Experiment-10

Aim: To perform basic and initial router configuration

Devices Used: Router, PCs, and Console Cable.

Objectives:

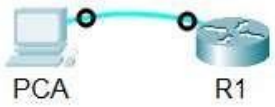
Part 1: Verify the Default Router Configuration

Part 2: Configure and Verify the Initial Router Configuration

Part 3: Save the Running Configuration File

Background:
In this activity, you will perform basic router configuration tasks. You will secure access to the CLI and console port using encrypted and plain-text passwords. You will also configure messages for users who are logging into the router. These banners warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration.

Figure:



Procedure:

Part 1: Verify the Default Router Configuration

Step 1: Establish a console connection to R1.
a. Choose a Console cable from the available connections.
b. Click PCA and select RS 232.
c. Click R1 and select Console.
d. Click PCA > Desktop tab > Terminal.
e. Click OK and press ENTER. You are now able to configure R1.

Part 2: Configure and Verify the Initial Router Configuration

Step 1: Perform initial router configuration
Router> enable
Router# show running-config
Router# show
startup-config
Router#
configure
terminal
Router(config) hostname R1
R1(config)# banner motd #Unauthorized access is strictly prohibited#
R1(config)#enable password cisco
R1(config)#enable secret itsasecret

R1(config)#line console 0
R1(config)#password letmein
R1(config)#login
R1(config)#service password-encyrption
R1(config)#exit
R1#show running-config
R1#copy running-config startup-config
R1# exit

Step 2:Verify the initial router configuration
Verify the initial settings by viewing the configuration for R1.
Type your answers here.
b. Exit the current console session until you see the following message:
R1 con0 is now available Press RETURN to get started.
c. Press ENTER; you should see the following message:
Unauthorized access is
strictly prohibited.
User Access
Verification Password:

Part 3: Save Running Configuration to NVRAM file
You have configured the initial settings for R1. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

Questions:

Q) What is the router's hostname?
Ans) Router

Q) How many Fast Ethernet interfaces does the Router have?
Ans) none

Q) How many Gigabit Ethernet interfaces does the
Router have? Ans) 2

Q) How many Serial interfaces does the router have?
Ans) 2

Q) What is the range of values shown for the vty lines?
Ans) 0-4

Q) What command do you use to verify ini al configura on
on router? Ans) show running-config

Q) Why should every router have a message-of-the-day (MOTD) banner?
Ans) Every router should have a banner to warn unauthorized users that access is prohibited. MOTD Banners can also be used to send messages to network personnel (such as impending system shutdowns or who to contact for access).

Q) If you are not prompted for a password before reaching the user EXEC prompt, what console line command did you forget to configure? Ans) R1(config-line)# login

Q) If you configure any more passwords on the router, are they displayed in the configura on file as plain text or in encrypted form? Explain.
Ans) The service password-encryp on command encrypts all current and future passwords.

Q) What command did you enter to save the configura on
to NVRAM? Ans) copy running-config startup-config

Q) Which command displays the contents of the NVRAM?
Ans) show startup-configura on or show start .

Result:

```
R1#show running-config
Building configuration...

Current configuration : 1277 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 0822455D0A16
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX152459PZ
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet0/1/0
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/1/1
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet0/1/2
```

```
Router>enable
Router#cofigure terminal
              ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#banner motd
% Incomplete command.
R1(config)#banner motd "Unauthorized access is strictly prohibited."
R1(config)#service password-encryption
R1(config)#enable password cisco
R1(config)#enable secret itsasecret
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login exit
                   ^
% Invalid input detected at '^' marker.

R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#
R1#exit



R1 con0 is now available



Press RETURN to get started.









Unauthorized access is strictly prohibited.

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Result: Hence, the initial and basic router configuration has been done.