

Name: REIMARC G. CORPUZ

Date: 3/3/2023

Course & Section: BSCPE 3 IE

Score: _____

Basic Router Configuration, Command Modes and Command-Line Fundamentals

Objectives

Upon completion of this laboratory exercise, the student will be able to

- Establish connection to a cisco router using PuTTY and SecureCRT.
- Use the help facility of the router.
- Know the different modes like User Mode (User Exec), Privileged Mode (Privilege Exec) and Global Configuration Mode.
- Change the Hostname of the Router, Set Passwords, Configure Banners, Save Changes and Verify Basic Configuration.

Equipment

PC
Cisco Router
Console Cable

Introduction

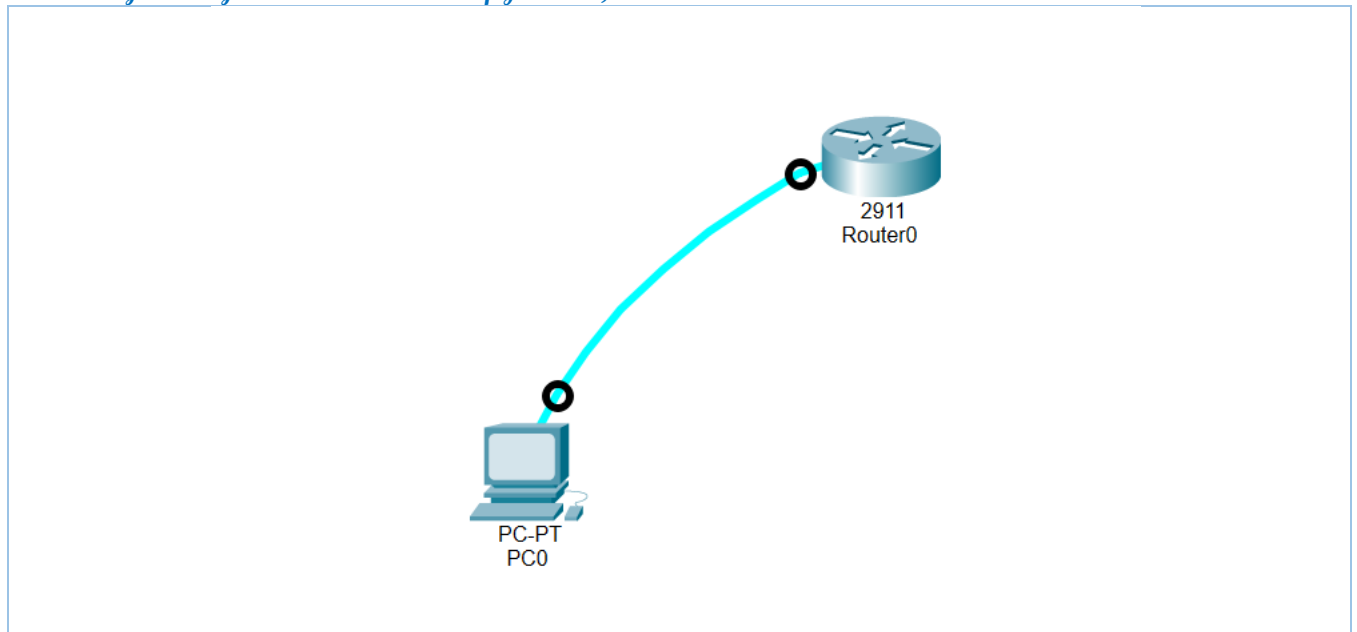
Router is a device that has many hardware components like a computer. Its primary function is to determine the best path to send packets and forward packets to their destination.

The first thing a network engineer must learn the basic router configuration. But before we should know how to set-up a connection to configure the router. We also need to know importance of the help facility. A router has different modes and we should know what command we can use under each mode. Lastly we should the basic configurations kike changing hostnames, adding passwords, configuring banners, saving router configurations and verify it.

Establishing Connection to a Cisco Router

1. Get a console cable
2. Plug the one end into your pc
3. Plug the other end into the console port of the router

Task #1 Draw the set-up of the PC to router using the console cable



4. Open a terminal program

- tera term
- securecrt
- hyperterm
- minicom
- PuTTY

5. If you are using SecureCRT, Set it to connect via COM port with as shown in Figure 1 and set the following parameters

- Baud Rate: 9600
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

If you are using Putty go to step 6.



Figure 1. Set-up Connection using SecureCRT

6. If you are using SecureCRT click connect and if you are using Putty click the radio button "Serial" and click "Open"

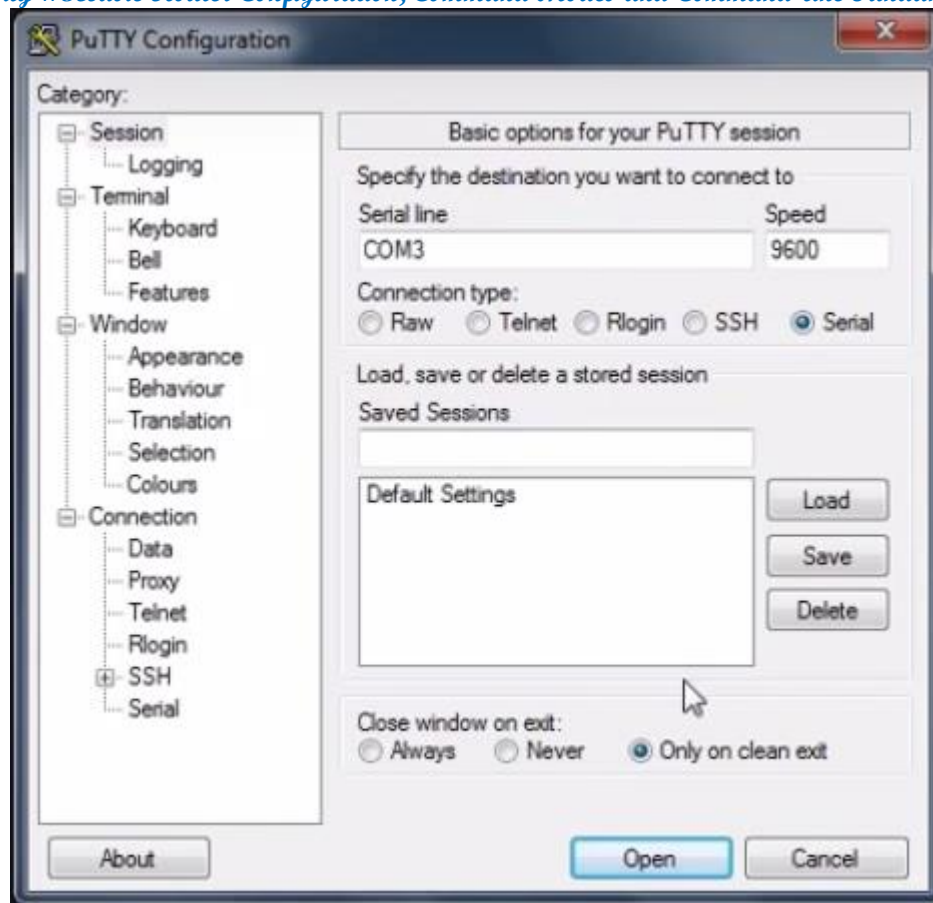
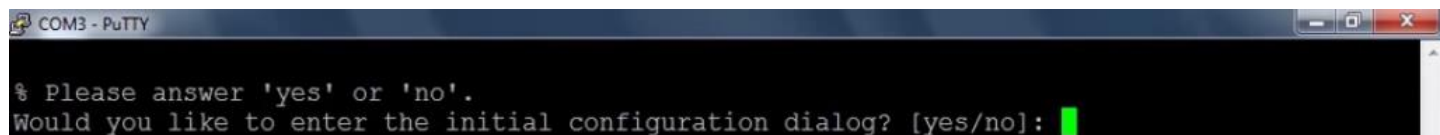


Figure 2. Set-up connection using PuTTY

7. The router will take some moments to complete its booting process. So wait until this message come out.

If the router ask for a password type “cisco”.



8. Type “No” and the following message will display.

```
COM3 - PuTTY

% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

*Jul 17 14:40:57.967: SERVICE_MODULE(Serial0/0/0): self test finished: Passed
*Jul 17 14:41:00.731: SERVICE_MODULE(Serial0/1/0): self test finished: Passed
*Jul 17 14:41:05.011: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
*Jul 17 14:41:05.011: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to down
*Jul 17 14:41:06.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
*Jul 17 14:41:06.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
*Jul 17 14:41:07.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Jul 17 14:41:07.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Jul 17 14:41:10.995: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Jul 17 14:48:31.919: %IP-5-WEBINST_KILL: Terminating DNS process
*Jul 17 14:48:32.599: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Jul 17 14:48:32.599: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
```

9. After all the interfaces are initialize, the prompts shows “Router”.

```
COM3 - PuTTY

Router> 
```

Using the help facility

1. In order to use the help facility we can type the symbol “?”.
Router>? [Enter]

Task #2 List all the commands after the router response.

<1-99>	Session number to resume
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
logout	Exit from the EXEC

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

ping	Send echo messages
resume	Resume an active network connection
show	Show running system information
ssh	Open a secure shell client connection
telnet	Open a telnet connection
terminal	Set terminal line parameters
tracert	Trace route destination

2. Now type “enable” then press “enter” then type “?” again.

Router>enable [Enter]

Router#? [Enter]

Task #3 List 12 of the command after the router response. To look for all the router responses just keep pressing enter.

auto	Exec level Automation
clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode
erase	Erase a filesystem
copy	Copy from one file to another
debug	Debugging functions
undebug	Disable debugging functions
mkdir	Create a new directory
dir	List files on a filesystem
write	Write running configuration to memory, network, or terminal
rmdir	Remove existing directory

3. Type the word “con?”, then press “enter”

Router#con? [Enter]

Task #4 List all the commands after the response.

configure	
connect	

4. To do a certain task sometimes it requires two or more commands, you can use question mark to determine the possible commands you can use with the previous command. Type “configure” then “?”

Router#configure ?

Task #5 List all the next command you can use after the word configure.

terminal	
----------	--

memory	
network	

Note: If the router response is only
 it only means that there is no other possible command you can use with the previous.

Entering different modes

The Cisco IOS command-line interface is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations.

When you start a session on a router, you generally begin in *user EXEC mode*, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration of the router, such as determining the router status.

In order to have access to all commands, you must enter *privileged EXEC mode*, which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. In privileged EXEC mode, you can enter any EXEC command, as the privileged EXEC mode is a superset of the user EXEC mode commands.

Most EXEC mode commands are one-time commands, such as **show** or **more** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the router.

From privileged EXEC mode, you can enter *global configuration mode*. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode.

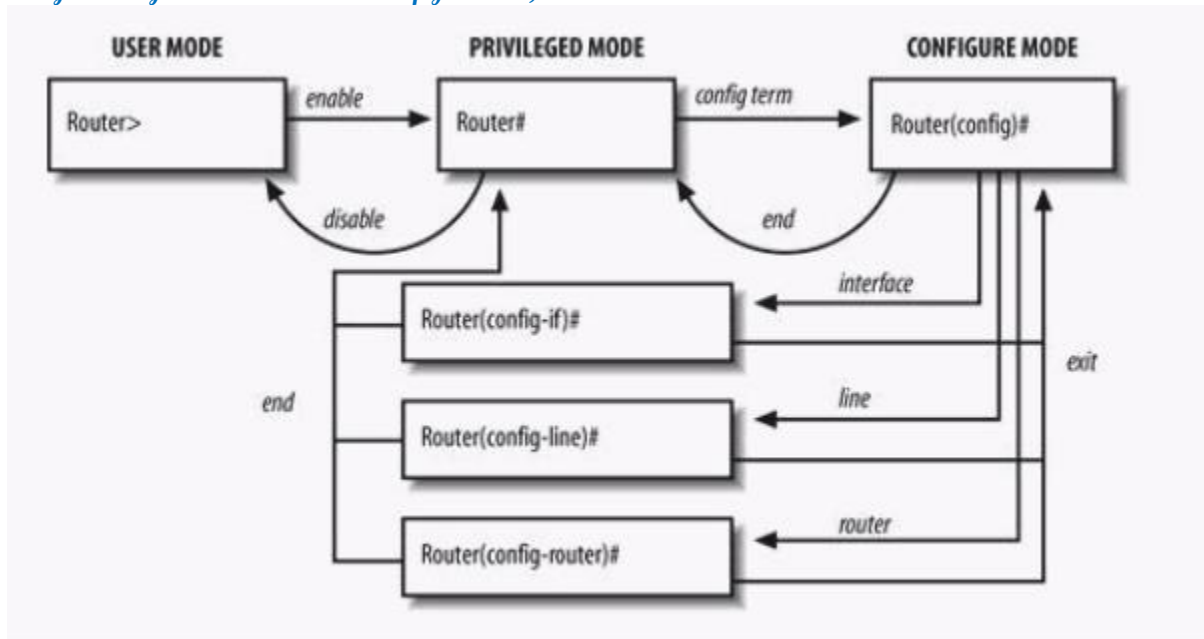


Figure 3. Summary on how to change from one mode to another.

Task #6 Answer the following questions

- What is the command in order to change from user mode to privileged mode?
enable
- What is the command in order to change from privilege mode to user mode?
disable
- What is the command in order to change from privilege mode to global configuration mode? config term
- What is the command in order to change from global configuration mode to privilege mode? end
- What is the command in order to change from sub-modes to global configuration mode? exit
- What is the command in order to change from sub-modes to privilege mode?
end

Basic Commands in Configuring a Cisco Router

Configuring the Router Hostname

Router can have their names like us. A hostname must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer.

Example #1 PH-MNL-MDF-R1, this can be interpreted as Router in Philippines, Manila, Main Distribution Frame and Router 1.

Command or Action	Purpose
-------------------	---------

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

Step 1	enable Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Router# configure terminal	Enters global configuration mode.
Step 3	hostname name Router(config)# hostname PH-MNL-MDF-R1	Specifies or modifies the hostname for the network server.
Step 4	Verify that the router prompt displays your new hostname. PH-MNL-MDF-R1 (config)#	—
Step 5	end PH-MNL-MDF-R1# end	(Optional) Returns to privileged EXEC mode.

Configuring the Enable and Enable Secret Passwords

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** command or **enable secret** command. Both commands accomplish the same thing—they allow you to establish an encrypted password that users must enter to access privileged EXEC (enable) mode.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm. Use the **enable password** command only if you boot an older image of the Cisco IOS software or if you boot older boot ROMs that do not recognize the **enable secret** command.

	Command or Action	Purpose
Step 1	enable Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Router# configure terminal	Enters global configuration mode.
Step 3	enable password password Router(config)# enable password password1	(Optional) Sets a local password to control access to various privilege levels. We recommend that you perform this step only if you boot an older image of the Cisco IOS software or if you boot older boot ROMs that do not recognize the enable secret command.
Step 4	enable secret password Router(config)# enable secret password2	Specifies an additional layer of security over the enable password command. Do not use the same password that you entered in Step 3 .

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

Step 5	end Router(config)# end	Returns to privileged EXEC mode.
Step 6	Exit Router#exit	Return to user Exec mode
Step 7	enable Router> enable	Enables privileged EXEC mode. Verify that your new enable or enable secret password works.
Step 8	Password2 Password: password2	

Configuring the Passwords on console and Telnet

	Command or Action	Purpose
Step 1	enable Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Router# configure terminal	Enters global configuration mode.
Step 3	service password-encryption Router(config)# service password-encryption	Encrypts the password
Step 4	line console 0 or line vty 0 15 Router(config)# line console 0 or Router(config)# line vty 0 15	Configures the console line or telnet and starts the line configuration command collection mode.
Step 5	password password Router(config-line)#password password1	Sets a local password to control access to various privilege levels.

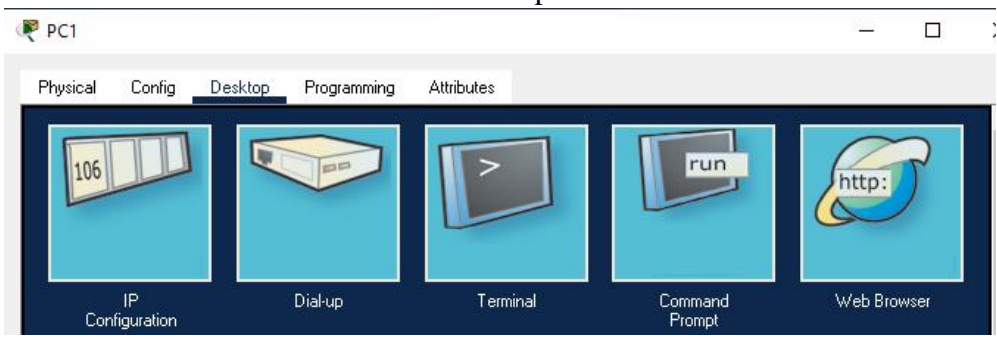
Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

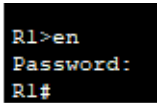
Step 6	exec-timeout <i>minutes</i> [<i>seconds</i>] Router(config-line)# exec-timeout 0 0	Sets the idle privileged EXEC timeout, which is the interval that the privileged EXEC command interpreter waits until user input is detected. The example shows how to specify no timeout. Setting the exec-timeout value to 0 will cause the router to never log out once logged in. This could have security implications if you leave the console without manually logging out using the disable command.
Step 7	Login Router(config)# login	Is a required configuration command to enable password checking at login
Step 8	end Router(config)# end	Returns to privileged EXEC mode.
Step 9	show running-config Router(config)# show running-config	Displays the running configuration file. Verify that you properly configured the idle privileged EXEC timeout.

Configuring the Passwords on Virtual Line using SSH

	Command or Action	Purpose
Step 1	enable Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Router# configure terminal	Enters global configuration mode.
Step 3	hostname <i>name</i> Router(config)#hostname R1	Specifies or modifies the hostname for the network server.
Step 4	username <i>name</i> secret <i>password</i> R1(config)#username Jerwin secret 4321	Create a Username and sets a password SSH requires a username and password
	ip ssh version 2	
	ip domain-name jobmerga.com	Create a Host domain for the Router/Switch
	line vty 0 15 Router(config)# line vty 0 15	Configures the console line or telnet and starts the line configuration command collection mode.

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

	exec-timeout <i>minutes</i> [<i>seconds</i>] R1 (config-line)# exec-timeout 0 0	Sets the idle privileged EXEC timeout, which is the interval that the privileged EXEC command interpreter waits until user input is detected. The example shows how to specify no timeout. Setting the exec-timeout value to 0 will cause the router to never log out once logged in. This could have security implications if you leave the console without manually logging out using the disable command.
Step 5	login local R1 (config-line)#login local	Is a required configuration command to enable password checking at login Local means that it will look for the router's database and find username and its passwords.
Step 6	R1 (config-line)#transport input ssh	Informs the router to allow only SSH connections
Step 7	crypto key generate rsa R1 (config-line)#crypto key generate rsa	Use this command to generate RSA key pairs for your Cisco device (such as a router). RSA keys are generated in pairs--one public RSA key and one private RSA key. If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys
Step 8	Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus: 1024	
Step 9	Click PC1 select PC1 and Select Command Prompt 	
Step 10	ssh -l username ip-address <pre>C:\>ssh -l Jerwin 192.168.0.1 Password: R1></pre>	ssh -L opens a local port and access the device based its username and ip address of the device

Step 11		Type your enable password
---------	---	---------------------------

Configuring a Message-of-the-Day Banner

You can configure a message-of-the-day (MOTD) banner to be displayed on all connected terminals. This banner is displayed at login and is useful for sending messages that affect all network users (such as impending system shutdowns). To do so, use the following command in global configuration mode:

	Command	Purpose
Step 1	banner motd <i>d</i> <i>message d</i> Router(config)# banner motd \$ <i>Warning this is a private network. You are not allowed to access it. \$</i>	Configures the system to display a message-of-the-day banner. The argument <i>d</i> indicates any delimiting character.
Step 2	Router(config)#exit Router(config)#exit	Exit twice to see the banner.

Saving Router Configuration

Saving Configuration Changes

After making all the configurations, you must save the changes to memory so they will not be lost if the system is rebooted. There are two types of configuration files: the running (current operating) configuration and the startup configuration. The running configuration is stored in RAM (volatile); the startup configuration is stored in NVRAM (Non-volatile).

To display the current running configuration, enter the **show running-config** command. Enter the **copy running-config startup-config** command to save the current running configuration to the startup configuration file in NVRAM.

```
Router> enable
Router# copy running-config startup-config
```

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals Screenshots

Make a screenshot that you perform the following

1. Change Hostname

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname PH-MNL-MDF-R1
PH-MNL-MDF-R1(config)#end
PH-MNL-MDF-R1#
%SYS-5-CONFIG_I: Configured from console by console

PH-MNL-MDF-R1#
```

2. Enable Password and Secret

```
PH-MNL-MDF-R1>enable
PH-MNL-MDF-R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PH-MNL-MDF-R1(config)#enable password 1234
PH-MNL-MDF-R1(config)#enable secret abcd
PH-MNL-MDF-R1(config)#end
PH-MNL-MDF-R1#
%SYS-5-CONFIG_I: Configured from console by console

PH-MNL-MDF-R1#exit
```

```
PH-MNL-MDF-R1>enable
Password:
PH-MNL-MDF-R1#
PH-MNL-MDF-R1#
PH-MNL-MDF-R1#
```

3. Password on Console

```
PH-MNL-MDF-R1>
PH-MNL-MDF-R1>enable
Password:
PH-MNL-MDF-R1#
PH-MNL-MDF-R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
PH-MNL-MDF-R1(config)#service password-encryption
PH-MNL-MDF-R1(config)#line vty 0 15
PH-MNL-MDF-R1(config-line)#password 1234
PH-MNL-MDF-R1(config-line)#exec-timeout 0 0
PH-MNL-MDF-R1(config-line)#login
PH-MNL-MDF-R1(config-line)#end
PH-MNL-MDF-R1#

enable secret 5 $1$mERr$YcSt/sTClKuDWnwoppttUQ.
enable password 7 08701E1D5D

line vty 0 4
exec-timeout 0 0
password 7 08701E1D5D
login
line vty 5 15
exec-timeout 0 0
password 7 08701E1D5D
login
!
!
!
end
```

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

4. Password on Telnet

Physical

Config

CLI

Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.BC72.2301

IP Configuration

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Physical

Config

Desktop

Programming

Attributes

IP Configuration

X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.0.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.0.1
Trying 192.168.0.1 ...Open
```

User Access Verification

Password:

Router>

Router>

Router>

5. Password on SSH

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/2

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 00D0.FF5B.9C01

IP Configuration

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.0.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals

```
Router(config)#hostname R2
R2(config)#username Reimarc secret 4321
R2(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R2(config)#ip domain-name reimarcorpuz.pka
R2(config)#line vty 0 15
R2(config-line)#exec-timeout 0 0
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key generate rsa
The name for the keys will be: R2.reimarcorpuz.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R2(config)#enable password 123
*Mar 1 0:5:20.230: %SSH-5-ENABLED: SSH 2 has been enabled
R2(config)#enable password 5678
R2(config)#login
% Incomplete command.
R2(config)#
R2(config)#interface GigabitEthernet0/0
R2(config-if)#
```

```
[Connection to 192.168.0.1 closed by foreign host]
C:\>ssh -l Reimarc 192.168.0.1
```

```
Password:
```

```
R2>en
```

```
Password:
```

```
R2#
```

6. Banner MOTD

```
R2(config)#banner motd $ Warning this is a private network. You are not allowed to access it.$
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

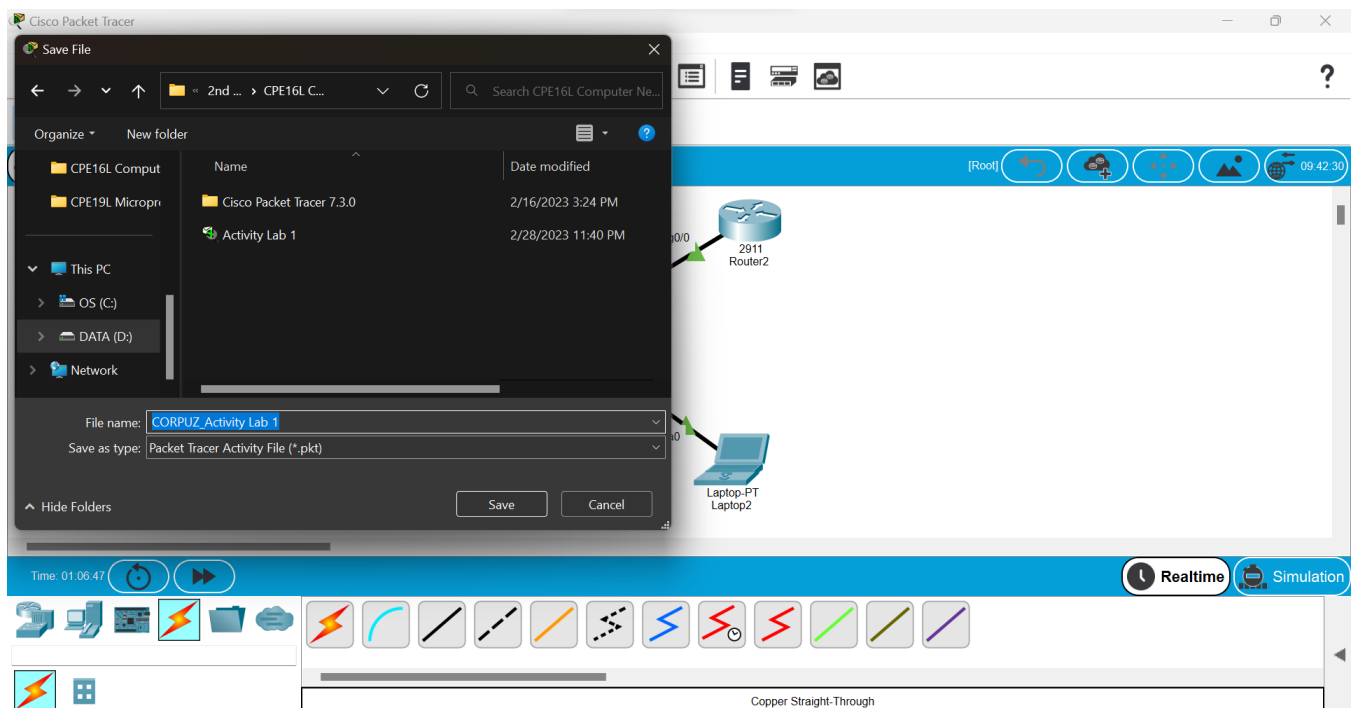
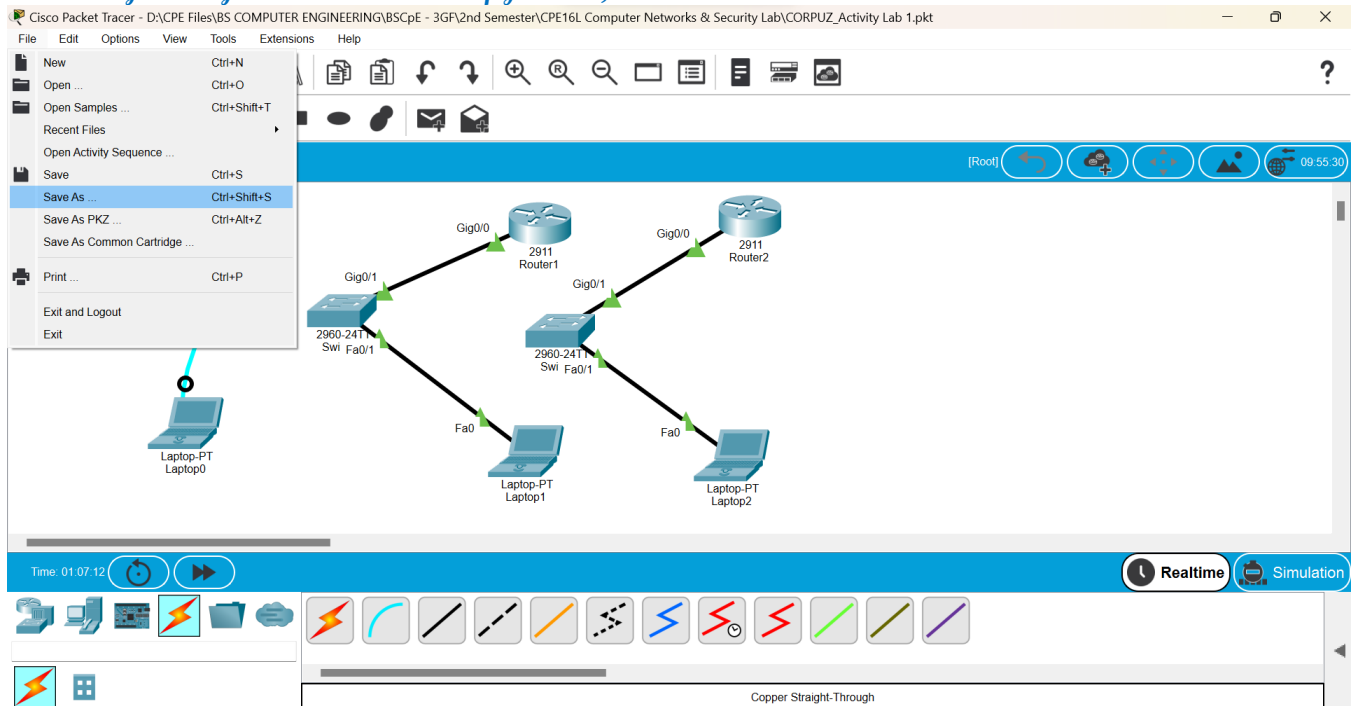
R2#exit
```

```
Warning this is a private network. You are not allowed to access it.
```

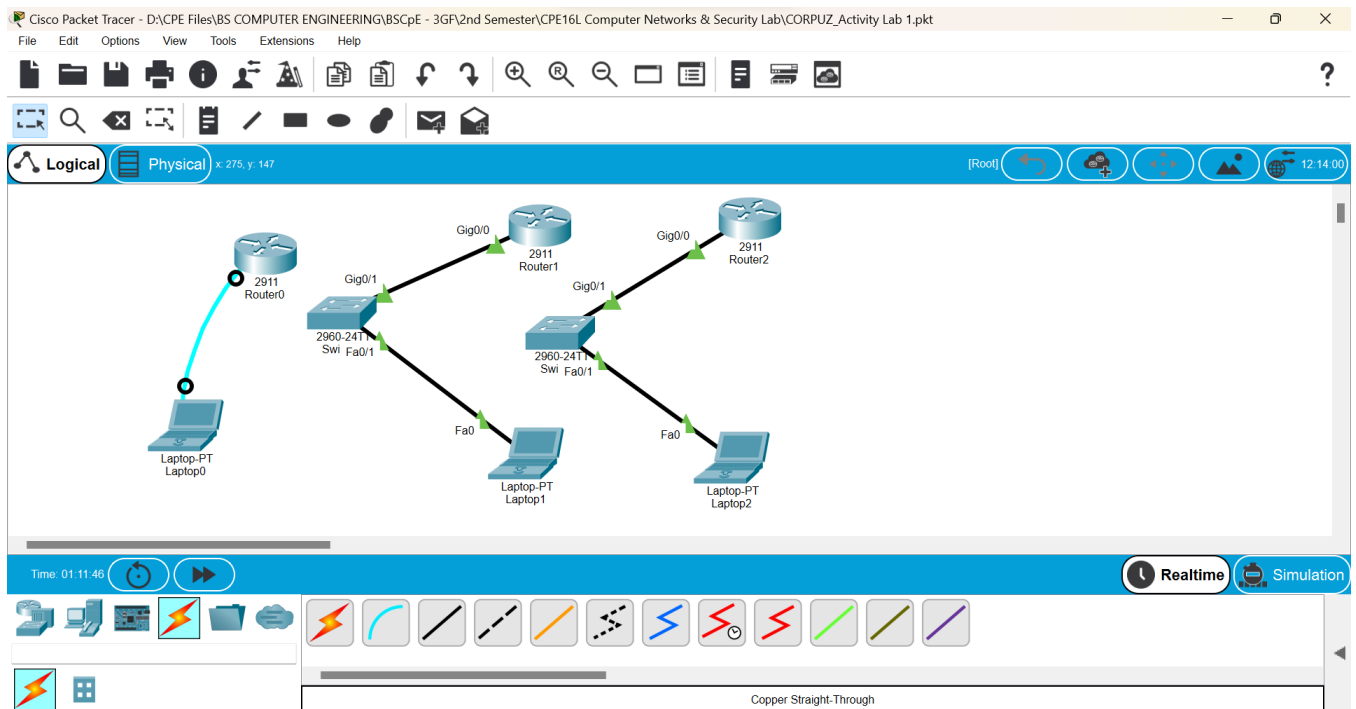
```
R2>
```

7. Saving Configuration

Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals



Laboratory Activity #3 Basic Router Configuration, Command Modes and Command-line Fundamentals



Conclusion: Draw a conclusion based on the objectives.

In conclusion, establishing a connection to a Cisco router using PuTTY and SecureCRT is essential to begin configuring the router. Knowing how to use the help facility of the router can assist in troubleshooting and understanding different commands. Understanding the different modes, such as User Mode, Privileged Mode, and Global Configuration Mode is crucial to effectively configure the router. Changing the hostname, setting passwords, configuring banners, saving changes, and verifying basic configuration are fundamental tasks that need to be completed to ensure the router is functioning correctly. Overall, having a comprehensive understanding of these objectives is critical in successfully configuring a Cisco router.