

Lab: Password Recovery Procedures

Have an instructor, lab assistant, or other student configure a basic configuration with an enable secret password. Perform **copy running-config startup-config** and reload the router.

Step 1 Attempt login to the router

a. Make the necessary console connection and establish a session with the router. Attempt to logon to the router using the enable password **cisco**. You are not able to login.

Step 2 Document the current config-register setting

a. At the user EXEC prompt type **show version**.
b. Record the value displayed for configuration register _____. For example 0x2102.

Step 3 Enter the ROM Monitor mode

a. Turn the router off, wait a few seconds and turn it back on. When the router starts displaying "System Bootstrap, Version ..." on the console screen, send „break signal“ to the router (on TeraTerm press **Alt + B**). 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.

Step 4 Examine the ROM Monitor mode help

a. Type **?** at the prompt.
b. Type **confreg** (on 2600 series router) or **o** (on 2500 series router) at the prompt. You should see the current config-register value.

Step 5 Change the configuration register setting to boot without loading configuration file

a. From the ROM Monitor mode, type **confreg 0x2142** (2600series) or **o/r 0x2142** (2500series) to change the config-register.

```
>confreg 0x2142                >o/r 0x2142
```

Step 6 Restart Router

a. From the ROM Monitor mode, type **reset** (2600series) **i** (2500series) or power cycle the router.

```
>reset                          >i
```

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

"Would you like to enter the initial configuration dialog? [yes]:"

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

Step 7 Enter Privileged EXEC mode and change password

a. Now at the user mode prompt Router>, type **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. Since the user is already in privileged EXEC no password is needed.

c. Type **configure terminal** to enter the global configuration mode.

d. In the global configuration mode type **enable secret class** to change the secret password.

e. While still in the global configuration mode, type **config-register xxxxxxxx**. xxxxxxxx is the original configuration register value recorded in Step 2. Press **Enter**.

- f. Use the **Ctrl z** combination to return to the privileged EXEC mode.
- g. Use the **copy running-config startup-config** command to save the new configuration.
- h. Before restarting the router, verify the new configuration setting. From the privileged EXEC prompt, enter the **show version** command and press **Enter**.
- i. Verify that the last line of the output reads:
Configuration register is 0x2142 (will be 0x2102 at next reload).
- j. Use the **reload** command to restart the router.

Step 8 Verify new password and configuration

- a. When the router reloads the password should be **class**.
Upon completion of the previous steps, logoff by typing **exit**. Turn the router off.

Step 9 Erase your router configuration

If startup-configuration is not empty you have to erase it.

```
Router# erase startup-configuration
```