Name: Dave Jhared G. Paduada Date: March 2, 2025

Course & Section: BSCpE III - IF 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 like 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

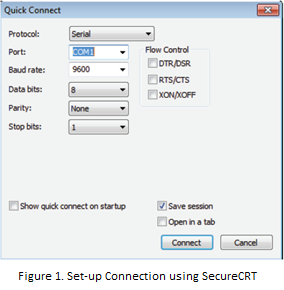
3. Plug the other end into the console port of the router

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.

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

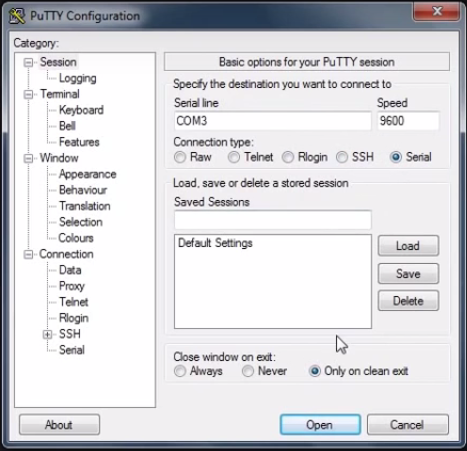


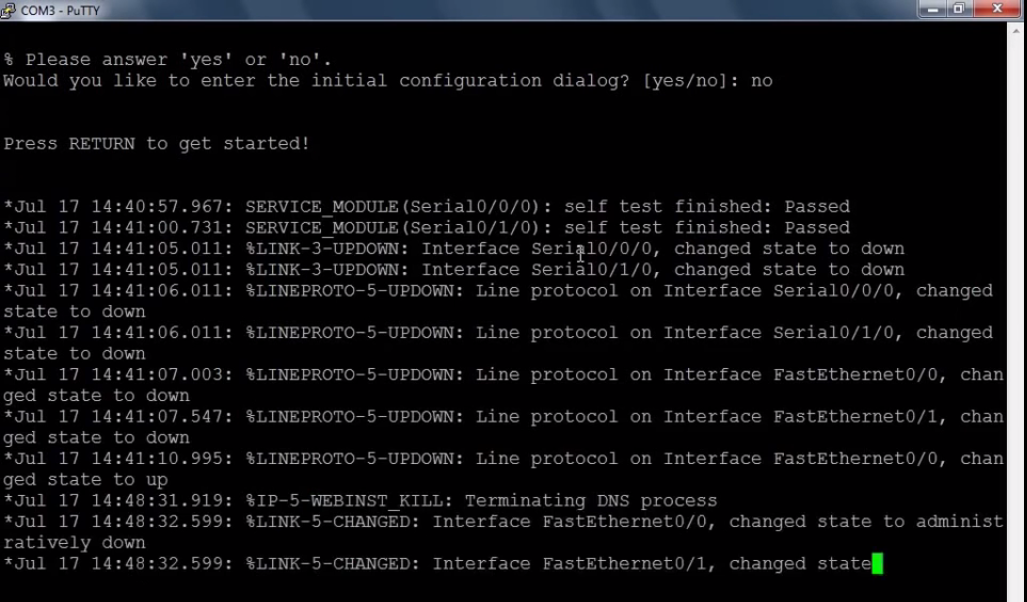
Figure 2. Set-up connection using PuTTY

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.



9. After all the interfaces are initialize, the prompts shows “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 command 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 |
| 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 |
| Traceroute | Trace route to destination |

1. 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 response just keep pressing enter.

|  |  |
| --- | --- |
| Auto | Exec level automation |
| Clear | Reset functions |
| Clock | Manage the system clock |
| Configure | Enter configuration mode |
| Connect | Open a terminal connection |
| Copy | Copy from one file to another |
| Debug | Debugging functions |
| Delete | Delete a file |
| Dir | List files on a filesystem |
| Disable | Turn off privileged commands |
| Disconnect | Disconnect an existing network connection |
| Enable | Turn on privileged commands |

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

Router#con? [Enter]

Task #4 List all the commands after the response.

|  |  |
| --- | --- |
| Configure | connect |

1. 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 | Configure form the terminal |

Note: If the router response is only <br> 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.

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 method.

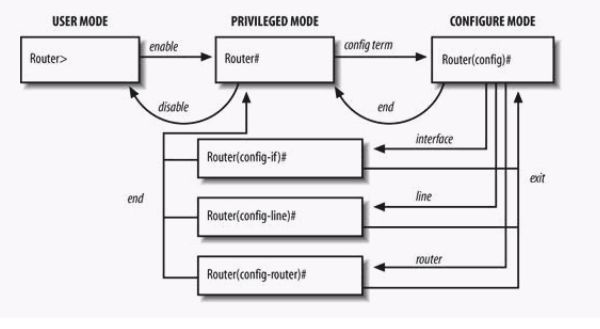


Figure 3. Summary on how to change from one mode to another.

Task #6 Answer the following questions

1. What is the command in order to change from user mode to privileged mode?

en

1. What is the command in order to change from privilege mode to user mode?

disable

1. What is the command in order to change from privilege mode to global configuration mode? conf t
2. What is the command in order to change from global configuration mode to privilege mode? end
3. What is the command in order to change from sub-modes to global configuration mode? exit
4. 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** |
| 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](http://www.cisco.com/c/en/us/td/docs/routers/access/2900/hardware/installation/guide/Hardware_Installation_Guide/Configure.html#73061). |
| 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

|  |  |  |
| --- | --- | --- |
|  | **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-en  cryption | Encrypts the password |
| Step 4 | **line** **console 0**    Router(config)# line console 0 | 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. |
| Step 6 | **exec-timeout** *minutes* [ *seconds* ]    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** *name*  Router(config)#hostname  R1 | Changes the name of the device to R1.  Useful for identifying the device in a network, especially when managing multiple devices. |
| Step 4 | **username** *name* **secret** *password*  R1(config)#username Jerwin secret 4321 | Creates a local user named Jerwin.  The password is encrypted (due to secret) and set to 4321.  This user can later be used for SSH or console login. |
|  | ip ssh version 2 | Enables SSH version 2 on the device (more secure than version 1).  SSH allows secure remote management of the device. |
|  | ip domain-name jobmerga.com | Sets the domain name of the device to jobmerga.com.  Required when generating cryptographic keys for SSH. |
|  | **line vty 0 15**    Router(config)# line vty 0 15 | Enters line configuration mode for VTY lines 0 to 15.  These lines allow up to 16 simultaneous remote connections (0-15). |
|  | **exec-timeout** *minutes* [ *seconds* ]    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.  Usually, you'd set this to something like exec-timeout 10 0 (10 minutes) to avoid leaving idle sessions open indefinitely. |
| 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 (disables Telnet, which is insecure). |
| 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* | **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** *d message d*  Router(config)# **banner motd** *$ Warning this is a private network. You are not allowed to access it. $* | Configures the system to display a message-of-the-day banner. The argument *d* 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**

## Screenshots

Make a screenshot that you perform the following

1. Change Hostname
2. Enable Password
3. Enable Secret
4. Password on Console
5. Password on SSH
6. Banner MOTD
7. Saving Configuration

|  |  |
| --- | --- |
| Command | Output |
| 1. Change Hostname  Router>en  Router#conf t  Router (config) #hostname Keqing  Keqing (config) #end  Keqing# |  |
| 2. Enable Password  Keqing>en  Keqing# conf t  Keqing (config) #enable password deepseek |  |
| 3. Enable Secret  Keqing (config) #enable secret deepseek-r1 |  |
| 4. Password on Console  Keqing>en  Password:  Keqing#conf t  Keqing (config) #line console 0  Keqing (config-line) #password deepseek-rl  Keqing (config-line) #exec-timeout 0 0  Keqing (config-line) #login  Keqing (config-line) #end |  |
| 5. Password on SSH  User Access Verification  Password:  Keqing>en  Password:  Keqing#conf t  Enter configuration commands, one per line. End with CNTL/Z. Keqing (config)#line vty 0 15  Keqing (config-line) #exec-timeout 0 0  Keqing (config-line)#login local  Keqing (config-line)#transport input ssh  Keqing (config-line)#crypto key generate rsa  The name for the keys will be: Keqing.Ganyu.com  Choose the size of the key modulus in the range of 360 to 4096 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  8 Generating 1024 bit RSA keys, keys will be non-exportable...[OK]  Keqing (config)#| |  |
| 6. Banner MOTD  Keqing>en Password:  Keqing#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Keqing (config)#banner\_motd\_d ### WARNING: Accessing the network is not Halal ### d  Keqing (config)#exit  Keqing#  %SYS-5-CONFIG\_I: Configured from console by console  exit |  |
| 7. Saving the configuration  [startup-config]?  Keqing#copy running-config startup-config Destination filename Building configuration...  [OK]  Keqing#copy run start  Destination filename [startup-config]?  Building configuration...  [OK]  Keqing#exit |  |

Conclusion: Draw conclusion based on the objectives.

In this laboratory exercise, we successfully established a connection to a Cisco router using PuTTY and SecureCRT, enabling direct interaction with the device. We explored the router’s help facility by utilizing the “?” command, which provided a list of available commands, helping us navigate through different operational modes. By transitioning between User Exec mode, Privileged Exec mode, and Global Configuration mode, we gained an understanding of their distinct functions and permissions. Additionally, we configured essential settings, such as changing the hostname, setting passwords for security, creating banners for informational purposes, and saving configurations to ensure persistence across reboots. Through verification commands, we confirmed the applied settings, reinforcing our ability to perform basic router configurations effectively.