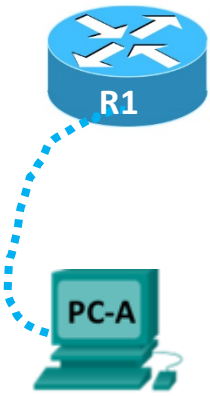
Lab 3a: Password Recovery on a Cisco Router

Topology



Objectives

Part 1: Configure Console Passwords on Router

Part 2: Perform Password Recovery on Router

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. We will use a procedure for resetting the enable password / console password on a Cisco router.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

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.

IMPORTANT:

This underlines the importance for companies to restrict access to physical communication devices and to implement physical security strategies.

Required Resources

- 1 Router between **two** students (Cisco 4321 with Cisco IOS Release 17.3 universal image or comparable)
- 1 PCs (Windows 8, 10, 11 with terminal emulation program, **such as Putty**)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1: Configure Console Password and enable password on Router

Step 1: Pair up with another student for this group activity

Working in groups of 2, students can work together to configure one router with a console and enable password(s).

a. Ensure the PC is connected to the console port of a router and has the terminal emulation (e.g. Putty) open. (Note: Lab Lecturer will assign you a router)

Step 2: Configure Console Password and enable password on Router

a. Boot the router and assign a password of **cisco** as the console password and an **enable** password set to **cisco**.

b. Set a hostname of **R1** on the router.

c. Test these to ensure that these passwords have been set correctly.

d. Reboot the router ensuring to save the configuration. Tip: Use the **reload** command to reboot.

You will prompted asking you the following:

e. Save configuration has been modified. Save? [yes/no]: **yes**

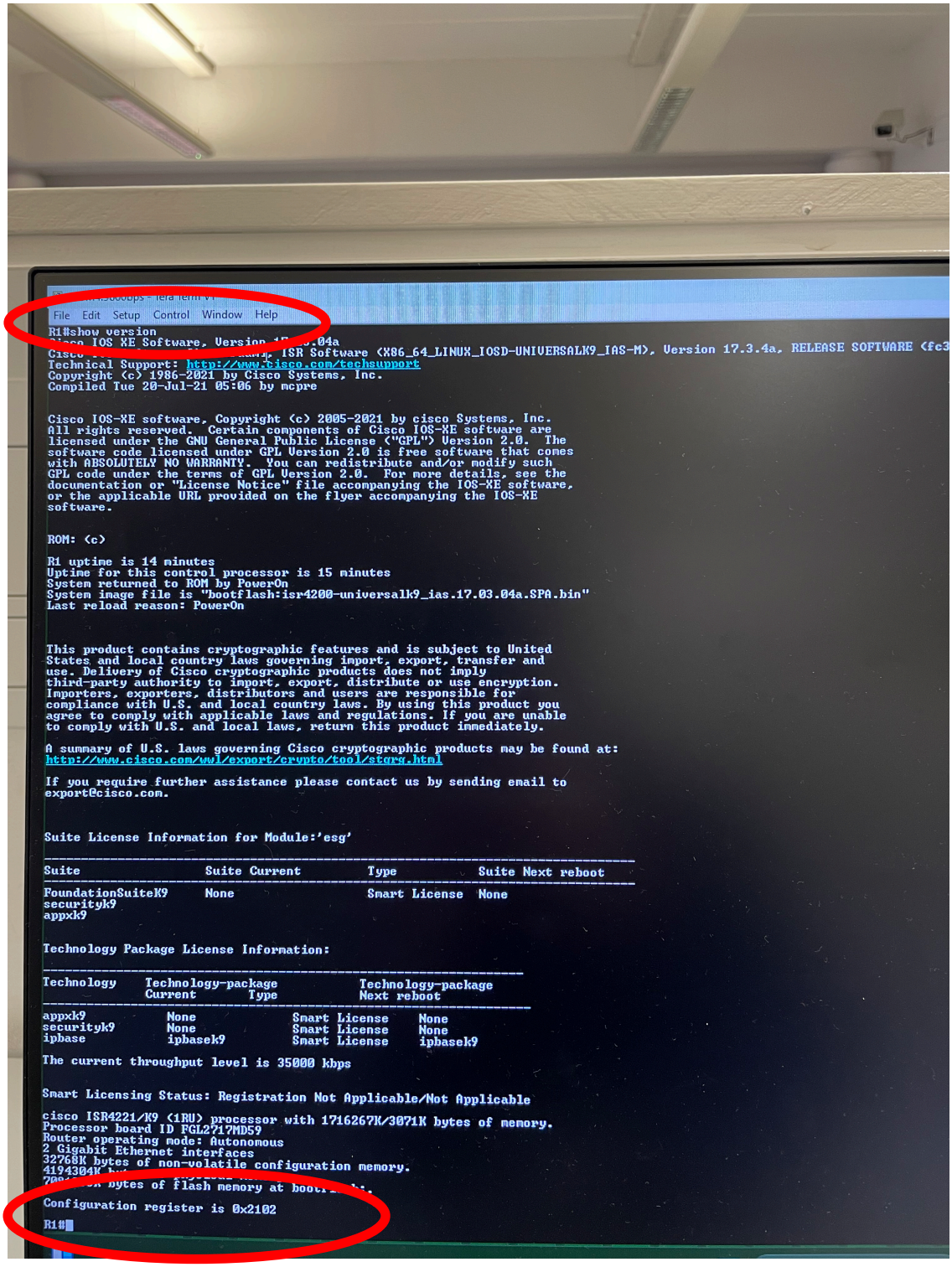
f. Proceed with reload[confirm] ***(Press enter)***

The router should boot with the hostname set to **R1** and also there should be a console password of **cisco** with a enable password of **cisco**.

Test these to ensure this is the case. At this point, if you didn't know these passwords you would be locked out of the router. Enter into privileged mode and check the value of the **configuration register** as detailed below.

g. Execute the command **show version**. You will need to be in privileged mode of the router.

Note the value of the configuration register at the end of the output (note: **you will need to press space a number of times to see this).**



The configuration register of the router plays a vital role in the process of password recovery.

As from the output above, the configuration register can viewed with the **show version** command. **The last line of output tells you what the configuration register is set to.**

The configuration register is a 16 bit field stored in NVRAM. Bits are represented in hexadecimal.

The two most important configuration register values for us to remember are:

0x2102 – This is the **default** register setting. **Your router should always be set to this value during normal operation of the device.**

0x2142 – This is the setting **used during the password recovery procedure.** It causes the router to boot while **ignoring the contents of NVRAM**. It does not erase or modify the contents of the NVRAM; **it just tells the router to ignore the contents of NVRAM** (which includes the startup-config file) during bootup.

Note: Once you complete the password recovery procedure, you will reset the configuration register back to 0x2102.

Part 2: Perform Password Recovery on Router

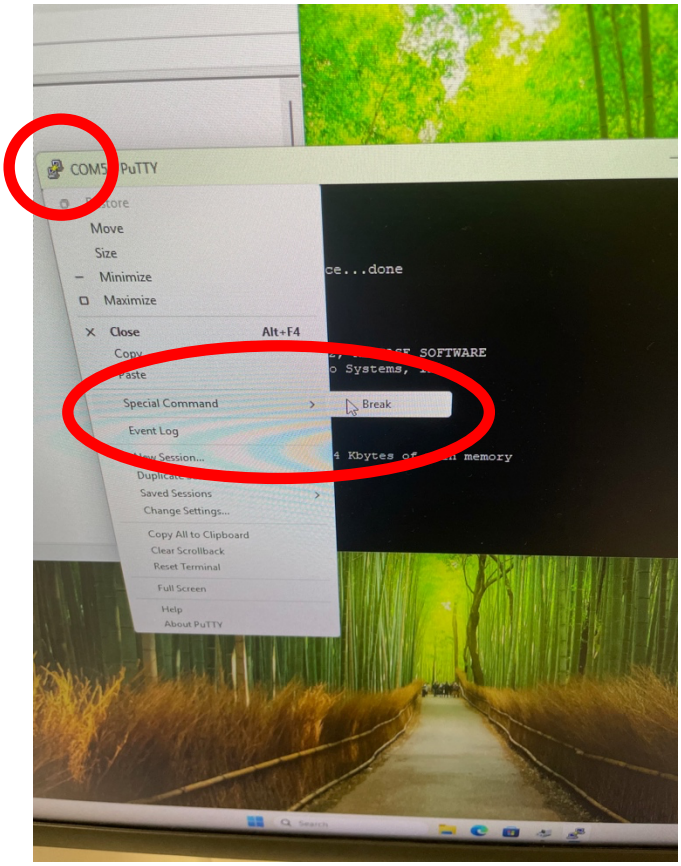
Once each group of students has configured the console & enable passwords on their device, you can proceed onto the following steps.

Step 1: Password Recover Router

a. Again, ensuring the PC is connected to the console port of the router and has the terminal emulation (e.g. Putty) open.

b. One group member, can press the power switch to turn off the router, and then turn the router back **on**. The other team member can be at the Putty window ready to perform step c below.

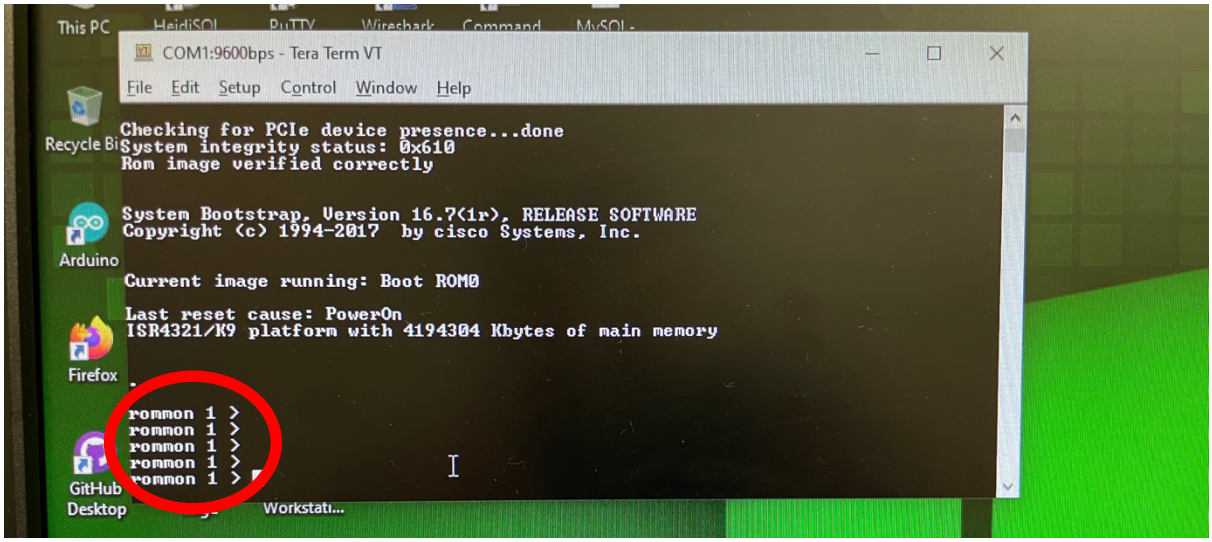
c. **Using Putty**, you will see output on the screen(router is booting e.g. Initializing Hardware), use your mouse to select the icon in the top left (to bring up the menu) and then select **Special Command-Break (as shown below)**



This will interrupt the normal boot sequence and bring us into Rommon mode below.

If you don't see the Rommon prompt below, again use the menu to select Special Command-Break until you see the rommon 1> menu (as shown below)

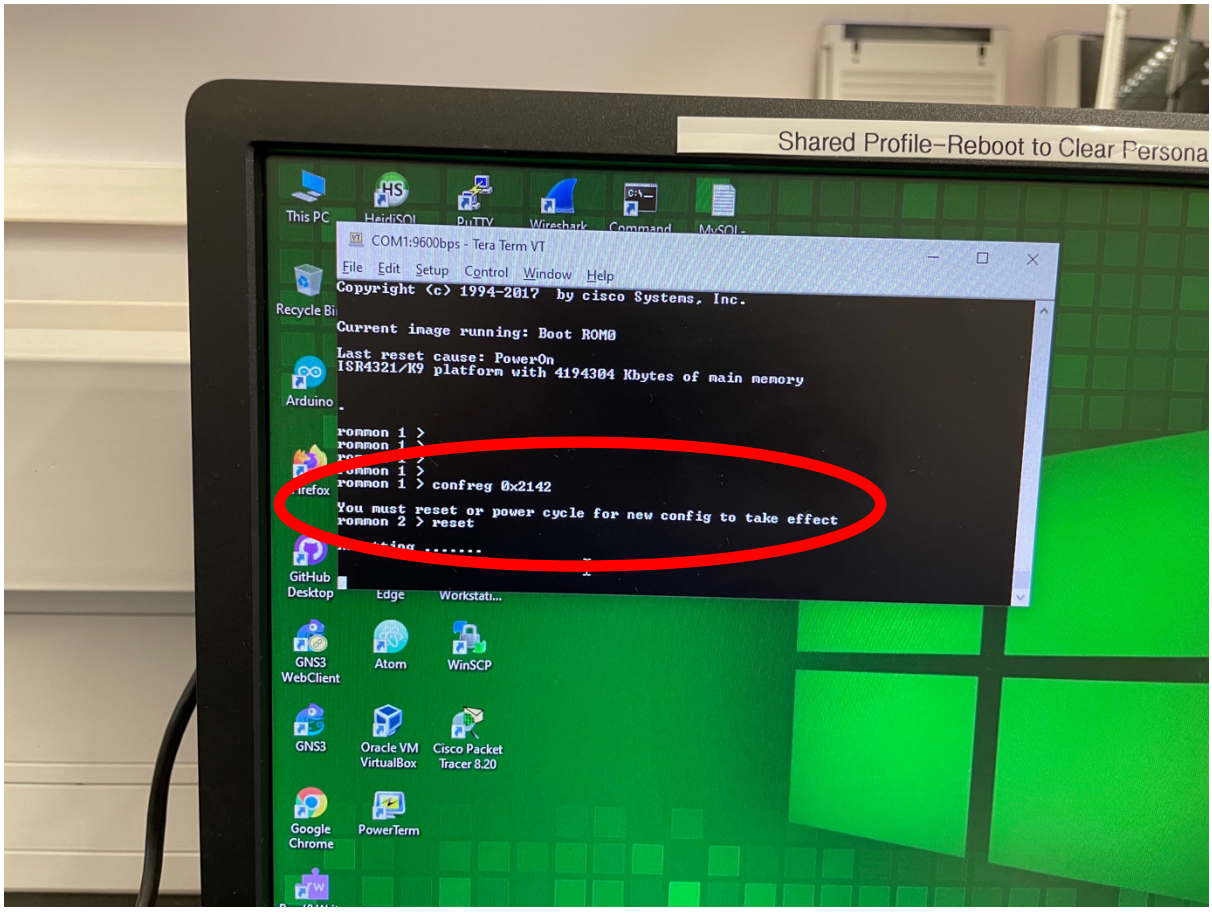
d. Note: **Rommon** mode will be indicated when the router shows the rommon prompt (as shown below)



You will need to access the ROMMON interface to instruct the router to ignore the startup configuration when booting.

e. 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. i.e. changing the configuration register to **0x2142** ignores contents of NVRAM (this ignores start-up configuration.

f. Type **reset** at the rommon 2> prompt (this step **reloads** the router).



The router will now reboot, *but ignores the saved configuration (in NVRAM).*

g. When the router reboots, if you get prompted: Type **no** after each setup question, or press **Ctrl-C** in order to skip the initial setup procedure **(if requested).**

h. Once at the router prompt, go to privileged mode. **Important Note: you will no longer have to type in a console and enable passwords. Notice how the prompt is no longer R1 (it has reverted back to Router)**

i. Type **enable**

j. Lets review the startup-config file.

- ***Router# show* startup-config**
- *Note: notice the hostname in the startup-config file - this should now show as R1 and it will also show the encrypted secret password, along with the unencrypted console password of* ***cisco*** *(that we set earlier).* Now we will merge the startup-config into the running config.
- ***Router# copy* start run**
- ***You will be prompted : Destination filename[running-config]? (press enter)***
- *IMPORTANT Note: the hostname changes to whatever was saved in the startup-config file. For us, the hostname should now show as* ***R1****.*
- *Just as a further note, when you merge the startup-config into the running-config, your interfaces will be in shutdown mode because the no shutdown command is not part of the startup-config file. You must issue the no shutdown command to enable the interfaces****. For us, in this exercise we can ignore this.***

Now we will look at the configuration register again.

- ***Router# show version***
- *Note: Press space to go to the bottom of output to see configuration register. the configuration register shows the value 0x2142. Before we reset this to its default value, we need to change the passwords.*
- ***R1#*conf t**
- ***R1(config)#* enable secret class**
- ***R1(config)#* line con 0**
- ***R1(config-line)#*password cisco**
- ***R1(config-line)#*exit**

Finally we will reset the configuration register using the following command:

- ***R1(config)#* *config-register 0x2102***

This resets the configuration register to its default value (at the next reload).

- ***R1(config)# exit***
- ***R1#* reload**
  - *IMPORTANT: Perform a reload on the device and, when asked if you wish to save changes, type* ***yes*** *to confirm. Once the device reloads you should now have full configuration access to it with* ***new updated*** *passwords – enable password is set to class and console password is set to cisco.*

Note: You may need to press **enter** to proceed with reload.

The router should reload.

Note the routers prompt – it is now back to R1.

You should now have full configuration access with the new passwords you set above.

Use the **show version** command to see that the configuration register is set to **0x2102**.

Enter your new console password **cisco** and then enter privileged mode using your new password of **class**.

How do you verify that password recovery was successful?

Use the **show running-config** command and displaying and confirming the password change.

Lastly,

Now that you have booted your router, ***we still have configuration (including passwords) on our router, we should erase it (for the next groups following us!).***

To clear the configuration, issue the **erase startup-config** command as outlined below. Confirm your intentions when prompted, and answer "no" if you are asked to save changes. The result should look something like this:

```
R1> enable

Router# erase startup-config
```

Erasing the nvram filesystem will remove all files! Continue?

[confirm] ***(press enter)***

[OK]

Erase of nvram: complete

When the prompt returns, issue the **reload** command. Confirm your intentions when prompted.

```
R1# reload
```

Proceed with reload [confirm] *(press enter)*

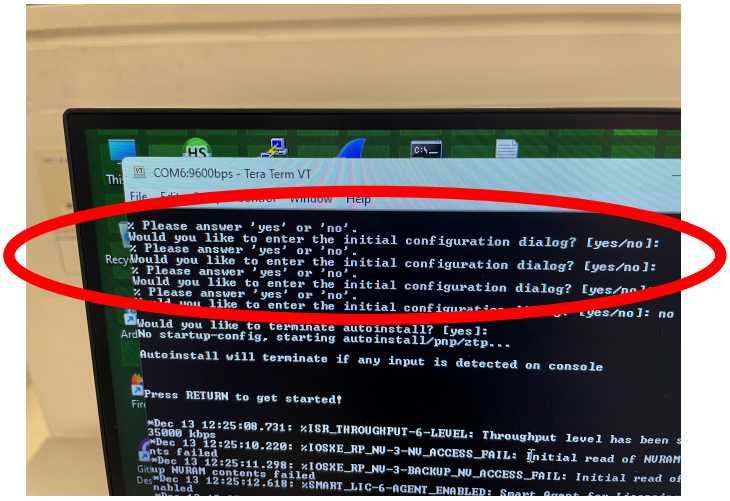
If you get the following:

System config has been modified. Save? **No**

Proceed with reload [Press enter]

The router will take a few minutes to reboot.

Once the router boots, it should show the following prompt:



Well done!

Open Lab 3a - Password Recovery on Cisco Router (Hands-on activity) - QUESTIONS 2% (2025)

This is located within Lecture 3 section of the WAN Brightspace page and attempt each question. For the last question, you will need to show evidence of your work as documented below.

IMPORTANT: Please call over your lecturer to ensure you demonstrate your work. Failure to do so will mean you are not awarded % marks for this part of the lab.

Note: be prepared to run the command: **show version**

This should indicate the configuration register value of 0x2102. This tells the router to load the IOS from flash memory and then load the start-up configuration from the NVRAM if present. If no operating system is found, the router will boot to ROMMON. The 0x2102 setting is for normal router operation.

Now go onto Lab 3b in the lab.

You will also need to open the Brightspace quiz - Lab 3b - Configure Extended ACLs - QUESTIONS 1% (2025).

Please note for your own information these are generic instructions for password recovery for Cisco Routers (other models may differ).

Further note: if you were using Tera Term the following would be the procedure to interrupt normal boot sequence of router:

> Note, if were using TeraTerm, press the **Alt+B keys** (press together – don't be afraid to tap these keys numerous times!) on the terminal keyboard within 60 seconds of power up in order to put the router into ROMmon mode.