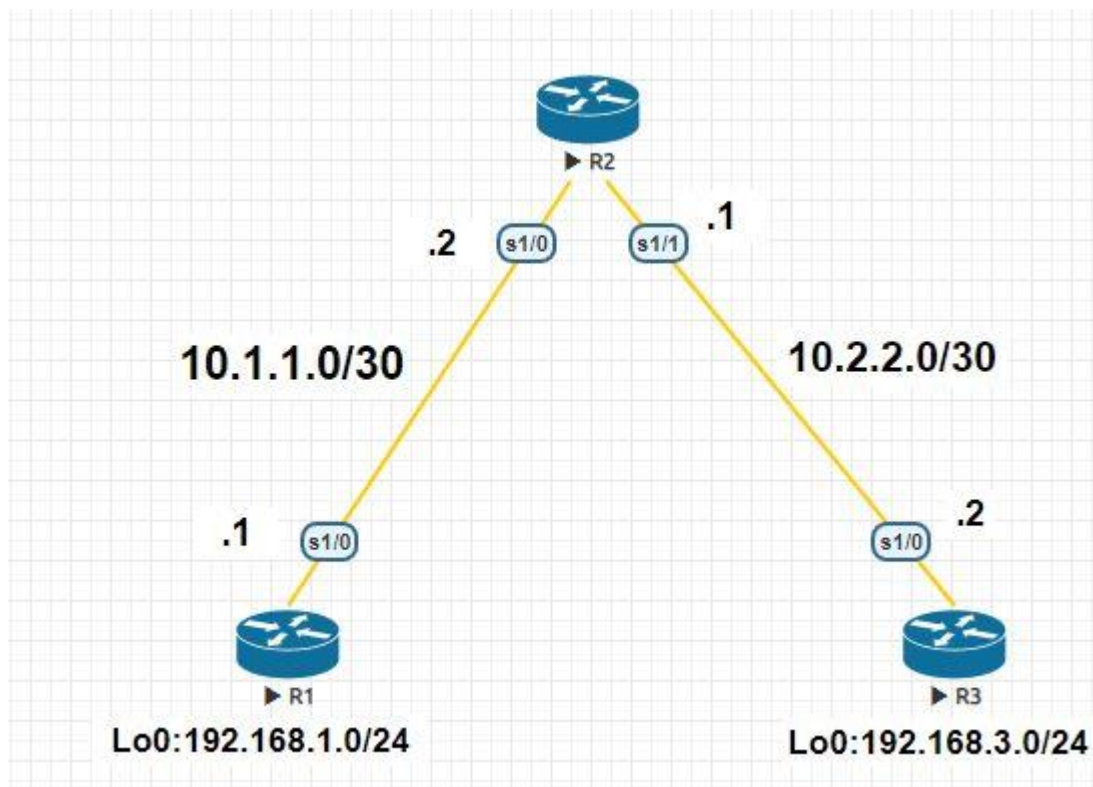**PRACTICAL NO 4: Secure the Management Plane**

NETWORK TOPOLOGY

TASKS

- **Secure Management Access**
- **Configure enhanced username password security**
- **Enable AAA RADIUS authentication**
- **Enable Secure Remote Management**

R1

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#interface Loopback 0

*Dec 19 07:53:42.473: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface s1/0

R1(config-if)#ip address 10.1.1.1 255.255.255.252

R1(config-if)#no shutdown

*Dec 19 07:57:21.998: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

*Dec 19 07:57:22.999: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R1(config-if)#exit

R1(config)#exit

Configure static routes

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

    R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default,U - per-user static route o - ODR, P - periodic downloaded static route,H - NHRP,l - LISP

   a - application route

   + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.1.1.2

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C   10.1.1.0/30 is directly connected, Serial1/0

L   10.1.1.1/32 is directly connected, Serial1/0

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C   192.168.1.0/24 is directly connected, Loopback0

L   192.168.1.1/32 is directly connected, Loopback0

Secure management access

R1(config)#security passwords min-length 10

R1(config)#enable secret class12345

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 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 aux 0

R1(config-line)#no exec

R1(config-line)#end

R1(config)#service password-encryption

R1(config)#banner motd $Unauthorized access strictly prohibited!$

R1(config)#exit
```

Configure enhanced username password security

```
R1(config)#username JR-ADMIN secret class12345

R1(config)#username ADMIN secret class54321

R1(config)#line console 0

R1(config-line)#login local

R1(config-line)#end

R1(config)#line vty 0 4

R1(config-line)#login local
```

R1(config-line)#end

Enabling AAA RADIUS Authentication with Local User for Backup

R1(config)# aaa new-model

R1(config)# radius server RADIUS-1

R1(config-radius-server)# address ipv4 192.168.1.101

R1(config-radius-server)# key RADIUS-1-pa55w0rd

R1(config-radius-server)# exit

R1(config)# radius server RADIUS-2

R1(config-radius-server)# address ipv4 192.168.1.102

R1(config-radius-server)# key RADIUS-2-pa55w0rd

R1(config-radius-server)# exit

R1(config)# aaa group server radius RADIUS-GROUP

R1(config-sg-radius)# server name RADIUS-1

R1(config-sg-radius)# server name RADIUS-2

R1(config-sg-radius)# exit

R1(config)# aaa authentication login default group RADIUS-GROUP local

R1(config)# aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

R1(config)# line vty 0 4

R1(config-line)# login authentication TELNET-LOGIN

R1(config-line)# exit

R2

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R2

R2(config)#interface s1/0

R2(config-if)#ip address 10.1.1.2 255.255.255.252

R2(config-if)#no shutdown

*Dec 19 08:01:10.279: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

*Dec 19 08:01:11.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R2(config-if)#exit

R2(config)#interface s1/1

R2(config-if)#ip address 10.2.2.1 255.255.255.252

R2(config-if)#no shutdown

*Dec 19 08:02:33.002: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up

*Dec 19 08:02:34.009: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up

R2(config-if)#exit

R2(config)#exit

Configure static routes

a. **On R2, configure two static routes.**

   R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1

   R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.2

   R2#show ip route

   Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2

   i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route

   o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

      a - application route

      + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C   10.1.1.0/30 is directly connected, Serial1/0

L   10.1.1.2/32 is directly connected, Serial1/0

C   10.2.2.0/30 is directly connected, Serial1/1

L   10.2.2.1/32 is directly connected, Serial1/1

S   192.168.1.0/24 [1/0] via 10.1.1.1

S   192.168.3.0/24 [1/0] via 10.2.2.2

Secure management access

R2(config)#security passwords min-length 10

R2(config)#enable secret class12345

R2(config)#line console 0

R2(config-line)#password ciscoconpass

R2(config-line)#exec-timeout 5 0

R2(config-line)#login

R2(config-line)#logging synchronous

R2(config-line)#exit

R2(config)#line vty 0 4

R2(config-line)#password ciscovtypass

R2(config-line)#exec-timeout 5 0

R2(config-line)#login

R2(config-line)#exit

R2(config)#line aux 0

R2(config-line)#no exec

R2(config-line)#end

R2(config)#service password-encryption

R2(config)#banner motd $Unauthorized access strictly prohibited!$

R2(config)#exit

Configure enhanced username password security

R2(config)#username JR-ADMIN secret class12345

R2(config)#username ADMIN secret class54321

R2(config)#line console 0

R2(config-line)#login local

R2(config-line)#end

R2(config)#line vty 0 4

R2(config-line)#login local

R2(config-line)#end

Enabling AAA RADIUS Authentication with Local User for Backup

R2(config)# aaa new-model
R2(config)# radius server RADIUS-1
R2(config-radius-server)# address ipv4 192.168.1.101
R2(config-radius-server)# key RADIUS-1-pa55w0rd
R2(config-radius-server)# exit

R2(config)# radius server RADIUS-2

R2(config-radius-server)# address ipv4 192.168.1.102

R2(config-radius-server)# key RADIUS-2-pa55w0rd

R2(config-radius-server)# exit

R2(config)# aaa group server radius RADIUS-GROUP

R2(config-sg-radius)# server name RADIUS-1

R2(config-sg-radius)# server name RADIUS-2

R2(config-sg-radius)# exit

R2(config)# aaa authentication login default group RADIUS-GROUP local

R2(config)# aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

R2(config)# line vty 0 4

R2(config-line)# login authentication TELNET-LOGIN

R2(config-line)# exit

R3

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R3

R3(config)#interface loopback 0

*Dec 19 08:07:50.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R3(config-if)#ip address 192.168.3.1 255.255.255.0

R3(config-if)#exit

R3(config)#interface s1/0

R3(config-if)#ip address 10.2.2.2 255.255.255.252

R3(config-if)#no shutdown

R3(config-if)#exit

*Dec 19 08:09:26.986: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

*Dec 19 08:09:27.996: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R3(config)#end

Configure static routes

a. **On R3, configure a default static route to ISP.**

   R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.1

   R3#show ip route

   Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2

   i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

   ia - IS-IS inter area, * - candidate default, U - per-user static route

   o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

   a - application route

   + - replicated route, % - next hop override

   Gateway of last resort is 10.2.2.1 to network 0.0.0.0

   S*   0.0.0.0/0 [1/0] via 10.2.2.1

   10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

   C   10.2.2.0/30 is directly connected, Serial1/0

   L   10.2.2.2/32 is directly connected, Serial1/0

   192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks

   C   192.168.3.0/24 is directly connected, Loopback0

L   192.168.3.1/32 is directly connected, Loopback0

Secure management access

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 ciscovtypass

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(config)#service password-encryption

R3(config)#banner motd $Unauthorized access strictly prohibited!$

Configure enhanced username password security

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)#exit

Enabling AAA RADIUS Authentication with Local User for Backup

R3(config)# aaa new-model

R3(config)# radius server RADIUS-1

R3(config-radius-server)# address ipv4 192.168.1.101

R3(config-radius-server)# key RADIUS-1-pa55w0rd

R3(config-radius-server)# exit

R3(config)# radius server RADIUS-2

R3(config-radius-server)# address ipv4 192.168.1.102

R3(config-radius-server)# key RADIUS-2-pa55w0rd

R3(config-radius-server)# exit

R3(config)# aaa group server radius RADIUS-GROUP

R3(config-sg-radius)# server name RADIUS-1

R3(config-sg-radius)# server name RADIUS-2

R3(config-sg-radius)# exit

R3(config)# aaa authentication login default group RADIUS-GROUP local

R3(config)# aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

R3(config)# line vty 0 4

R3(config-line)# login authentication TELNET-LOGIN

R3(config-line)# exit