access and change the password of Cisco routers and switches. At first, an attempt to telnet to the router is made by trying to log in by guessing the password. When this proves unsuccessful, physical access to the console port on the router is made so that the passwords can be changed and control of the router is established. This demonstrates why it is of critical importance that routers and switches have physical security to prevent unauthorized access, in addition to strong password protection.

When a console connection is made, the following principles apply to the process of accessing and changing the passwords of a router:

- Router passwords are in the startup-configuration file stored in NVRAM. The router boot sequence is changed so that it starts without loading the configuration. When running without the startup-configuration loaded, the router can be reconfigured with new, known passwords.
- A memory location in NVRAM, called the configuration register, holds a binary value that determines the router startup sequence. The configuration register value needs to be changed so that the router boots but does not load the startup-configuration. When the passwords are changed, the configuration register is reset to a value that loads the changed startup-configuration when the router next powers on.

Task 1: Access and Change the Router Passwords

Step 1: Attempt login to the router

NOTE: If the PC used in this lab is also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so these can be restored at the conclusion of the lab.

a. Referring to the Topology 1, connect the host PC NIC Ethernet port to the router Fa0/0 Ethernet port using a crossover cable. Ensure that power has been applied to both the host computer and router.

b. Using the given preconfigured topology, attempt to telnet to the router from the PC command line.

Which IP address is used to telnet to the router? _____

What does the message-of-the-day display?

_____

_____

How many login attempts are allowed? _____

What message is displayed to indicate failure of the login attempts?

_____

c. When this attempt at remote login fails, establish a direct physical connection to the router by making the necessary console connections between the PC and router. Then establish a terminal session using HyperTerminal or TeraTerm.

What does the message-of-the-day display?

_____

_____

Attempt to log in by guessing the password.

How many login attempts are allowed? _____

What message is displayed to indicate failure of the log-in attempts?

_____

The configuration register needs to be changed so that the startup-configuration is not loaded. Normally, this is this done from the global configuration mode, but because you cannot log in at all, the boot process must first be interrupted so that the change can be made in the ROM Monitor mode.

Step 2: Enter the ROM Monitor mode

ROM Monitor mode (ROMMON) is a limited command-line environment used for special purposes, such as low-level troubleshooting and debugging. ROMMON mode is invoked when a Break key sequence sent to the console port interrupts the router boot process. This can only be done via the physical console connection.

The actual Break key sequence depends on the terminal program used:

- With HyperTerminal, the key combination is Ctrl+Break.
- For TeraTerm, it is Alt+b.

The list of standard break key sequences is available at http://www.cisco.com/warp/public/701/61.pdf

a. To enter ROM Monitor mode, turn the router off, wait a few seconds, and turn it back on.

b. When the router starts displaying "`System Bootstrap, Version` …" on the terminal screen, press the **Ctrl** key and the **Break** key together if using HyperTerminal, or the **Alt** key and the **b** key together if using TeraTerm.

The router will boot in ROM monitor mode. Depending on the router hardware, one of several prompts such as "**`rommon 1 >`**" or simply "**`>`**" may show.

Example output may be similar to:

```
Router>System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
####################################
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Step 3: Examine the ROM Monitor mode help

Enter **?** at the prompt. The output should be similar to this:


```
rommon 1 > ?
alias       set and display aliases command
boot        boot up an external process
break       set/show/clear the breakpoint
confreg     configuration register utility
context     display the context of a loaded image
dev         list the device table
dir         list files in file system
dis         display instruction stream
help        monitor builtin command help
history     monitor command history
meminfo     main memory information
repeat      repeat a monitor command
reset       system reset
set         display the monitor variables
sysret      print out info from last system return
tftpdnld    tftp image download
xmodem      x/ymodem image download
```

Step 4: Change the configuration register setting to boot without loading configuration file

From the ROM Monitor mode, enter **confreg 0x2142** to change the config-register.

```
rommon 2 > confreg 0x2142
```

NOTE: The ROMMON prompt increments when a command is issued – this is normal behavior. The increment does not mean a change of mode. The same ROMMON commands are still available.

"**0x**" (zero- x) denotes that 2142 is a hexadecimal value. What is this value in binary?

_____

Step 5: Restart router

a. From the ROM Monitor mode, enter **reset**, or power cycle the router.

```
rommon 3 > reset
```

Due to the new configuration register setting, the router will not load the configuration file. After restarting, the system prompts:

```
"Would you like to enter the initial configuration dialog? [yes/no]:"
```

b. Enter **no** and press **Enter**.

Step 6: Enter Privileged EXEC mode and view and change passwords

The router is now running without a loaded configuration file.

a. At the user mode prompt `Router>`, enter **enable** and press **Enter** to go to the privileged mode without a password.

b. Use the command **copy startup-config running-config** to restore the existing configuration. Because the user is already in privileged EXEC, no password is needed.

c. Enter **show running-config** to display the configuration details. Note that all the passwords are shown.

What two measures could be taken to prevent the passwords from being readable?

_____

_____

d. If the passwords were not readable, they can be changed. Enter **configure terminal** to enter the global configuration mode.

e. In global configuration mode, use these commands to change the passwords:

```
FC-CPE-1(config)#enable password cisco
FC-CPE-1(config)#line console 0
FC-CPE-1(config-line)#password console
FC-CPE-1(config-line)#login
FC-CPE-1(config-line)#line vty 0 4
FC-CPE-1(config-line)#password telnet
FC-CPE-1(config-line)#login
```

Step 7: Change the configuration register setting to boot and load the configuration file

a. The instructor will provide you with the original configuration register value, most likely 0x2101. While still in the global configuration mode, enter **config-register 0x2101** (or the value provided by your instructor). Press **Enter**.

```
FC-CPE-1(config)#config-register 0x2101
```

b. Use the **Ctrl+z** combination to return to the privileged EXEC mode.

c. Use the **copy running-config startup-config** command to save the new configuration.

d. Before restarting the router, verify the new configuration setting. From the privileged EXEC prompt, enter the **show version** command and press **Enter**.

e. Verify that the last line of the output reads:

```
Configuration register is 0x2142 (will be 0x2101 at next reload).
```

f. Use the **reload** command to restart the router.

Step 8: Verify new password and configuration

a. When the router reloads, log in and change mode using the new passwords.

b. Issue the **no shutdown** command on the fa0/0 interface to bring it up to working status.

FC-CPE-1(config-if)# **no shutdown**

c. Save the running configuration to startup configuration

FC-CPE-1# **copy run start**

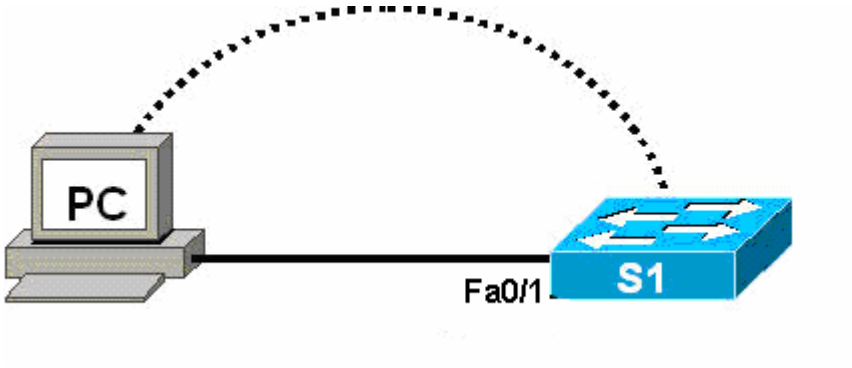
d. Disconnect the console cable and access the router using Telnet from the PC command line.

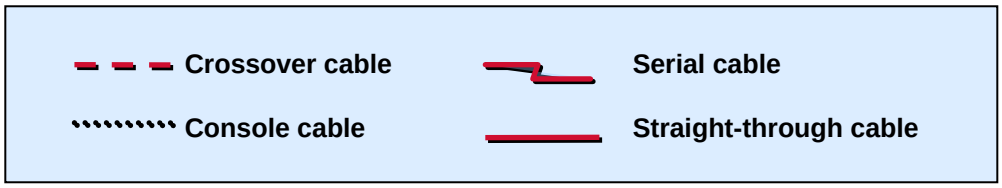
The newly configured passwords will allow a successful login.

Step 9: Clean up

Erase the configurations and reload the router. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Topology 2





Device Designation	Device Name	IP Address	Subnet Mask
S1	FC-ASW-1	10.0.0.2	255.255.255.0
PC	PC1	10.0.0.254	255.255.255.0

Background / Preparation

This task demonstrates that physical access is required to access and change the password of Cisco switches, and again why it is of critical importance that routers and switches also have physical security to prevent unauthorized access.

After unsuccessful attempts to remotely log in, a console connection is made and the following principles are applied to the process of accessing and changing the passwords of a switch:

- Switch passwords are in the configuration file called **config.txt**, which is stored in flash memory. The switch boot sequence is changed so that it starts without loading the configuration.
- When running without the configuration loaded, the switch can be reconfigured with new, known passwords.

Task 2: Access and Change the Switch Passwords

Step 1: Attempt login to the switch

NOTE: If the PC used in this lab is also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so these can be restored at the conclusion of the lab.

a. Referring to the Topology 2, connect the host PC NIC Ethernet port to the switch Fa0/1 Ethernet port using a straight-through cable. Ensure that power has been applied to both the host computer and switch.

b. Using the given preconfigured topology, attempt to telnet to the router from the PC command line.

Which IP address is used to telnet to the router? _____

What does the message-of-the-day display?

_____

_____

How many login attempts are allowed? _____

What message is displayed to indicate failure of the login attempts?

_____

c. When this attempt at remote login fails, establish a direct physical connection to the router by making the necessary console connections between the PC and switch. Then establish a terminal session using HyperTerminal or TeraTerm.

What does the message-of-the-day display?

_____

_____

Attempt to log in by guessing the password.

How many login attempts are allowed? _____

What message is displayed to indicate failure of the log-in attempts?

_____

To prevent the configuration from loading, the **config.txt** file is renamed so that the switch IOS cannot locate and load a valid configuration file. To rename the file, the boot process must be interrupted so that the change can be made in the "**`switch:`**" mode.

Step 2: Enter the `switch:` mode

a. Power off the switch.

b. Locate the MODE button on the front of the switch.

c. Hold down the MODE button on the front of the switch while powering on the switch. Release the MODE button after 10 seconds.

Output similar to the following should be displayed:

```
Base ethernet MAC Address: 00:0a:b7:72:2b:40
Xmodem file system is available.
The password-recovery mechanism is enabled.

The system has been interrupted prior to initializing the
flash files system. The following commands will initialize
the flash files system, and finish loading the operating
system software:

flash_init
load_helper
boot

switch:
```

d. To initialize the file system and finish loading the operating system, enter the following commands at the `switch:` prompt:

```
switch: flash_init
switch: load_helper
```

e. To view the contents of flash memory, enter **`dir flash:`** at the `switch:` prompt.


```
switch: dir flash:
```

NOTE: Do not forget to type the colon (**:**) after the word “flash” in the command **dir flash:**

The file **config.txt** should be seen listed.

f. Enter **rename flash:config.text flash:config.old** to rename the configuration file. This file contains the password definitions.

g. Enter **dir flash:** at the switch: prompt to view the name change.

```
switch: dir flash:
```

Step 3: Restart the switch

a. Enter **boot** to restart the switch.

```
switch: boot
```

The configuration file **coinfig.txt** cannot be located; therefore, the switch boots into Setup mode.

b. Would you like to terminate autoinstall? [Yes]: **Y**

c. Would you like to enter the initial configuration dialog? [yes/no] **N**

Switch>

Step 4: Enter Privileged EXEC mode and view and change passwords

The switch is now running without a loaded configuration file.

a. At the user mode prompt Router>, type **enable** and press **Enter** to go to the privileged mode without a password.

b. Enter **rename flash:config.old flash:config.text** to rename the configuration file with its original name.

```
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]?
Press Enter to confirm file name change.
```

c. Copy the configuration file into RAM.

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?
Press Enter to confirm file name.
```

d. Press **Enter** to accept the default file names.

```
Source filename [config.text]?
Destination filename [running-config]
```

The configuration file is now loaded.

e. Enter **show running-config** to display the configuration details. Note that all the passwords are shown.

What two measures could be taken to prevent the passwords from being readable?

_____

_____

f. If the passwords were not readable they can be changed. Enter **configure terminal** to enter the global configuration mode.

g. Change the unknown passwords.


```
FC-ASW-1#configure terminal
FC-ASW-1(config)#enable password cisco
FC-ASW-1(config)#line console 0
FC-ASW-1(config-line)#password console
FC-ASW-1(config-line)#line vty 0 15
FC-ASW-1(config-line)#password telnet
FC-ASW-1(config-line)#exit
FC-ASW-1(config)#exit
```

Step 5: Save the configuration file

Use the **copy running-config startup-config** command to save the new configuration.

```
FC-ASW-1#copy running-config startup-config
Destination filename [startup-config]?[enter]
Building configuration...
[OK]
FC-ASW-1#
```

Step 6: Verify new password and configuration

Power cycle the switch and verify that the passwords are now functional.

Step 7: Clean up

Erase the configurations and reload the switch. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Task 3: Reflection

Consider the different methods of securing physical access to networking devices such as routers and switches. List how only those people who require access can be identified and how this security can be implemented.

_____

_____

_____

_____

_____

NOTE: It is important to remember that the passwords (console, cisco, class, telnet) used in these labs are for convenience only. These are *not* secure passwords that would be used in production networks.