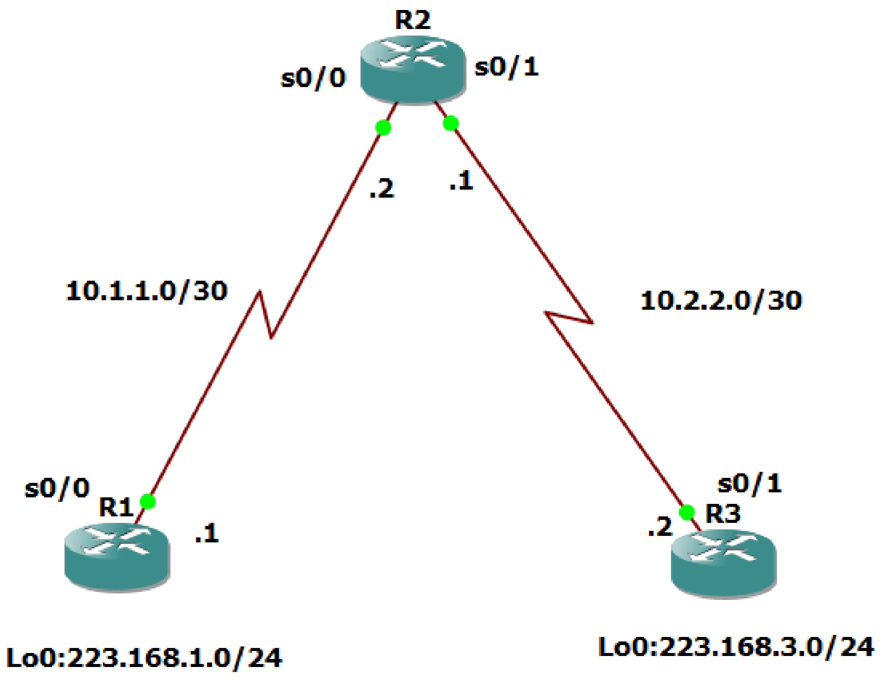
Practical No 4

Aim: Secure Management Plane

Topology:



Objectives:

Secure management access.

– Configure enhanced username password security.

– Enable AAA RADIUS authentication.

– Enable secure remote management.

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. You can copy and paste the following configurations into your routers to begin.

Router 1

interface Loopback 0

ip address 223.168.1.1 255.255.255.0

exit

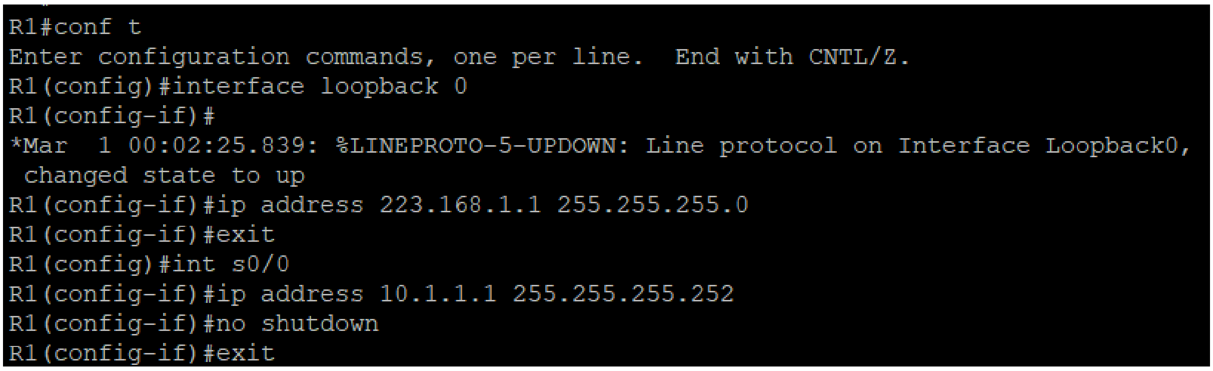
interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

end



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface loopback 0
R1(config-if)#
*Mar  1 00:02:25.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
 changed state to up
R1(config-if)#ip address 223.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#int s0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Router R2

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

no shutdown

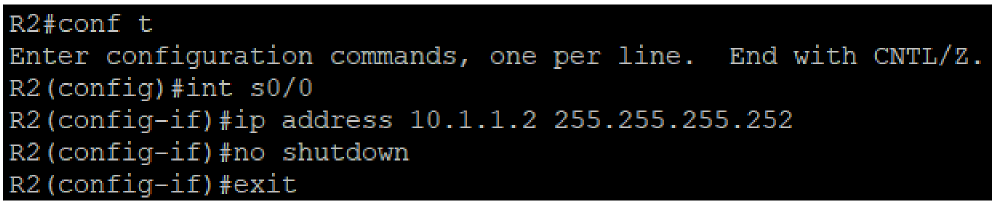
exit interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

end



```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

Router R3

interface Loopback0

ip address 223.168.3.1 255.255.255.0

exit

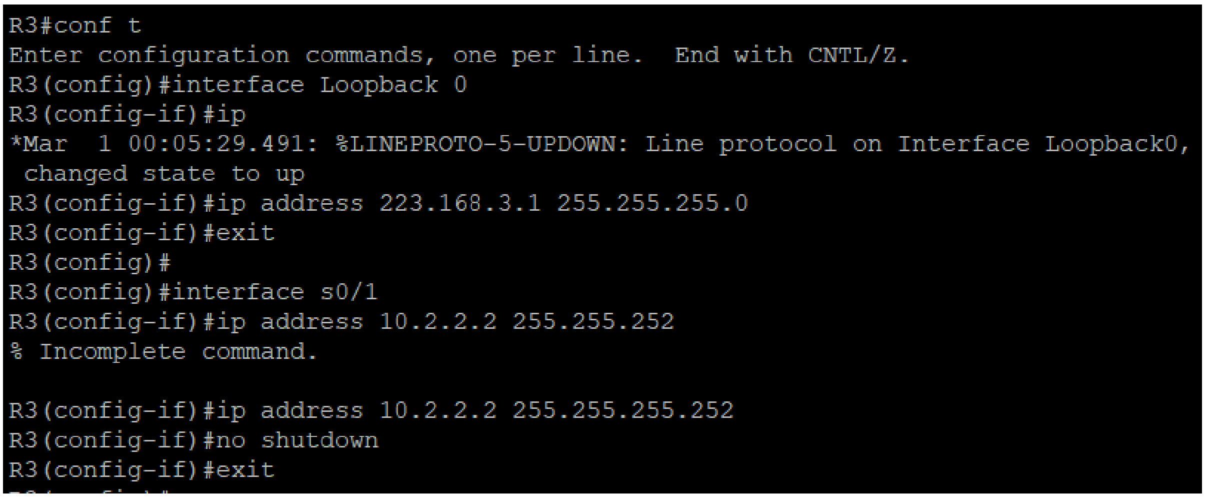
interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

end

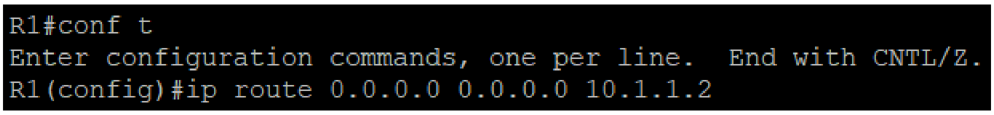


```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface Loopback 0
R3(config-if)#ip
*Mar  1 00:05:29.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
 changed state to up
R3(config-if)#ip address 223.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#
R3(config)#interface s0/1
R3(config-if)#ip address 10.2.2.2 255.255.252
% Incomplete command.

R3(config-if)#ip address 10.2.2.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

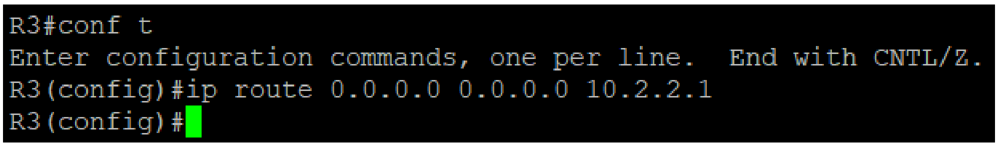
Step 2: Configure static routes.

R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

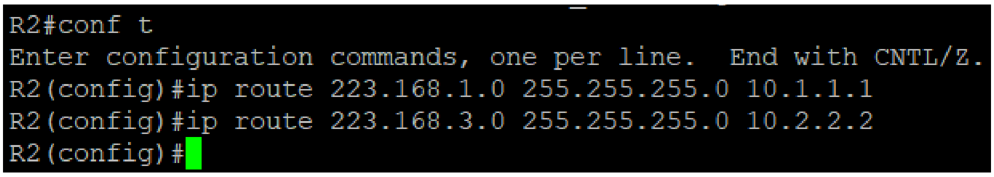


```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.1



```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1
R3(config)#
```



```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 223.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 223.168.3.0 255.255.255.0 10.2.2.2
R2(config)#
```

R2(config)# ip route 223.168.1.0 255.255.255.0 10.1.1.1

R2(config)# ip route 223.168.3.0 255.255.255.0 10.2.2.2

foreach address {

223.168.1.1

10.1.1.1

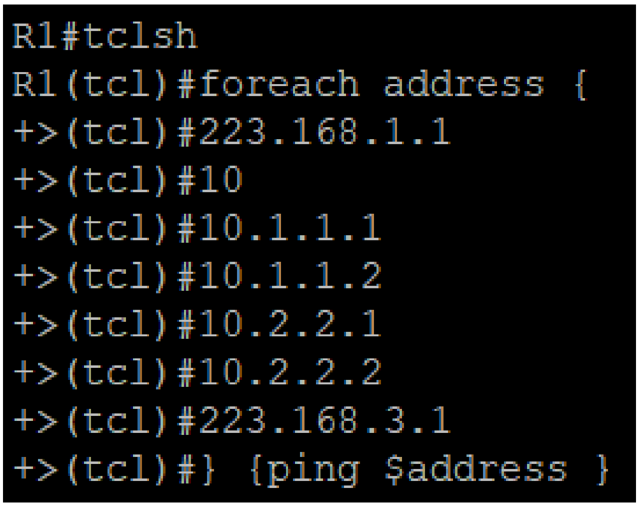
10.1.1.2

10.2.2.1

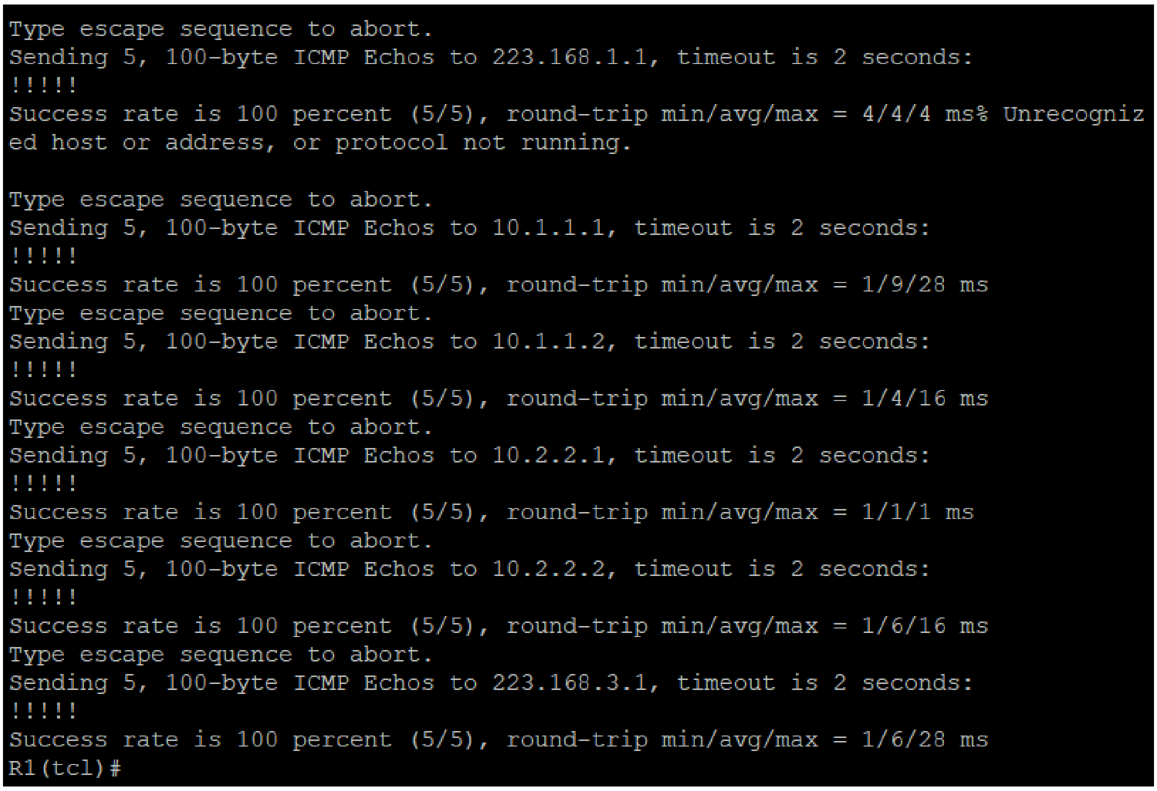
10.2.2.2

223.168.3.1}

{ping $address}



```
R1#tclsh
R1(tcl)#foreach address {
+>(tcl)#223.168.1.1
+>(tcl)#10
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#223.168.3.1
+>(tcl)#} {ping $address }
```



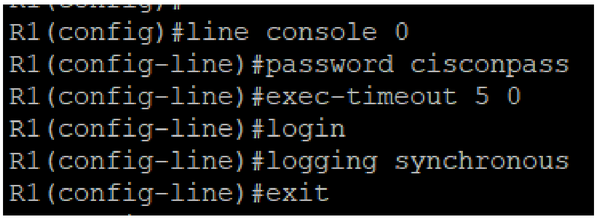
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 223.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms% Unrecogniz
ed host or address, or protocol not running.

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 = 1/9/28 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 = 1/6/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 223.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/28 ms
R1(tcl)#
```

Step 3: Secure management access.

1. On R1, use the security passwords command to set a minimum password length of 10 characters.
2. **R1(config)# security passwords min-length 10**
3. 2. Configure the enable secret encrypted password on both routers. **R1(config)# enable secret class12345.**
4. Configure a console password and enable login for routers. For additional security, the exectimeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

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



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

Configure the password on the vty lines for router R1.

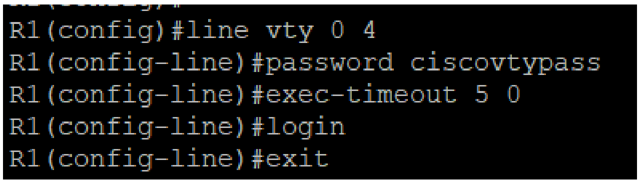
R1(config)# line vty 0 4

R1(config-line) # password ciscovtypass

R1(config-line) # exec-timeout 5 0

R1(config-line) # login

R1(config-line) # exit



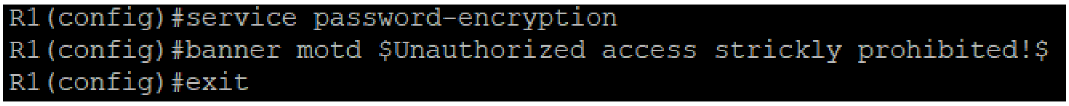
```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#exit
```

5. 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(config)# line aux 0
   R1(config-line) # no exec
   R1(config-line) # end
6. Enter privileged EXEC mode and issue the show run command. Can you read the enable secret password? Why or why not?

   R1(Config)# service password-encryption

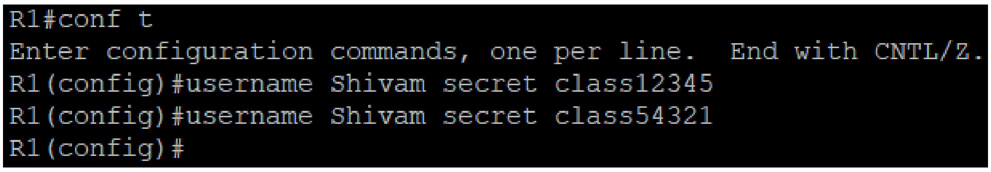
7. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the banner motd command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.



```
R1(config)#service password-encryption
R1(config)#banner motd $Unauthorized access strickly prohibited!$
R1(config)#exit
```

Step 4: Configure enhanced username password security.

1. 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:
2. R1(config)# username Shivam secret class12345
3. R1(config)# username Shivam secret class5432



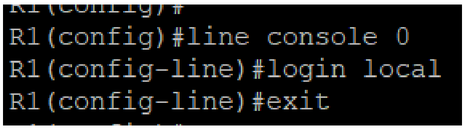
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username Shivam secret class12345
R1(config)#username Shivam secret class54321
R1(config)#
```

4. 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

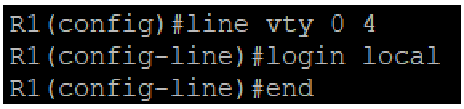


```
R1(config)#
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
```

R1(config)# line vty 0 4

R1(config-line) # login local

R1(config-line) # end



```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
```