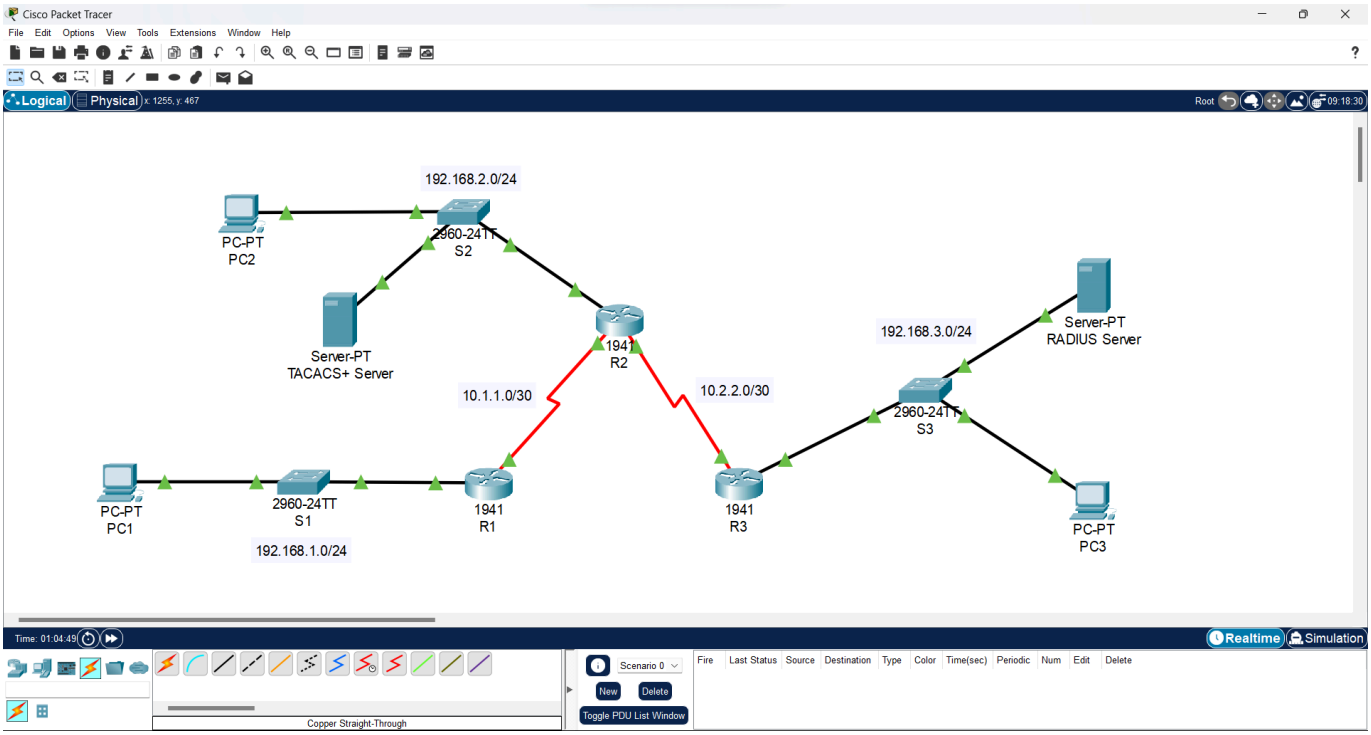
Security in Computing
Practical - 2

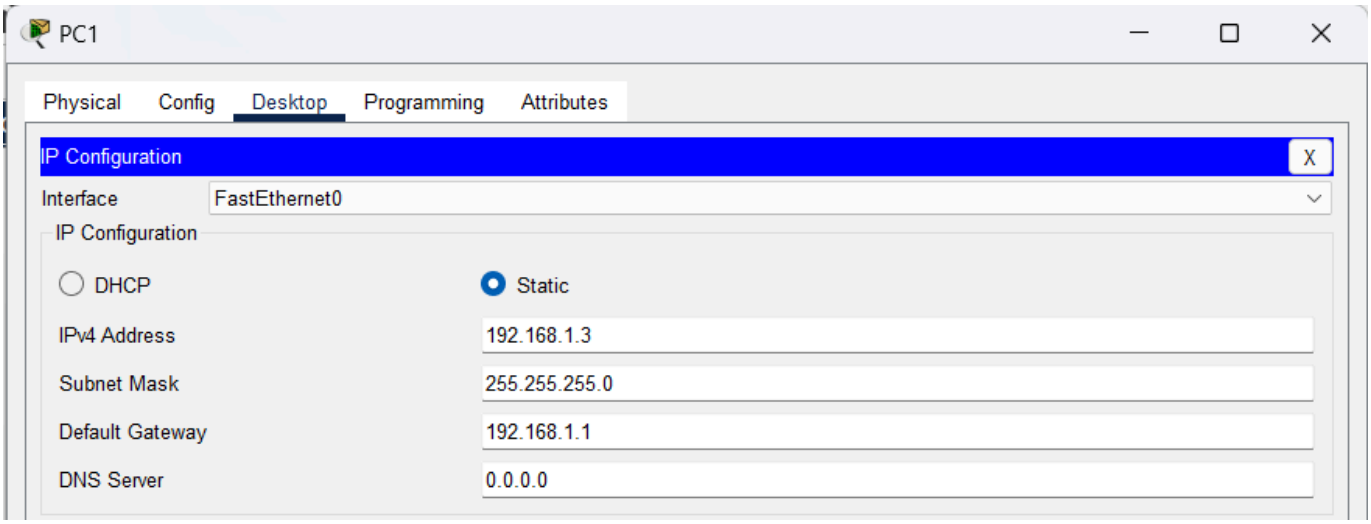
➢Aim: Configure AAA Authentication

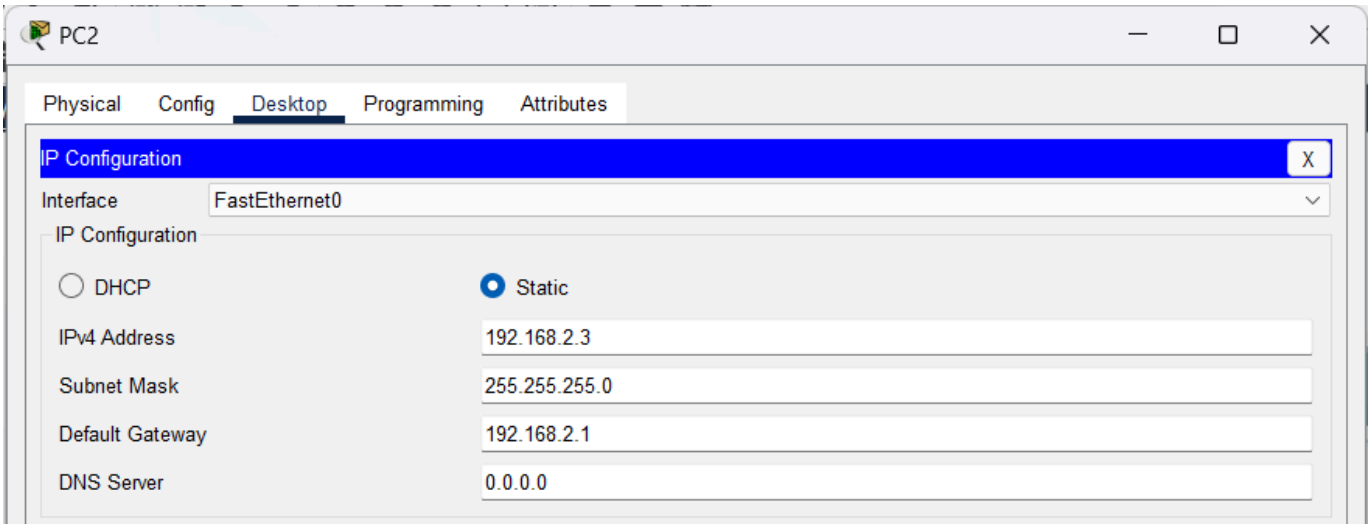
a. Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA.
b. Verify local AAA authentication from the Router console and the PC1 client.

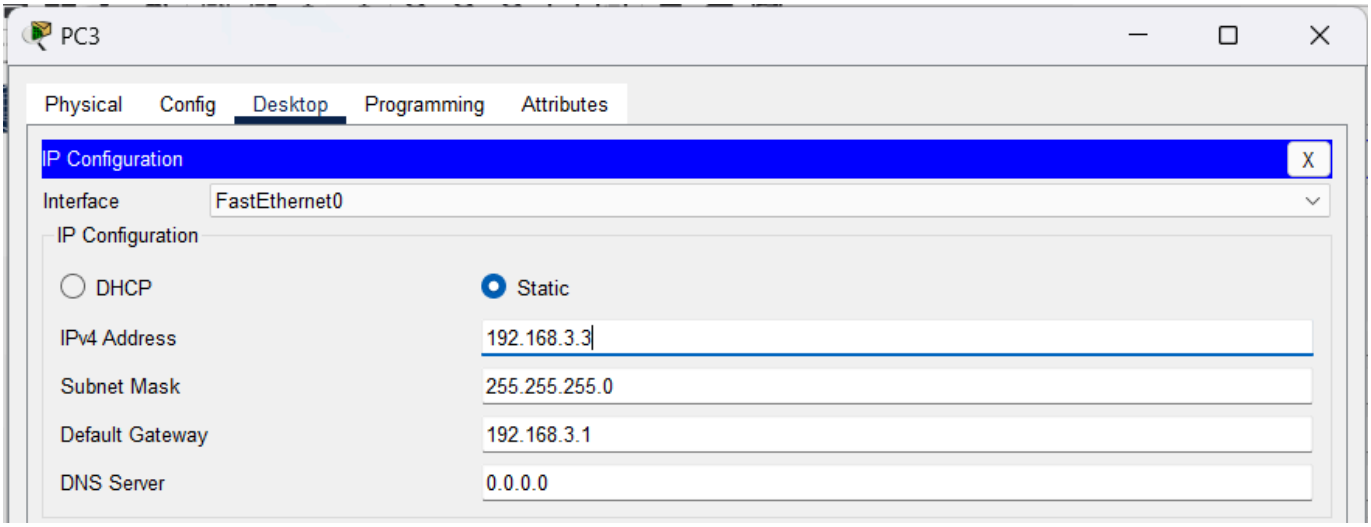
Topology Diagram:

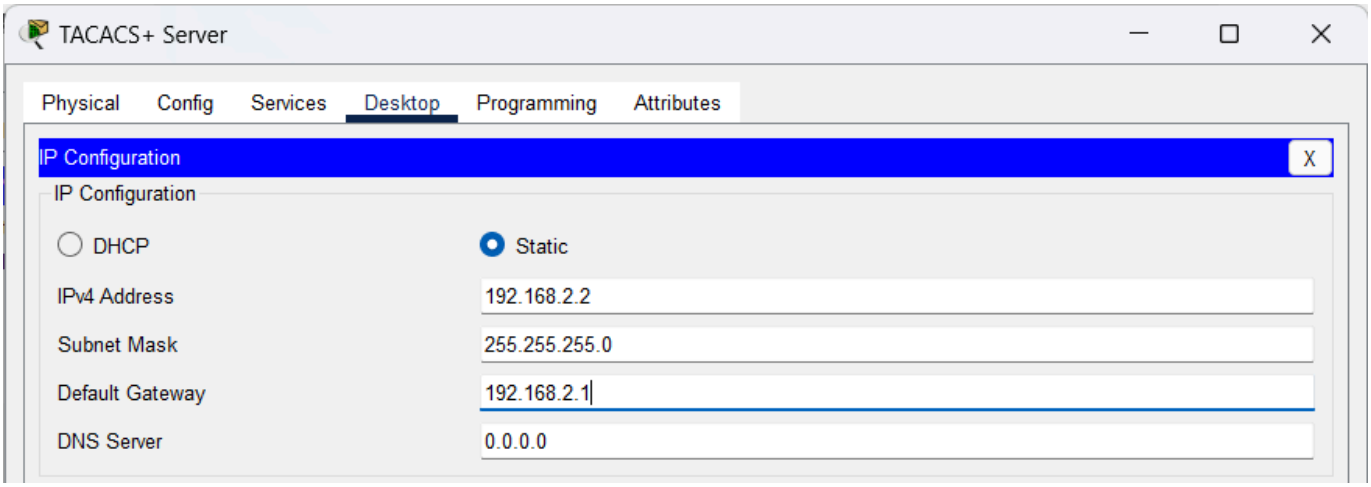


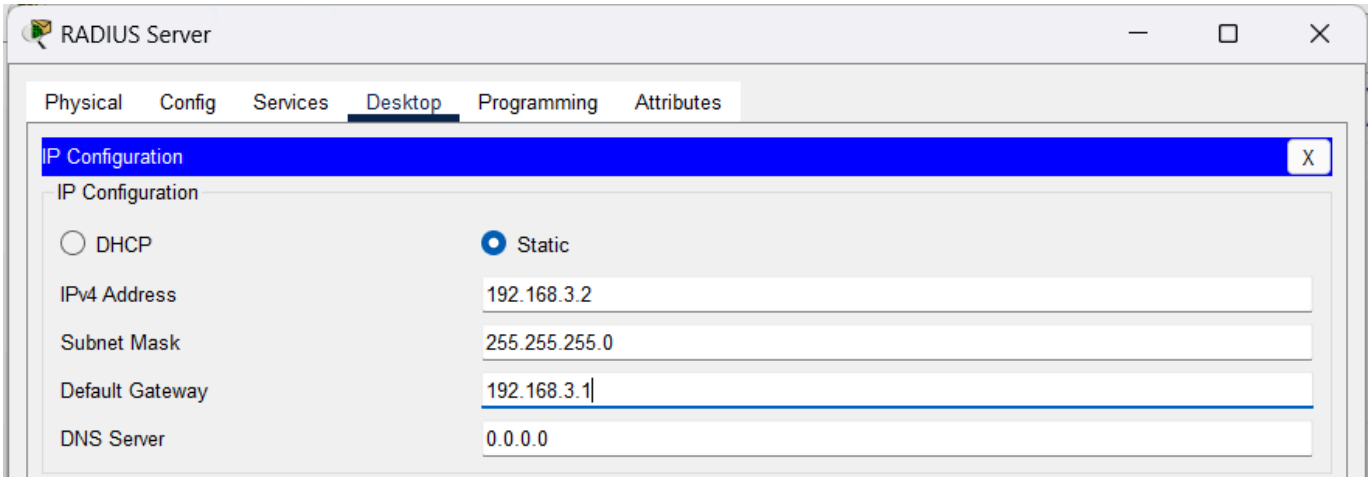
Assign IP Addresses:




PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0


TACACS+ Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0




```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R1
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.2 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R2
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.1 255.255.255.252
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.1 255.255.255.252
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R3
R3(config)#interface GigabitEthernet0/1
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R3(config-if)#interface Serial0/0/1
R3(config-if)#ip address 10.2.2.2 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Displaying IP Address details of Routers:

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     192.168.1.1     YES manual up                    up
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down

R2>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down

R3>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     192.168.3.1     YES manual up                    up
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            10.2.2.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Configure RIP on Routers:

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit


R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 10.2.2.0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit


R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 192.168.3.0
R3(config-router)#network 10.2.2.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Displaying Routing Tables of Routers:

```
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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.1, 00:00:02, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R    192.168.2.0/24 [120/1] via 10.1.1.1, 00:00:02, Serial0/0/0
R    192.168.3.0/24 [120/2] via 10.1.1.1, 00:00:02, Serial0/0/0
```

```
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, E - EGP
       i - IS-IS, 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

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, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/1] via 10.1.1.2, 00:00:11, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
R    192.168.3.0/24 [120/1] via 10.2.2.2, 00:00:25, Serial0/0/1
```

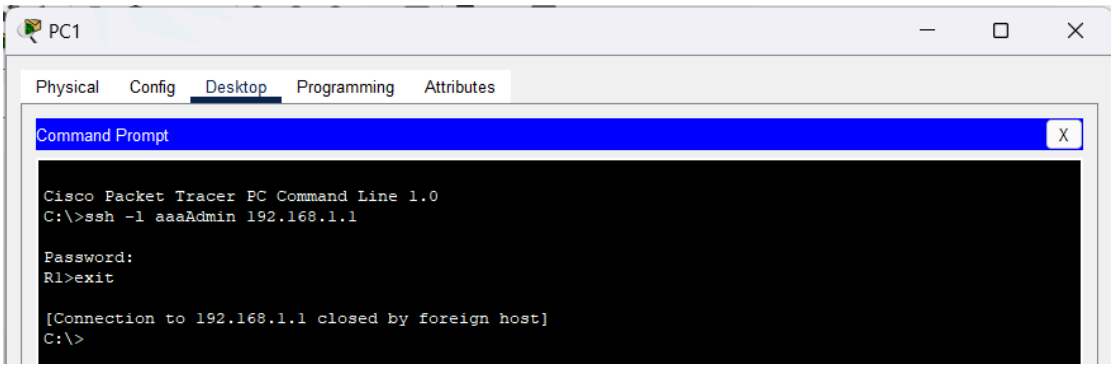
```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    192.168.1.0/24 [120/2] via 10.2.2.1, 00:00:10, Serial0/0/1
R    192.168.2.0/24 [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1
```

Configure Local AAA Authentication for Console Lines on R1:

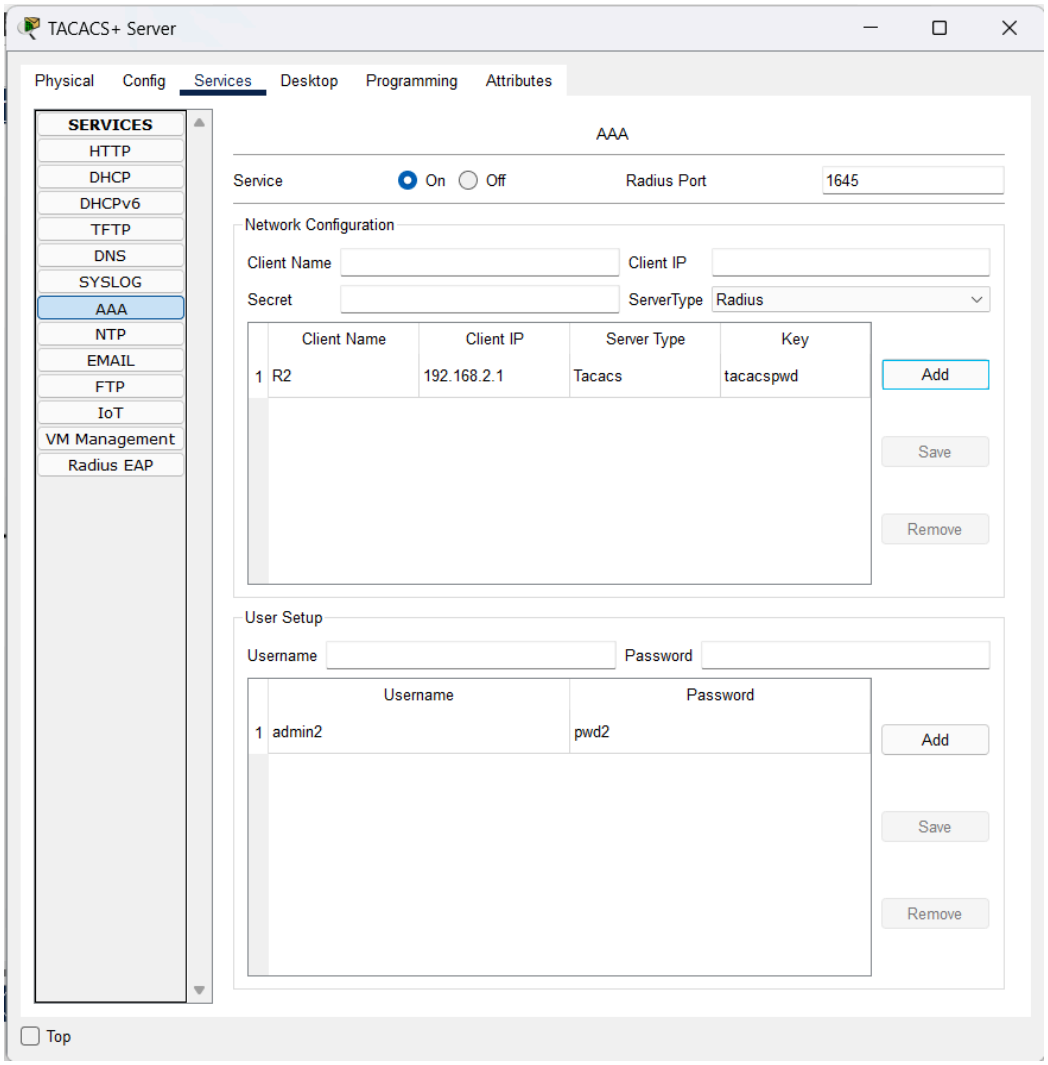
```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username aaaAdmin secret aaapwd
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit

                User Access Verification

                Username: aaaAdmin
                Password:
                R1>
```

Configure Local AAA Authentication for VTY Lines on R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name sic.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.sic.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
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#aaa authentication login SSH-LOGIN local
*Mar 1 0:44:16.390: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

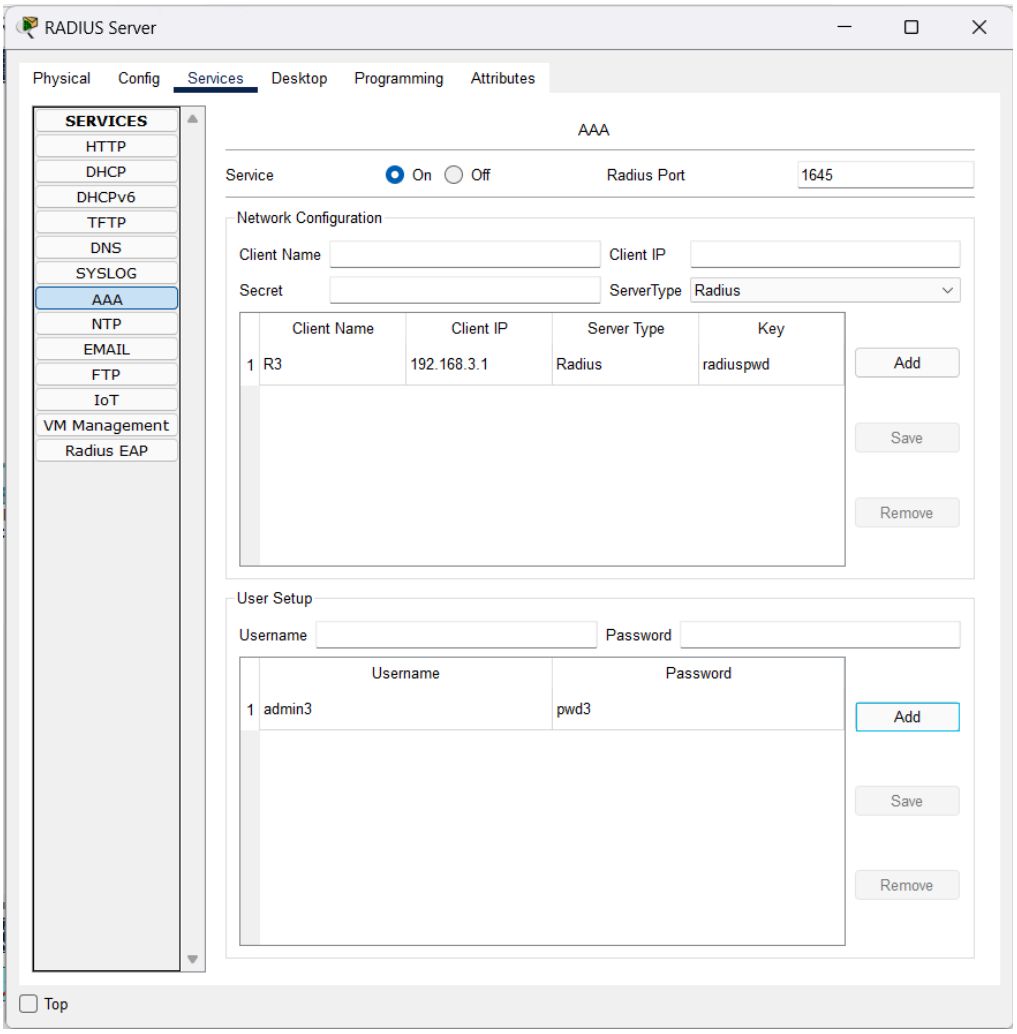


Configure Server-Based AAA Authentication Using TACACS+ on R2:




```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username admin2 secret pwd2
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspwd
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#line console 0
R2(config-line)#login authentication default
R2(config-line)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit


                User Access Verification

                Username: admin2
                Password:
                R2>
```

Configure Server-Based AAA Authentication Using RADIUS on R3:




```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username admin3 secret pwd3
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspwd
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit

                User Access Verification

                Username: admin3
                Password:
                R3>
```