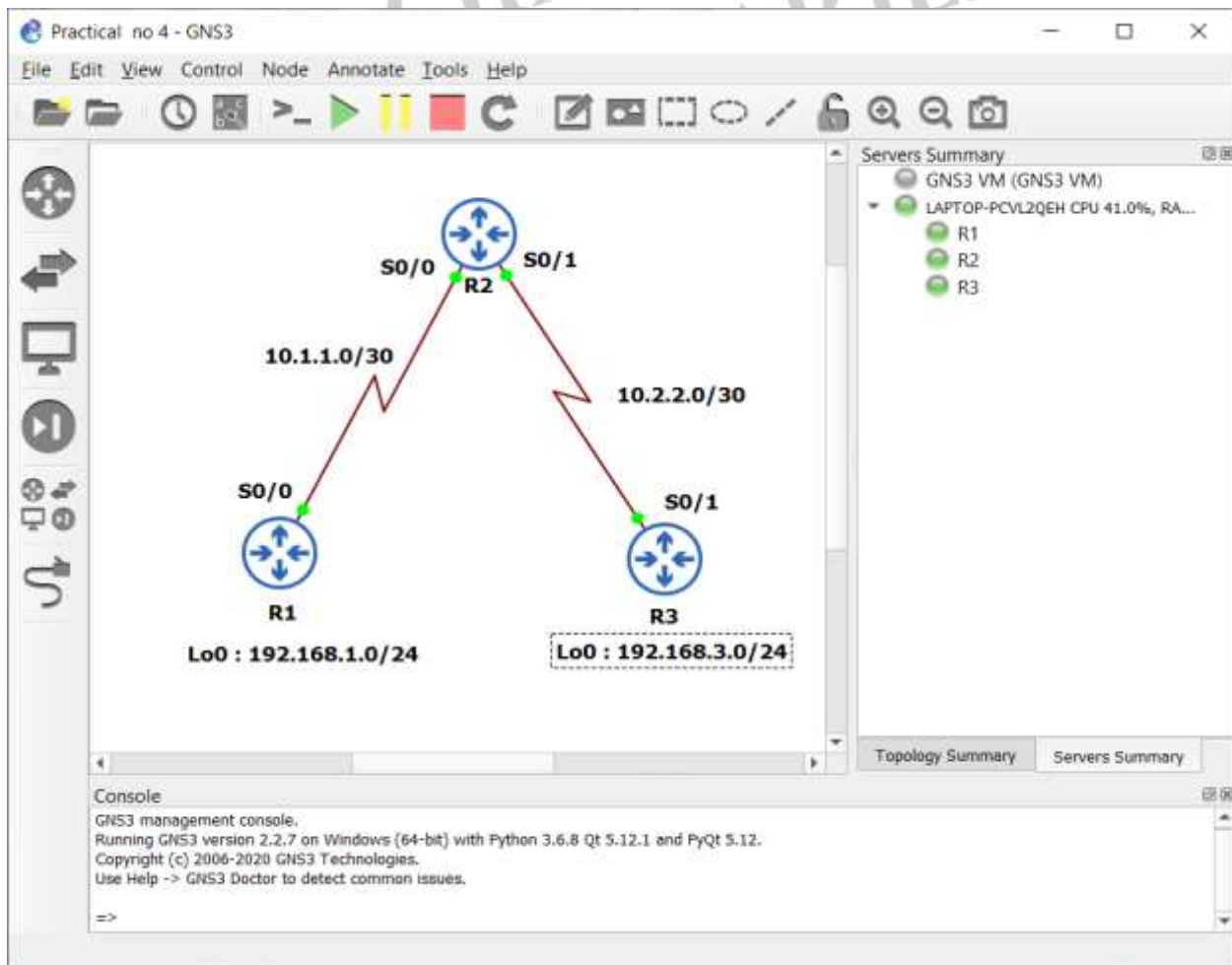


PRACTICAL NO. 4**Aim:** Secure the Management Plane**Topology:****Objectives:**

- Secure management access.
- Configure enhanced username password security.
- Enable AAA RADIUS authentication.
- Enable secure remote management

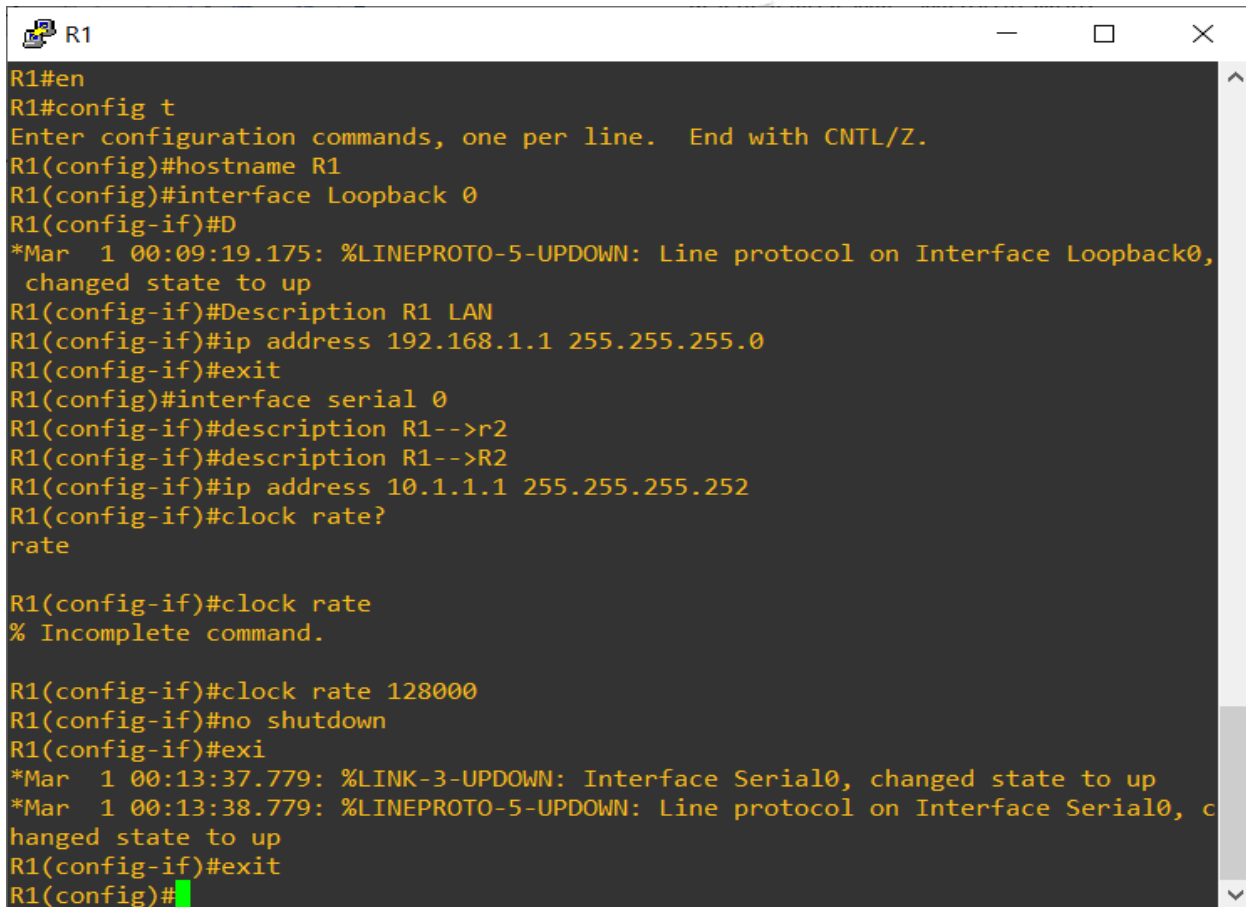
Required Resources

- 3routers
- Serial and Ethernet cables

Procedure:**Step 1: Configure loopbacks and assign addresses**

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the R1, R2, and R3 routers.

R1:

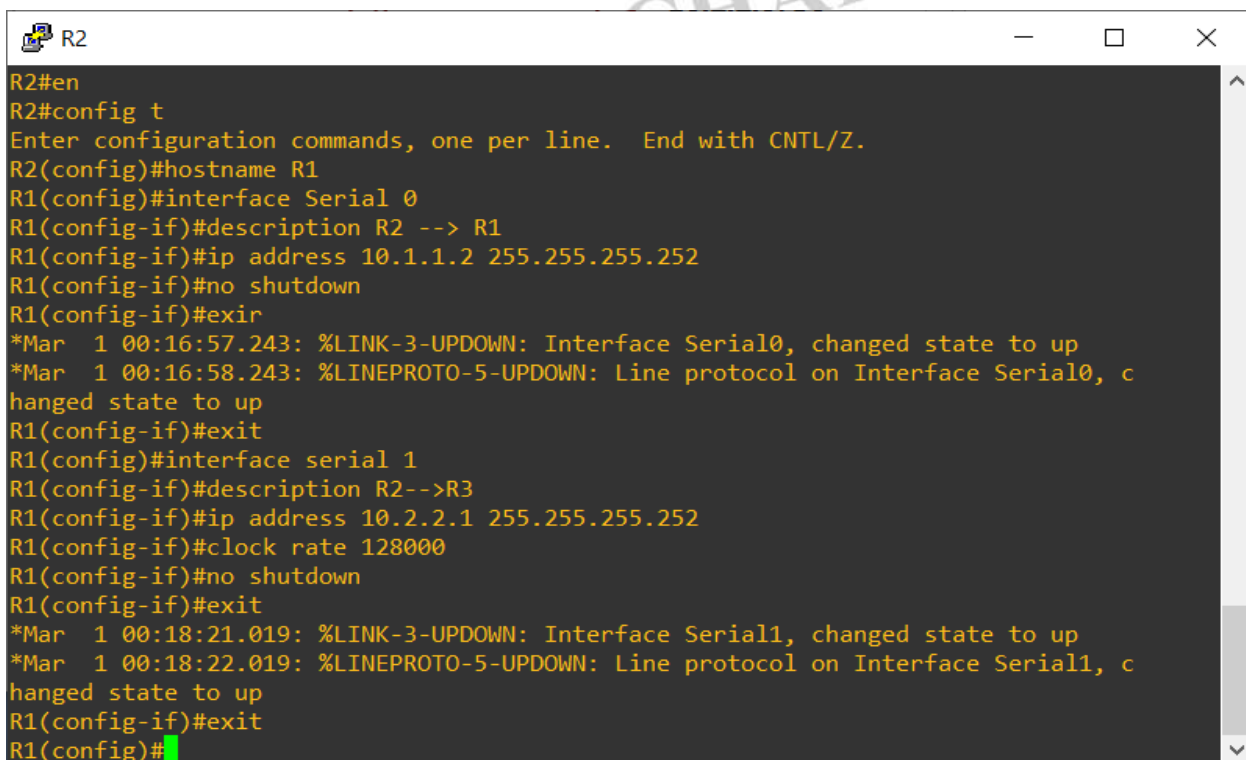
A screenshot of a terminal window titled 'R1'. The terminal shows the configuration of a Cisco router. The user enters 'en' to enter enable mode, then 'config t' to enter configuration mode. The prompt changes from 'R1#' to 'R1(config)#'. The user configures the hostname to 'R1', then enters interface configuration mode for 'Loopback 0'. It shows the interface coming up with the message '*Mar 1 00:09:19.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up'. Then, the user sets the description to 'R1 LAN', the IP address to '192.168.1.1 255.255.255.0', and exits the interface configuration. Next, the user enters interface configuration mode for 'serial 0'. It shows the interface coming up with the message '*Mar 1 00:13:37.779: %LINK-3-UPDOWN: Interface Serial0, changed state to up'. The user sets the description to 'R1-->r2', then 'R1-->R2', the IP address to '10.1.1.1 255.255.255.252', and attempts to set the clock rate. The prompt returns to 'R1(config-if)#' and the user enters 'clock rate', which results in the message '% Incomplete command.'. Then, the user enters 'clock rate 128000', and the prompt returns to 'R1(config-if)#'. The user enters 'no shutdown', and the interface comes up with the message '*Mar 1 00:13:38.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up'. Finally, the user enters 'exit' twice to return to the 'R1(config)#' prompt, where a green cursor is visible.

```
R1#en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#interface Loopback 0
R1(config-if)#D
*Mar 1 00:09:19.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#Description R1 LAN
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface serial 0
R1(config-if)#description R1-->r2
R1(config-if)#description R1-->R2
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate?
rate

R1(config-if)#clock rate
% Incomplete command.

R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exi
*Mar 1 00:13:37.779: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar 1 00:13:38.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, c
hanged state to up
R1(config-if)#exit
R1(config)#
```

R2:

A screenshot of a terminal window titled 'R2'. The terminal shows the configuration of a Cisco router. The user enters 'en' to enter enable mode, then 'config t' to enter configuration mode. The prompt changes from 'R2#' to 'R2(config)#'. The user configures the hostname to 'R1' (likely a typo for R2), then enters interface configuration mode for 'Serial 0'. It shows the interface coming up with the message '*Mar 1 00:16:57.243: %LINK-3-UPDOWN: Interface Serial0, changed state to up'. The user sets the description to 'R2 --> R1', the IP address to '10.1.1.2 255.255.255.252', and enters 'no shutdown'. The interface comes up with the message '*Mar 1 00:16:58.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, c hanged state to up'. Then, the user enters 'exit' to return to 'R2(config)#'. Next, the user enters interface configuration mode for 'serial 1'. It shows the interface coming up with the message '*Mar 1 00:18:21.019: %LINK-3-UPDOWN: Interface Serial1, changed state to up'. The user sets the description to 'R2-->R3', the IP address to '10.2.2.1 255.255.255.252', the clock rate to '128000', and enters 'no shutdown'. The interface comes up with the message '*Mar 1 00:18:22.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, c hanged state to up'. Finally, the user enters 'exit' twice to return to the 'R2(config)#' prompt, where a green cursor is visible.

```
R2#en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R1
R1(config)#interface Serial 0
R1(config-if)#description R2 --> R1
R1(config-if)#ip address 10.1.1.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exir
*Mar 1 00:16:57.243: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar 1 00:16:58.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, c
hanged state to up
R1(config-if)#exit
R1(config)#interface serial 1
R1(config-if)#description R2-->R3
R1(config-if)#ip address 10.2.2.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
*Mar 1 00:18:21.019: %LINK-3-UPDOWN: Interface Serial1, changed state to up
*Mar 1 00:18:22.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, c
hanged state to up
R1(config-if)#exit
R1(config)#
```

R3:

```
R3
R3(config)#hostname R3
R3(config)#interface Loopback 0
R3(config-if)#description R3 LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#
```

```
R3
R3(config)#interface serial 1
R3(config-if)#description R3-->R2
R3(config-if)#ip address 10.2.2.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

Step 2: Configure static routes

- a. On R1, configure a default static route to ISP

```
R1
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 10
% Incomplete command.

R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)#
```

- b. On R3, configure a default static route to ISP.

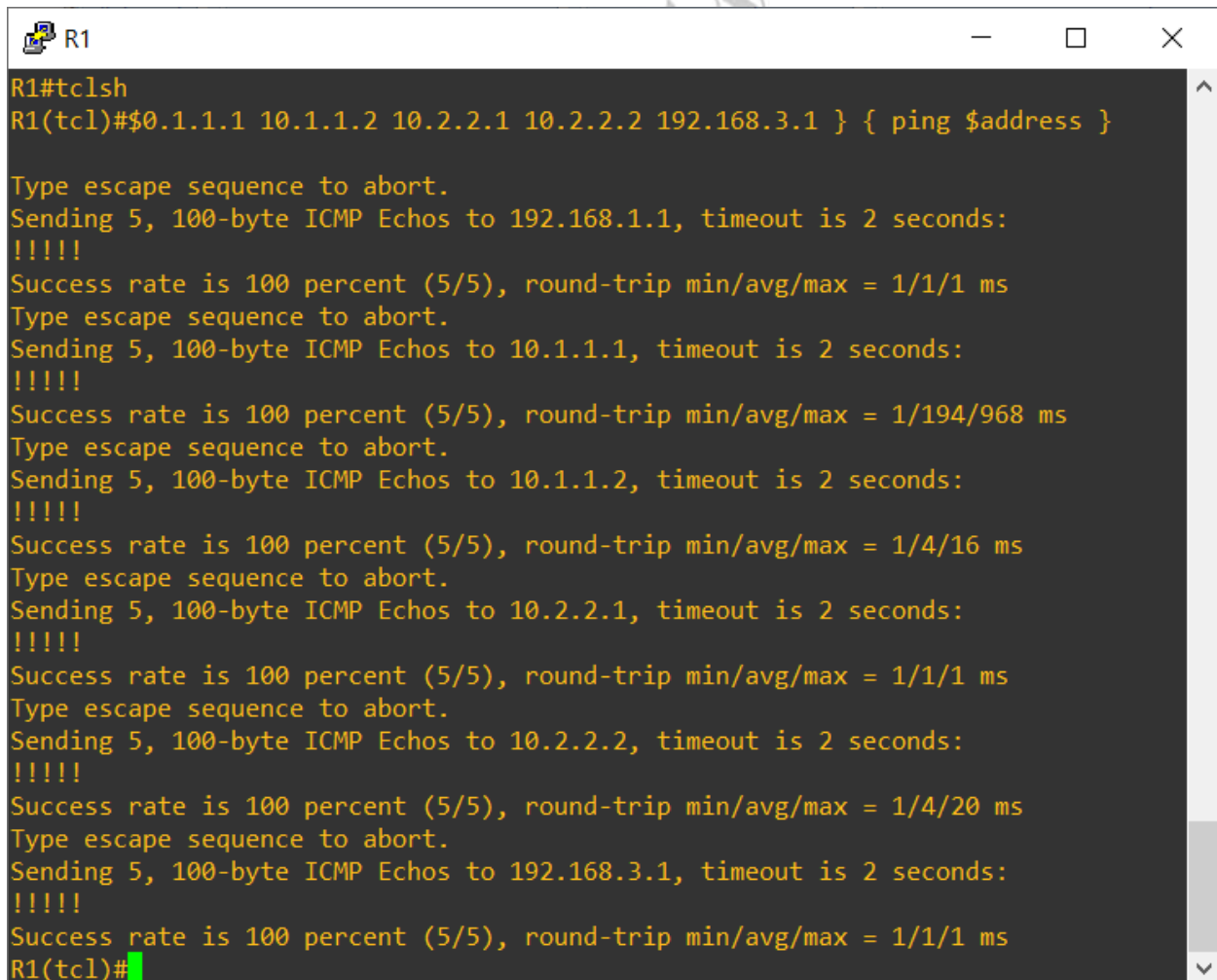
```
R3
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1
R3(config)#
```

- c. On R2, configure two static routes.

```
R2
R1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R1(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.2
R1(config)#
```

- d. From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {  
  192.168.1.1  
  10.1.1.1  
  10.1.1.2  
  10.2.2.1  
  10.2.2.2  
  192.168.3.1  
} { ping $address }
```

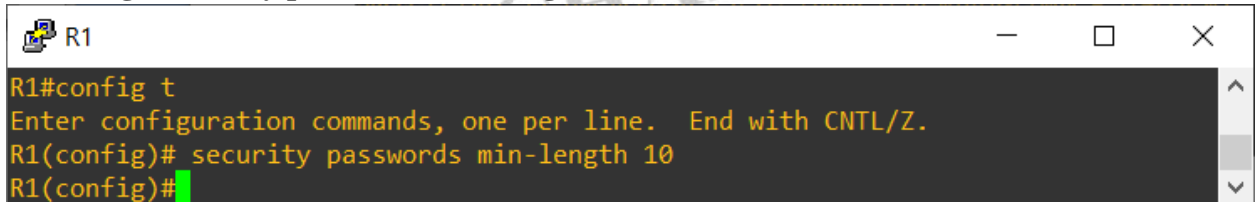


```
R1#tclsh  
R1(tcl)#$0.1.1.1 10.1.1.2 10.2.2.1 10.2.2.2 192.168.3.1 } { ping $address }  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/194/968 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms  
R1(tcl)#
```

Step 3: Secure management access

- a. On R1, use the security passwords command to set a minimum password length of 10 characters.

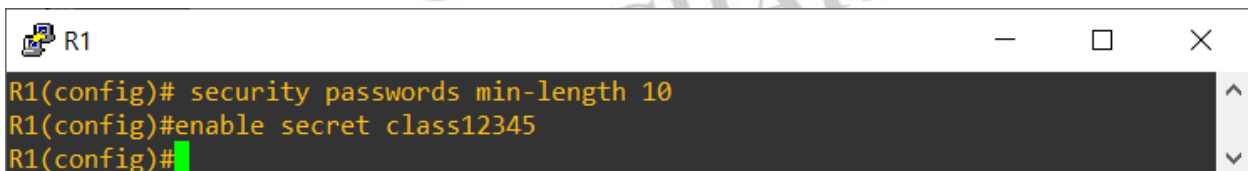
R1(config)# security passwords min-length 10



```
R1
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# security passwords min-length 10
R1(config)#
```

- b. Configure the enable secret encrypted password on both routers.

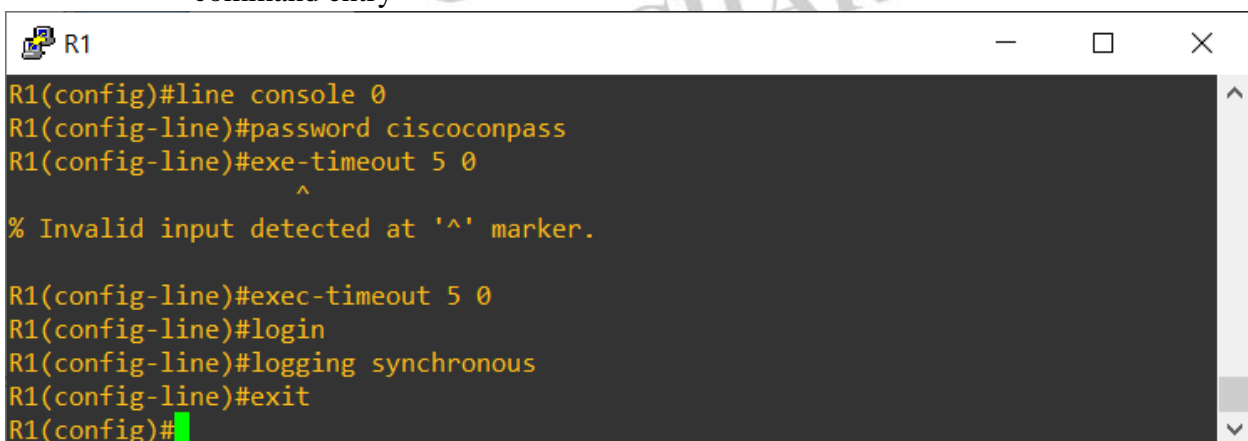
R1(config)# enable secret class12345



```
R1
R1(config)# security passwords min-length 10
R1(config)#enable secret class12345
R1(config)#
```

- c. Configure a console password and enable login for routers.

- For additional security, the **exec-timeout** command causes the line to log out after 5 minutes of inactivity.
- The **logging synchronous** command prevents console messages from interrupting command entry



```
R1
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exe-timeout 5 0
^
% Invalid input detected at '^' marker.

R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

- d. Configure the password on the vty lines for router R1.

```
R1
R1(config)#line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)#login
R1(config-line)# exit
R1(config)#
```

- e. The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port

```
R1
R1(config)# line aux 0
R1(config-line)#no exec
R1(config-line)# end
R1#
*Mar  1 01:24:42.635: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

- f. Use the *service password-encryption* command to encrypt the line console and vty passwords.

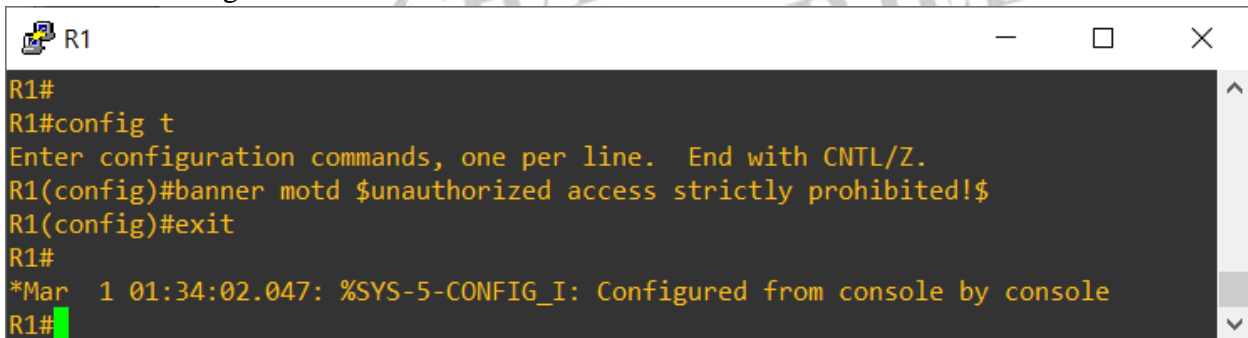
```
R1
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# service password-encryption
R1(config)#
```

- g. Issue the *show run* command. Can you read the console, aux, and vty passwords? Why or why not?

```
R1
R1#config t
*Mar  1 01:29:07.735: %SYS-5-CONFIG_I: Configured from console by console
R1#show run
Building configuration...

Current configuration : 1201 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5 $1$b1Fd$KKZHE9gpiSRvpKHAssB7b/
!
no aaa new-model
!
resource policy
```

- h. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the banner motd command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign (\$) is used to start and end the message.



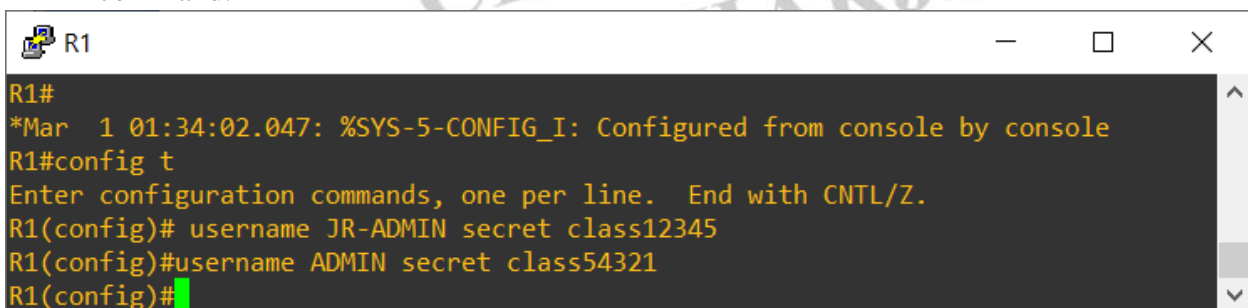
```
R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#banner motd $unauthorized access strictly prohibited!$
R1(config)#exit
R1#
*Mar  1 01:34:02.047: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

(Note : Repeat the configuration portion of steps 3a through 3k on router R3.)

Step 4: Configure enhanced username password security.

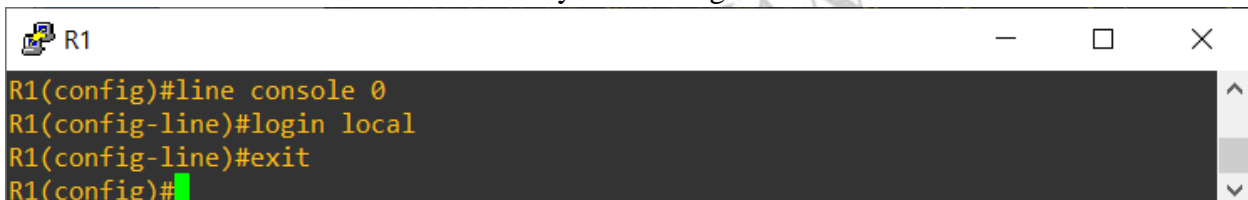
To increase the encryption level of console and VTY lines, it is recommended to enable authentication using the local database. The local database consists of usernames and password combinations that are created locally on each device. The local and VTY lines are configured to refer to the local database when authenticating a user.

- a. To create local database entry encrypted to level 4 (SHA256), use the **username** name **secret** password global configuration command. In global configuration mode, enter the following command:



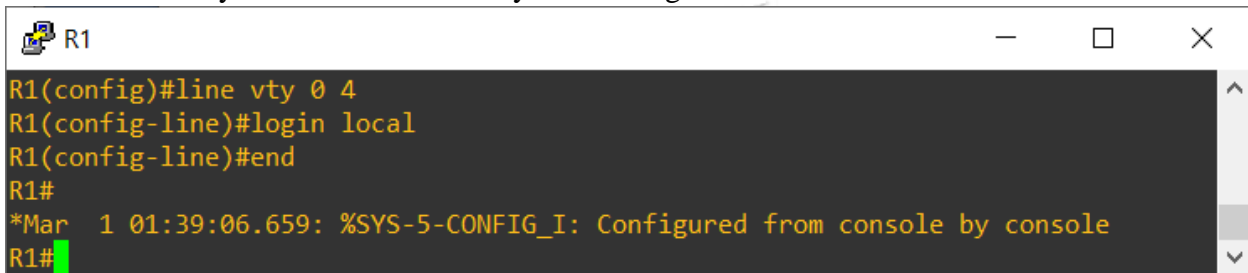
```
R1#
*Mar  1 01:34:02.047: %SYS-5-CONFIG_I: Configured from console by console
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# username JR-ADMIN secret class12345
R1(config)#username ADMIN secret class54321
R1(config)#
```

- b. Set the console line to use the locally defined login accounts



```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

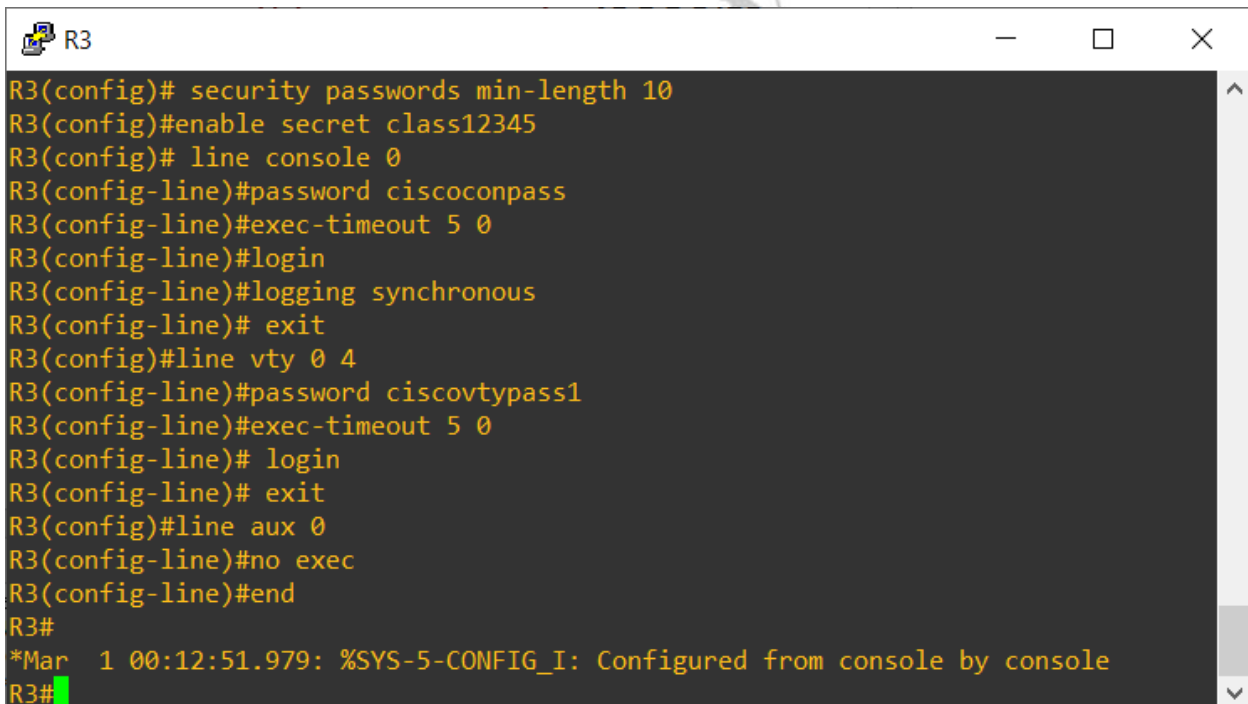

- c. Set the vty lines to use the locally defined login accounts.



```
R1
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#
*Mar  1 01:39:06.659: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

(Note : Repeat the steps 4a to 4c on R3.)

- d. To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.



```
R3
R3(config)# security passwords min-length 10
R3(config)#enable secret class12345
R3(config)# line console 0
R3(config-line)#password ciscoconpass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)# exit
R3(config)#line vty 0 4
R3(config-line)#password ciscovtypass1
R3(config-line)#exec-timeout 5 0
R3(config-line)# login
R3(config-line)# exit
R3(config)#line aux 0
R3(config-line)#no exec
R3(config-line)#end
R3#
*Mar  1 00:12:51.979: %SYS-5-CONFIG_I: Configured from console by console
R3#
```



```
R3#
R3#
R3#
R3#
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized access strictly prohibited!$
R3(config)#username JR-ADMIN secret class12345
R3(config)#username ADMIN secret class54321
R3(config)#line console 0
R3(config-line)#login local
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#end
R3#
*Mar  1 00:17:53.635: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

```
R3#
Translating "class54321"
Translating "class54321"
% Unknown command or computer name, or unable to find computer address
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#username ADMIN secret class56789
R3(config)#username JR-ADMIN secret class98765
R3(config)#line console 0
R3(config-line)#login local
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#end
R3#
*Mar  1 00:25:16.671: %SYS-5-CONFIG_I: Configured from console by console
R3#do wr
^
% Invalid input detected at '^' marker.
```

- e. To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account

```
R1
R1>telnet 10.2.2.2
Trying 10.2.2.2 ... Open
Unauthorized access strictly prohibited!

User Access Verification

Username: ADMIN
Password:
% Login invalid

Username:
% Username: timeout expired!
Username:
% Username: timeout expired!
[Connection to 10.2.2.2 closed by foreign host]
R1>telnet 10.2.2.2
Trying 10.2.2.2 ... Open
Unauthorized access strictly prohibited!

User Access Verification

Username: ADMIN
Password:
R3>
```

```
R3
% Invalid input detected at '^' marker.

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
R3#
*Mar  1 00:27:26.511: %SYS-5-CONFIG_I: Configured from console by console
R3#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
unauthorized access strictly prohibited!

User Access Verification

Username: ADMIN
Password:
R1>
```

BHATTACHARJEE