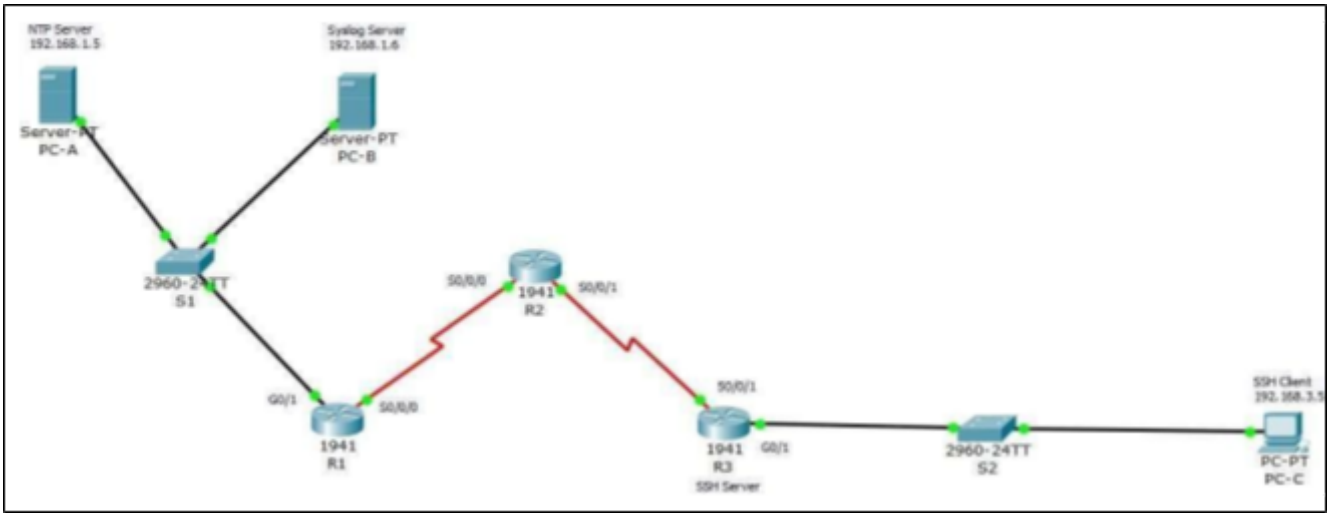
BSITP602

Name :Harsh Kadu Roll No : 33

PRACTICAL 1

Aim : Configure Cisco Routers for Syslog, NTP, and SSH Operations.



Addressing Table :

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6

Name :Harsh Kadu Roll No : 33

PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

Step 1: Place the components as shown in the figure above and setup a network . It is necessary to configure each components placed in the network . Use proper connection wire to connect between the devices.

To Configure Server PC-A (NTP Server), PC-B (Syslog server), PC-C (SSH Client):

Click on PC-A → Select Desktop Tab → Click on IP Configuration → Give IP Address as

(192.168.1.5) → Subnet mask will automatically appear (255.255.255.0) → Give default gateway as (192.168.1.1).

Click on PC-B → Select Desktop Tab → Click on IP Configuration → Give IP Address as

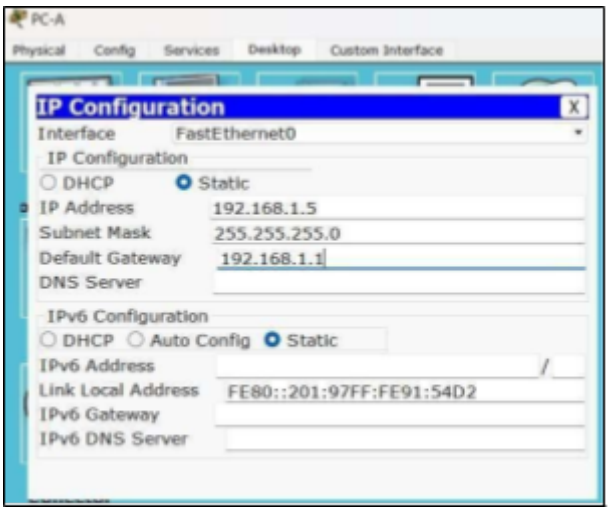
(192.168.1.6) → Subnet mask will automatically appear (255.255.255.0) → Give default gateway as (192.168.1.1).

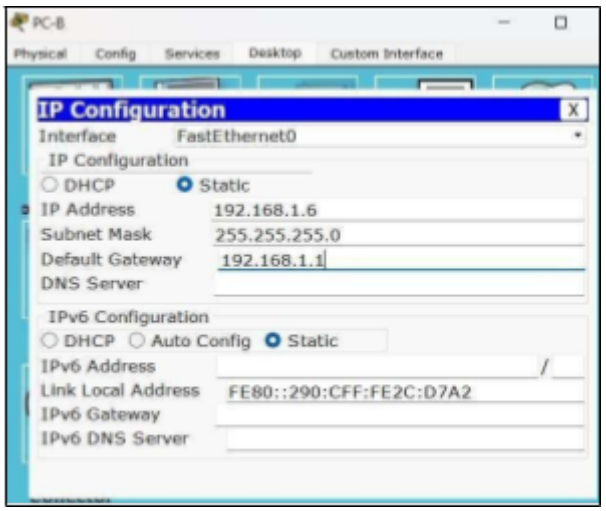
Click on PC-C → Select Desktop Tab → Click on IP Configuration → Give IP Address as

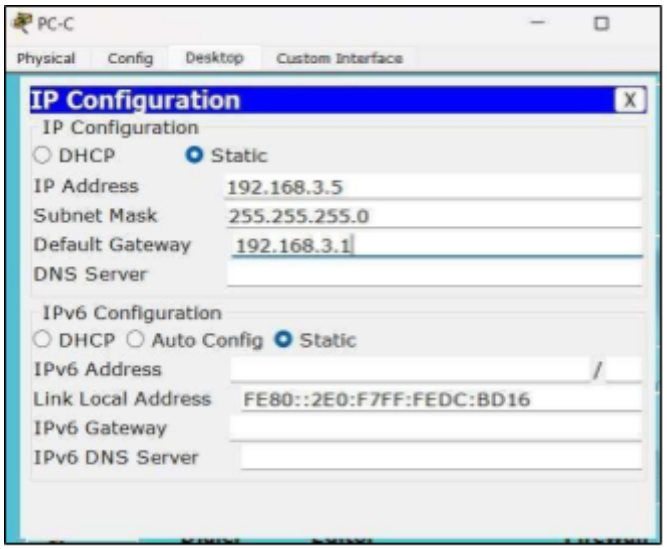
(192.168.3.5) → Subnet mask will automatically appear (255.255.255.0) → Give default gateway as (192.168.3.1).

BSITP602

Name :Harsh Kadu Roll No : 33





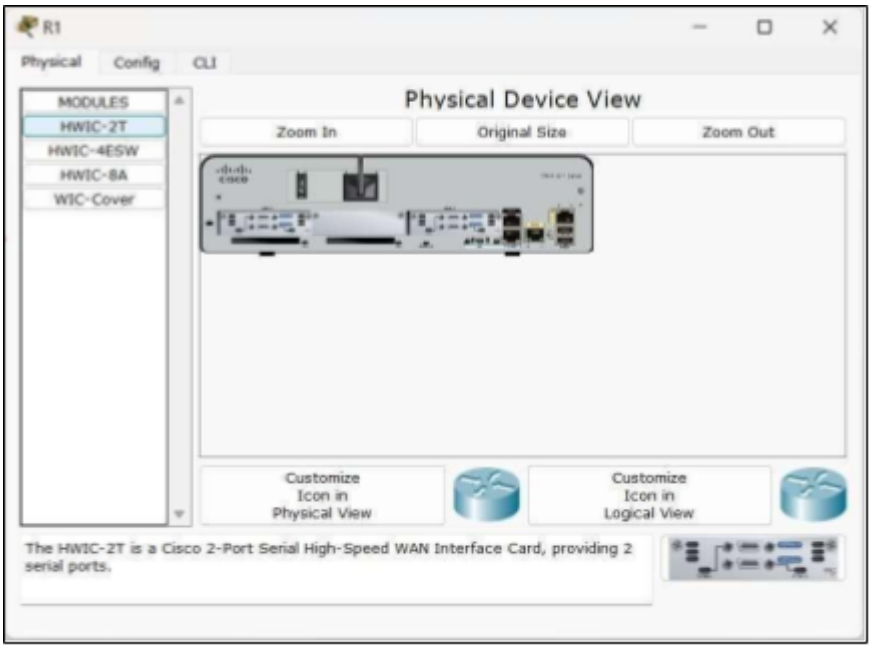


To Configure Routers R1, R2, R3 :

As given in the addressing table we require two more serial ports with S0/0/0 and S0/0/1. To add these ports go to each Router. Click on Router 1→ Go to Physical tab → Click on HWIC-2T

→ In the Physical Device View power off the machine and add 2 serial ports in the slot → Once placed power on the machine and go to config option to see whether the ports

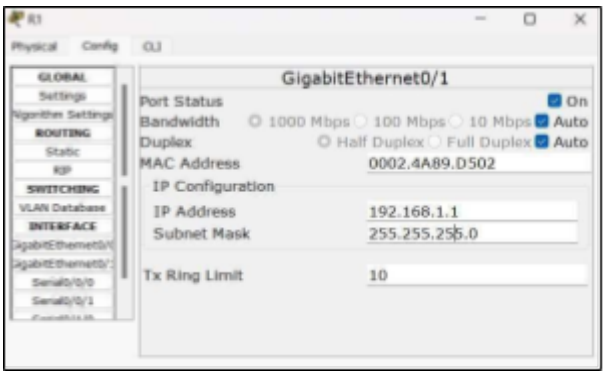
are added → It will ask to wait since the device is in booting mode → Once booting process gets completed you can see the ports which we have added.

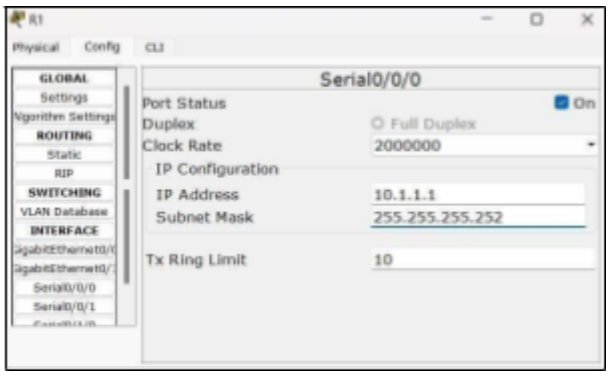


Now we can Configure the routers according to the Serial ports given in the addressing table.

Click on Router R1 → Go to Config tab → Click on GigabitEthernet0/1 → Give IP Address as (192.168.1.1) → Subnet mask will automatically appear (255.255.255.0) → Port Status ON → Again Click on S0/0/0 → Give IP Address as (10.1.1.1) → Give Subnet mask as (255.255.255.252) → Port Status ON.

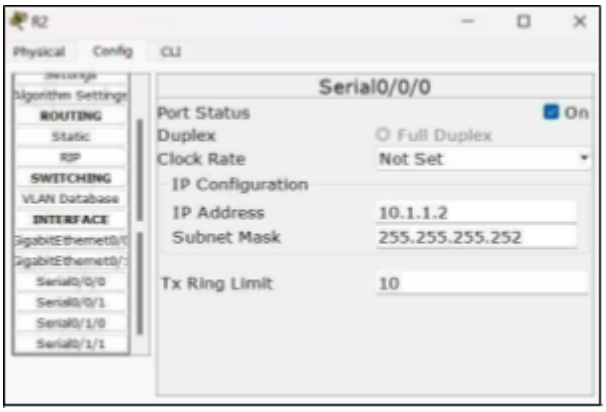
Name :Harsh Kadu Roll No : 33

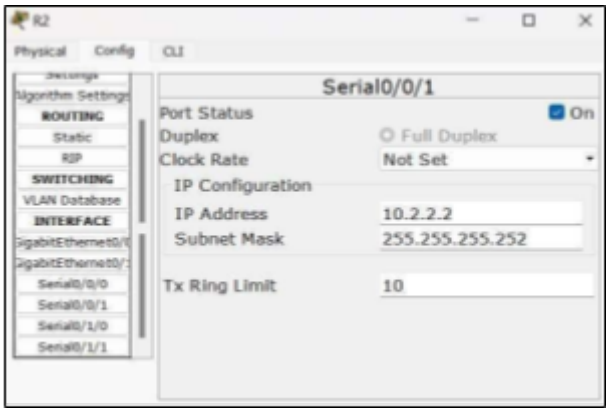




Click on Router R2 → Go to Config tab → Click on S0/0/0 → Give IP Address as (10.1.1.2)

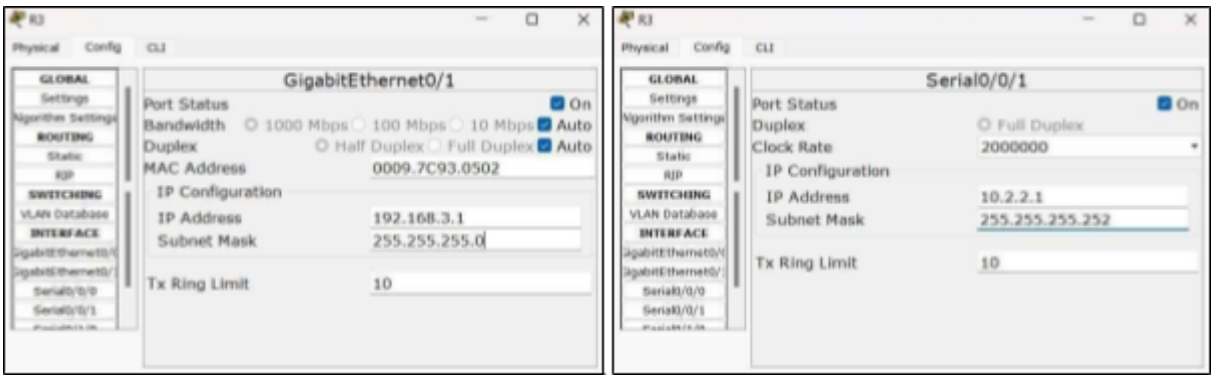
→ Subnet mask will automatically appear (255.255.255.252) → Port Status ON → Again Click on S0/0/1 → Give IP Address as (10.2.2.2) → Subnet mask will automatically appear (255.255.255.252) → Port Status ON.



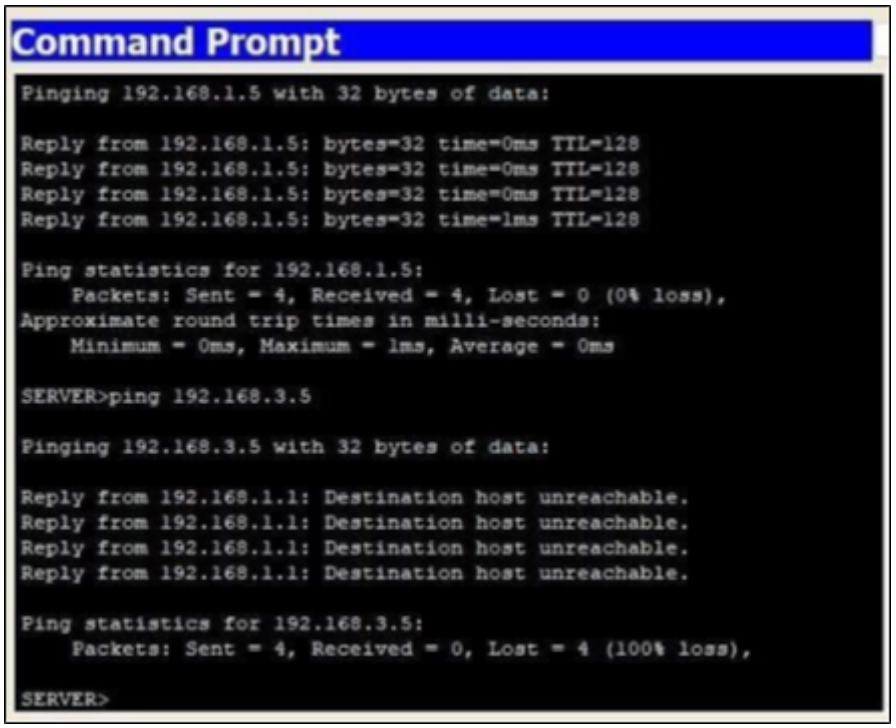


Click on Router R3 → Go to Config tab → Click on GigabitEthernet0/1 → Give IP Address as (192.168.3.1) → Subnet mask will automatically appear (255.255.255.0) → Port Status ON → Again Click on S0/0/1 → Give IP Address as (10.2.2.1) → Subnet mask will automatically appear (255.255.255.252) → Port Status ON.

Name :Harsh Kadu Roll No : 33



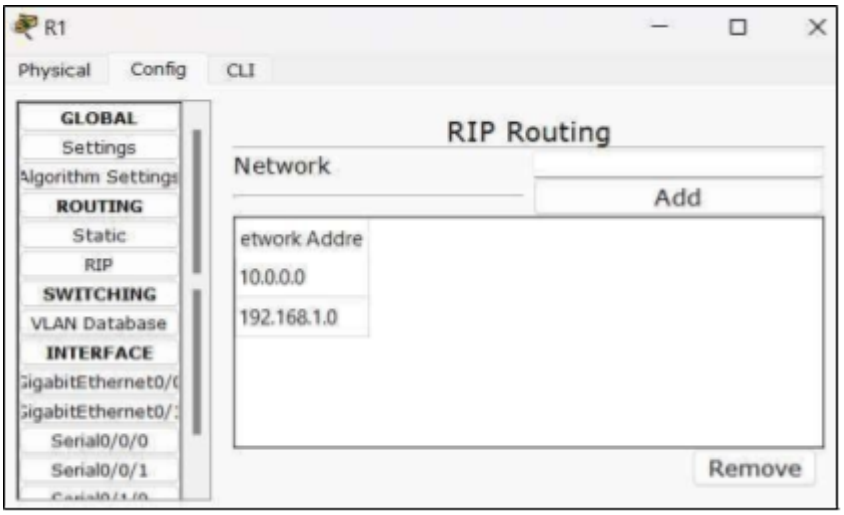
Check whether devices are able to communicate from one network to another. Click on PC-A → Go to desktop option → Go to Command prompt → enter the command as shown below:



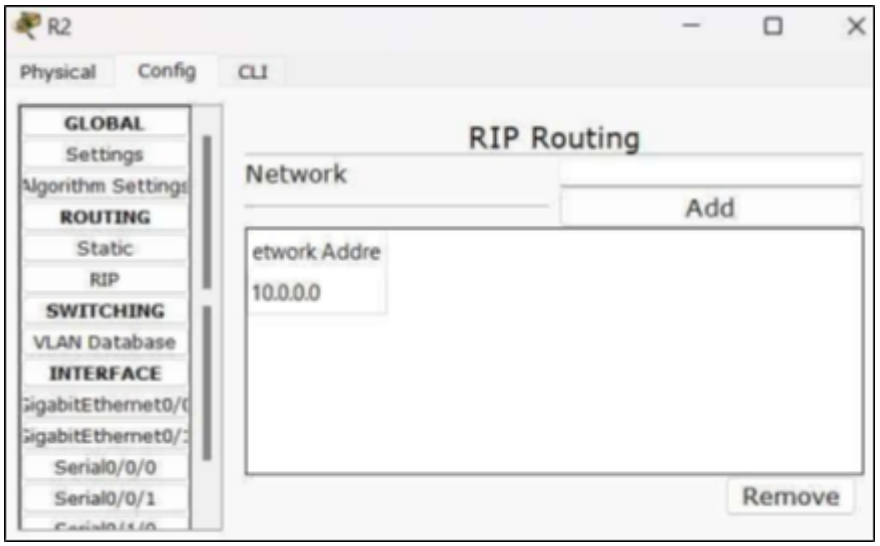
If this fails we have to do static RIP routing on R1, R2, R3 to connect from one network to another .

Name :Harsh Kadu Roll No : 33

Click on Router R1 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (192.168.1.0 , 10.0.0.0) in RIP routing .



Click on Router R2 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (10.0.0.0, 10.0.0.0) in RIP routing .

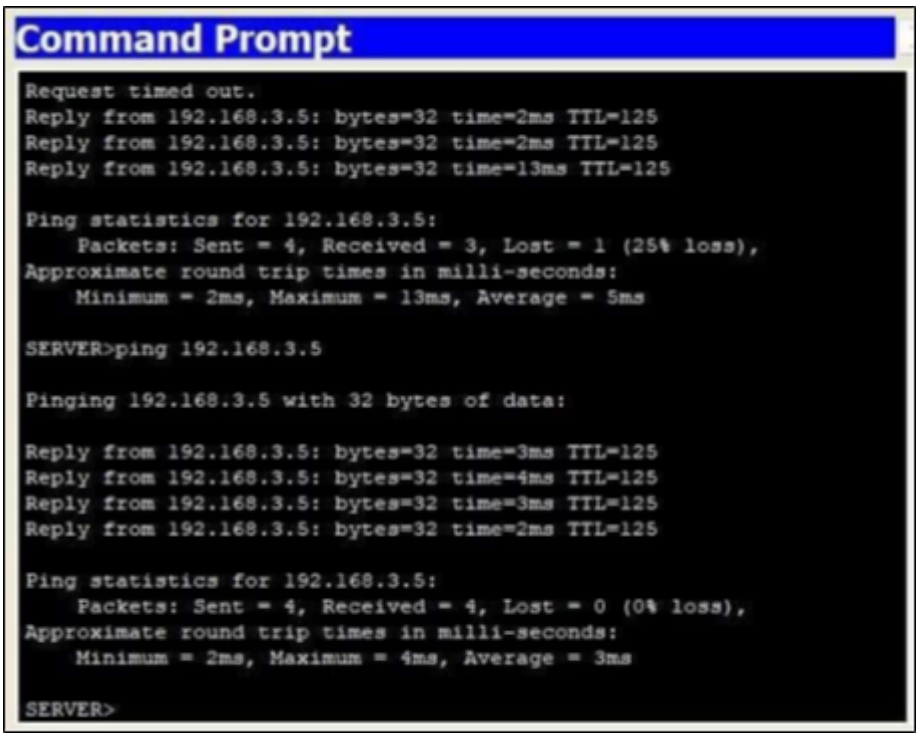


Name :Harsh Kadu Roll No : 33

Click on Router R3 → Go to Config tab → Click on RIP → Give network address as per addressing table. → Add these two network addresses (192.168.3.0, 10.0.0.0) in RIP routing .

Now check whether the devices are connected from one network to another once connection is done.

Name :Harsh Kadu Roll No : 33

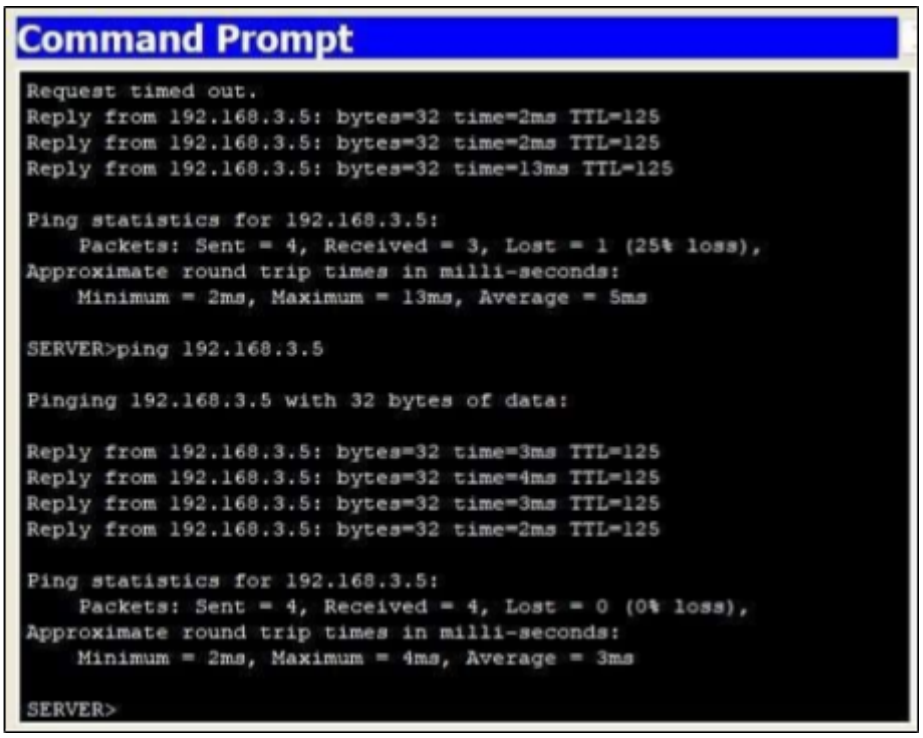


Since its now get connected and we can share messages from one network to another and further Operation can be performed . Hence it is necessary to configure devices within network and outside the network to do further operations on it.

Part 1 : Configure OSPF MD5 Authentication

Step 1 : Test the connectivity. All devices should be able to ping with all other IP addresses connected in the network . Go to PC - A → click on desktop → click on command prompt → type the following command: → We will get reply as Destination host unreachable.

Name :Harsh Kadu Roll No : 33



Step 2 : Configure OSPF MD5 authentication for all the routers in area 0 .

Go to Router R1 → Click on CLI tab → Type the following Commands :

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
```

Go to Router R2 → Click on CLI tab → Type the following Commands :

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
```

Name :Harsh Kadu Roll No : 33

Go to Router R3 → Click on CLI tab → Type the following Commands :

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
```

Step 3 : Configure an MD5 key on the serial interfaces on R1, R2 and R3 . Use the password MD5pa55.

Go to Router R1 → Click on CLI tab → Type the following Commands :

```
R1(config)#interface se0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

Go to Router R2 → Click on CLI tab → Type the following Commands :

```
R2(config)#interface se0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

```
R2(config)#interface se0/0/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

Go to Router R3 → Click on CLI tab → Type the following Commands :

```
R3(config)#interface se0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

Step 4 : Verify MD5 authentication configuration of each router and verify end-to-end connectivity.

Router R1 :

Go to Router R1 → Click on CLI → Type the following command:

Name :Harsh Kadu Roll No : 33

```
R1>show ip ospf interface se0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Router R2 :

Go to Router R2 → Click on CLI → Type the following commands:

```
R2>show ip ospf interface se0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost:
64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Name :Harsh Kadu Roll No : 33

```
R2>show ip ospf interface se0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost:
64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Router R3 :

Go to Router R3 → Click on CLI → Type the following commands:

```
R3>show ip ospf interface se0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.1/30, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Part 2 : Configure NTP

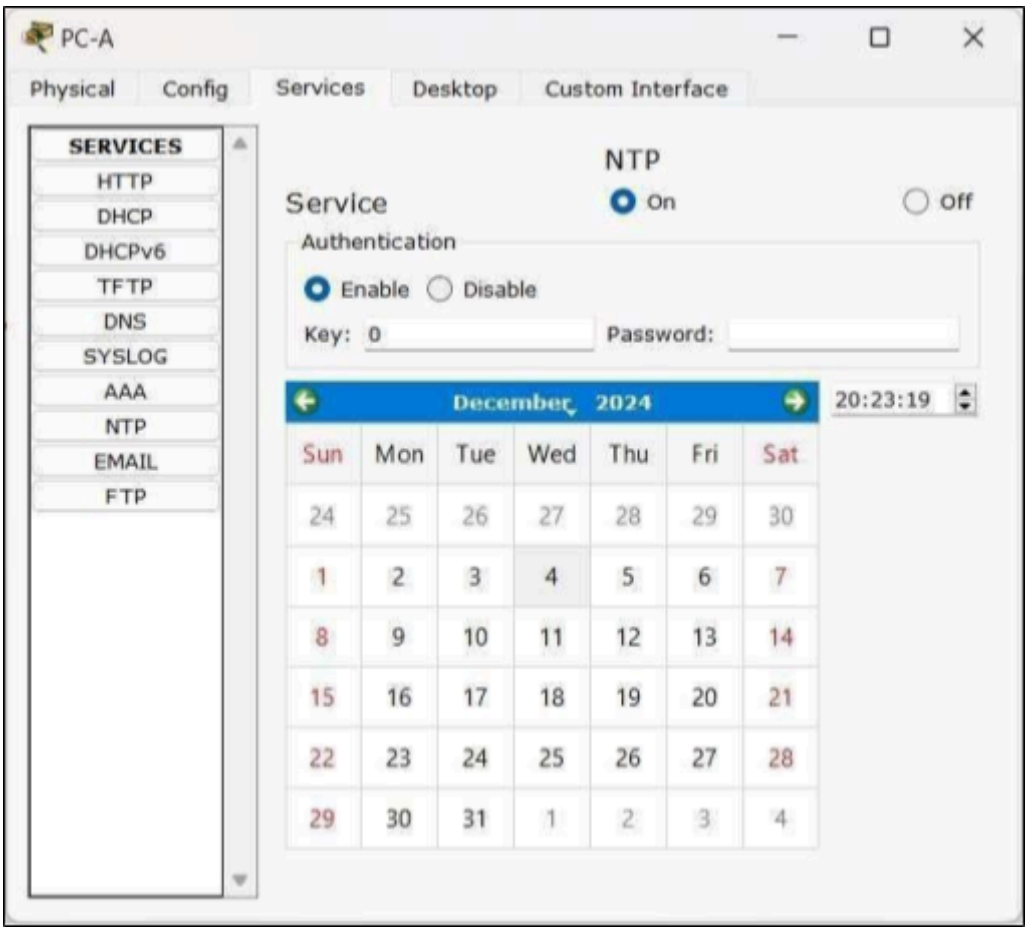
Step 1 :

Name :Harsh Kadu Roll No : 33

a. On PC-A, Click NTP under the Services tab to verify NTP service is enabled.

b. To configure NTP authentication, click Enable under authentication. Use key 1 and password NTPpa55 for authentication.

Go to NTP server → Services Tab → Under Services Pannel → Select NTP → Make it ON.



Step 2 : Configure R1, R2, and R3 as NTP Clients and Configure routers to update hardware clock .

Router 1 :

Go to Router R1 → Click on CLI → Type the following commands:

Name :Harsh Kadu Roll No : 33

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
```

Router 2 :

Go to Router R2 → Click on CLI → Type the following commands:

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
```

Router 3 :

Go to Router R3 → Click on CLI → Type the following commands:

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ntp server 192.168.1.5
R3(config)#ntp update-calendar
```

Exit global configuration and verify that the hardware clock was updated using the following command :

Router 1 :

```
R1>show clock
*20:28:41.373 UTC Wed Dec 4 2024
```

Router 2 :

```
R2>show clock
*20:31:55.717 UTC Wed Dec 4 2024
```

Name :Harsh Kadu Roll No : 33

Router 3 :

```
R3>show clock
*20:34:6.246 UTC Wed Dec 4 2024
```

Step 3 : Configure NTP authentication on the routers and to configure routers to timestamp log messages.

Router 1 :

Go to Router R1 → Click on CLI → Type the following commands:

```
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate-key 1 md5 NTPpwd
                                 ^
% Invalid input detected at '^' marker.

R1(config)#ntp authentication-key 1 md5 NTPpwd
R1(config)#service timestamps log datetime msec
```

Router 2 :

Go to Router R2 → Click on CLI → Type the following commands:

```
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authenticate-key 1 md5 NTPpwd
                                 ^
% Invalid input detected at '^' marker.

R2(config)#ntp authentication-key 1 md5 NTPpwd
R2(config)#service timestamps lo datetime msec
```

Router 3 :

Go to Router R2 → Click on CLI → Type the following commands:

Name :Harsh Kadu Roll No : 33

```
R3(config)#ntp authenticate
R3(config)#ntp trusted-key 1
R3(config)#ntp authentication-key 1 md5 NTPpwd
R3(config)#service timestamps log datetime msec
```

Step 4 : Verify client configuration using the following command on each router

Router 1 :

Go to Router R1 → Click on CLI → Type the following commands:

```
R1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**19
reference time is EACD1484.000001F9 (20:24:36.505 UTC Wed Dec 4 2024)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

Router 2 :

Go to Router R2 → Click on CLI → Type the following commands:

```
R2#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**19
reference time is EACD15B7.0000008E (20:29:43.142 UTC Wed Dec 4 2024)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

Router 3 :

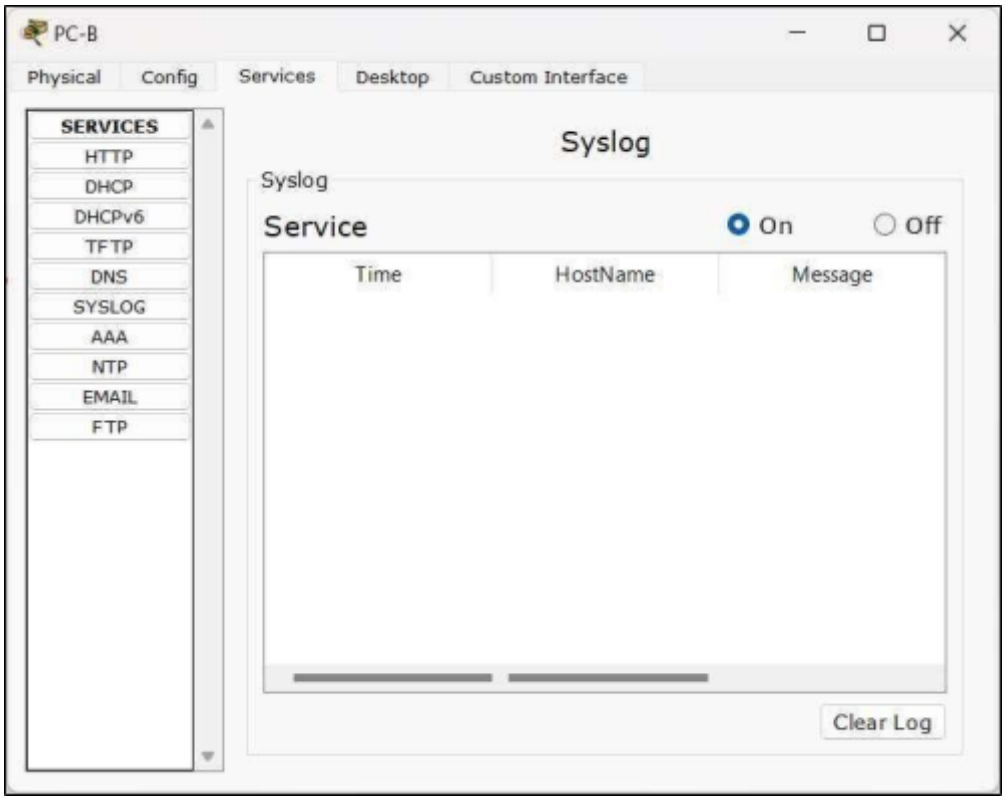
Go to Router R3 → Click on CLI → Type the following commands:

```
R3#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**19
reference time is EACD1657.00000396 (20:32:23.918 UTC Wed Dec 4 2024)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

Name :Harsh Kadu Roll No : 33

Part 3 : Configure Routers to Log Messages to the Syslog Server

Step 1 : Go to SYSLOG server → Services Tab → Under Services Pannel → Select SYSLOG option → Make it ON. There will be empty logs . By logging into each device we will able to see the logins in the box.



Step 2 : Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

Router R1:

Go to Router R1 → CLI Tab → Type commands as follows:

Name :Harsh Kadu Roll No : 33

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#logging host 192.168.1.6
```

Router R2:

Go to Router R2 → CLI Tab → Type commands as follows:

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#logging host 192.168.1.6
```

Router R3:

Go to Router R3 → CLI Tab → Type commands as follows:

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#logging host 192.168.1.6
```

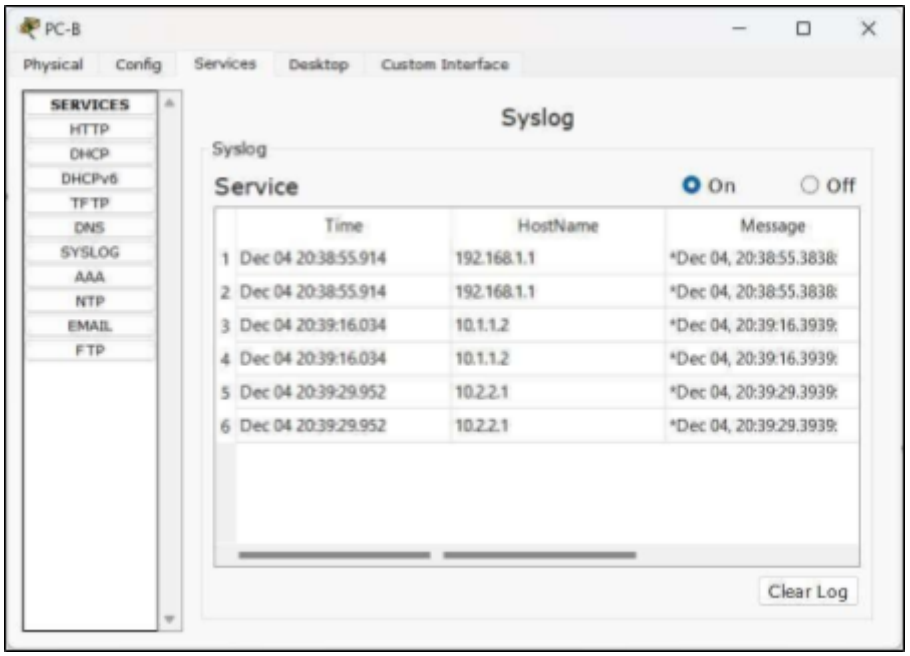
Step 3 : Verify Logging configuration.

Use the command show logging on on each routers to verify logging has been enabled.

Name :Harsh Kadu Roll No : 33

Step 4 : Examine logs of the Syslog Server.

Go to SYSLOG server → Services Tab → Under Services Pannel → Select SYSLOG option → Observe the logging messages received from the routers.



Part 4 : Configure R3 to support SSH Connections

Step 1: Configure a domain name of ccnasecurity.com on R3.

Go to Router R3 → CLI Tab → Type commands as follows:

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip domain-name ccnasecurity.com
```

Step 2: Configure users for login to SSH server on R3 and the incoming vty lines on R3.

Create user id of SSHadmin with the highest privilege level and a secret password of ciscosshpa55. And accept only SSH connections

Name :Harsh Kadu Roll No : 33

Go to Router R3 → CLI Tab → Type commands as follows:

```
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
```

Step 4 : Erase existing key pairs on R3 and generate the RSA encryption key pair for R3.

Go to Router R3 → CLI Tab → Type commands as follows:

```
R3(config)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 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]

R3(config)#
```

Step 5 : Verify the SSH configuration

```
R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

Step 6 : Configure SSH timeouts and authentication parameters.

Go to Router R3 → CLI Tab → Type commands as follows:

```
R3(config)#ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#
```

Name :Harsh Kadu Roll No : 33

Step 7 : Attempt to connect to R3 via Telnet from PC-C.

Open Desktop of PC-C → Click on Command Prompt icon → Enter the command to connect to R3 via Telnet .

This connection should fail because R3 has been configured to accept only SSH connections on the virtual terminal lines.

Step 8 : Connect to R3 using SSH on PC-C

Open Desktop of PC-C → Click on Command Prompt icon → Enter the command to connect to R3 via SSH → When prompted for the password, enter the password configured for the administrator 'ciscosshpa55' .

Step 9 : Connect to R3 using SSH on R2 .

To troubleshoot and maintain R3, the administrator at the ISP must use SSH to access the router CLI.

Click on Router → R2 Go to CLI tab → Enter the command to connect to R3 via SSH version

2 using the SSHadmin user account → When prompted for the password, enter the password configured for the administrator ciscosshpa55.

Name :Harsh Kadu Roll No : 33

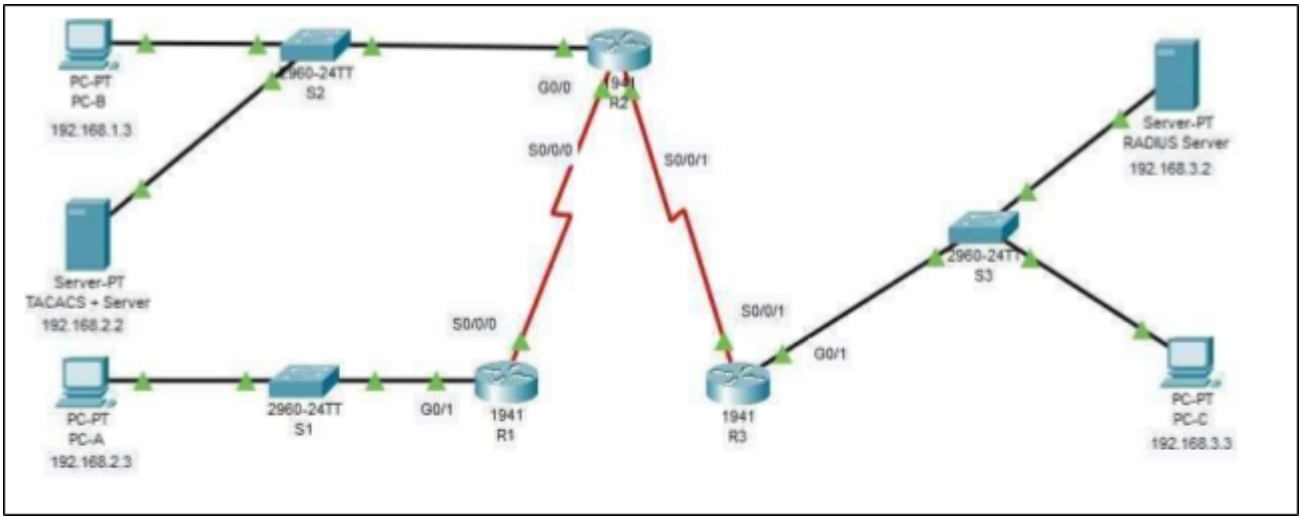
```
R2>enable
R2#ssh -v 2 -l SSHadmin 10.2.2.1
Open
Password:



R3#
```

BSITP602

Name :Harsh Kadu Roll No : 33

PRACTICAL 2

Aim : Configure AAA Authentication on Cisco Routers.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS + Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6

BSITP602

Name :Harsh Kadu Roll No : 33

RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2

PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Step 1 : Place the components as shown in the figure above and setup a network . It is necessary to configure each components placed in the network . Use proper connection wire to connect between the devices.

Step 2 : Test the Connectivity between the devices and see whether they are able to communicate with each other.

Click on PC-B → Go to desktop option → Go to Command prompt → enter the command as shown below:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

If this fails we have to do static routing on routers to connect devices with another.

Name :Harsh Kadu Roll No : 33

Step 3 : Configure RIP routing on all routers.

For Router R1:

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1>enable
R1#
R1#configure terminal
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 10.0.0.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

```
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, 00:00:11, 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, 00:00:11, Serial0/0/0
R    192.168.3.0/24 [120/2] via 10.1.1.1, 00:00:11, Serial0/0/0
```

For Router R2:

Click on Router R2 → Go to CLI tab → And the following commands :

Name :Harsh Kadu Roll No : 33

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.2.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
```

```
Router>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, 00:00:28, Serial0/0/1
```

For Router R3:

Click on Router R3 → Go to CLI tab → And the following commands :

Name :Harsh Kadu Roll No : 33

```
R3>enable
R3#
R3#configure terminal
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 10.0.0.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

```
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, 00:00:21, 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, 00:00:21, Serial0/0/1
R    192.168.2.0/24 [120/1] via 10.2.2.1, 00:00:21, 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
```

Step 4 : Now Test the connectivity between the devices.

Ping from PC-A to PC-B

Name :Harsh Kadu Roll No : 33

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=11ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms
```

Since its now get connected and we can share messages from one network to another and further Operation can be performed . Hence it is necessary to configure devices within network and outside the network to do further operations on it.

Part 1 : Configure Local AAA Authentication for Console Access on R1

Step 1 : Test Connectivity.

- Ping from PC-A to PC-B.

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=11ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms
```

- Ping from PC-A to PC-C.

Name :Harsh Kadu Roll No : 33

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=13ms TTL=125
Reply from 192.168.3.3: bytes=32 time=8ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 8ms
```

- Ping from PC-B to PC-C.

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 8ms
```

Step 2 : Configure a local username on R1.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username Admin1 secret admin1pa55
```

Step 3 : Configure a local AAA authentication for console access on R1.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
```

Name :Harsh Kadu Roll No : 33

Step 4 : Configure the line console to use the defined AAA authentication method.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1(config)#line console 0
R1(config-line)#login authentication default
```

Step 5 : Verify the AAA authentication method.

Verify the user EXEC login using the local database.

Click on Router R1 → Go to CLI tab → And the following commands :

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

R1#exit
```

Authorized access are only allowed. After exiting from the privilege mode it will ask for user access verification. Give proper username and password :

```
User Access Verification

Username: Admin1
Password:
R1>
```

Part 2 : Configure Local AAA Authentication for vty Lines on R1.

Step 1 : Configure domain name and crypto key for use with SSH.

Create a RSA crypto key using 1024 bits.

Click on Router R1 → Go to CLI tab → And the following commands :

Name :Harsh Kadu Roll No : 33

```
User Access Verification

Username: Admin1
Password:
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name ccnasecurity.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 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 1:31:38.347: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 2 : Configure a named list AAA authentication method for the vty lines on R1.

Click on Router R1 → Go to CLI tab → And the following commands :

```
R1(config)#AAA authentication login SSH-LOGIN local
*Mar 1 1:31:38.347: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 3 : Configure the vty lines to use the defined AAA Authentication method.

Click on Router R1 → Go to CLI tab → And the following commands :

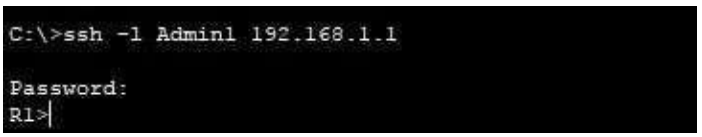
```
R1(config)#line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input SSH
R1(config-line)#end
```

Step 4 : Verify the AAA authentication method.

Verify the SSH configuration SSH to R1 from the command prompt of PC-A.

Go to PC-A → Click on Desktop tab → Click on Command prompt → and type the following command :

Name :Harsh Kadu Roll No : 33



Name :Harsh Kadu Roll No : 33

Part 3 : Configure Server-Based AAA Authentication Using TACACS+ on R2.

Step 1 : Configure a backup local database entry called Admin.

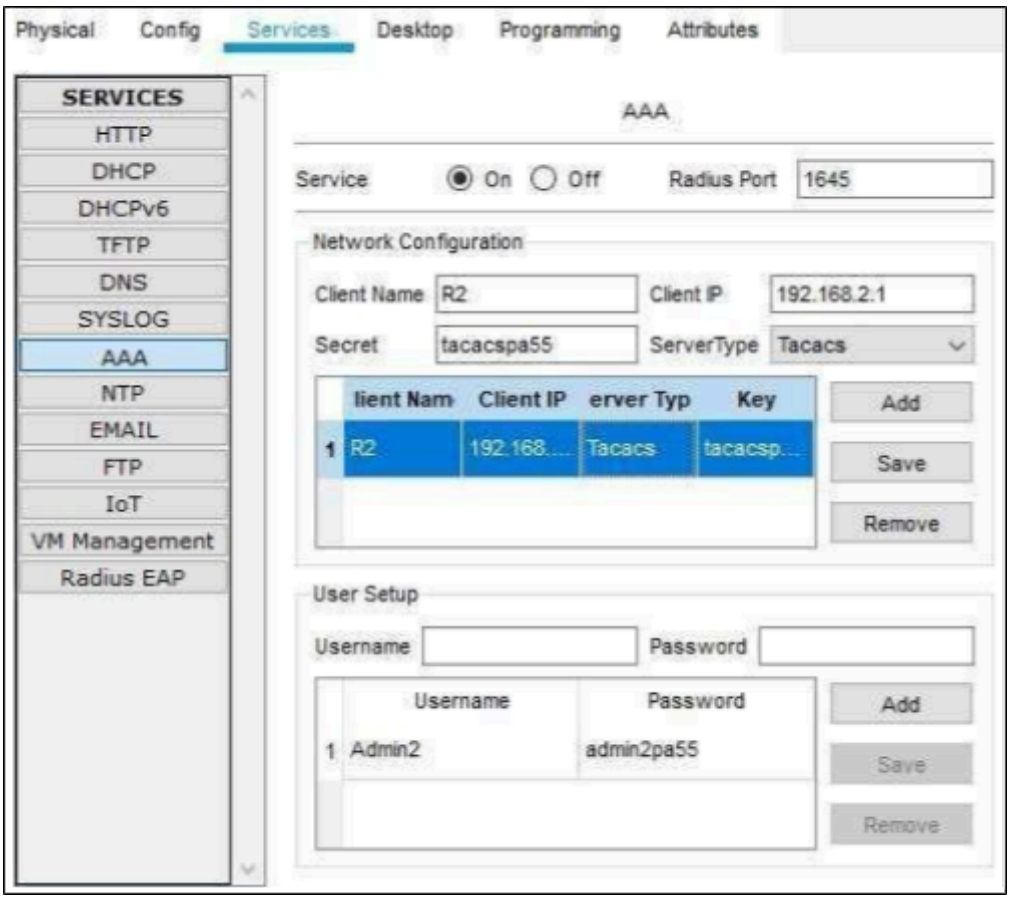
Click on Router R2 → Go to CLI tab → And the following commands :

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username Admin2 secret admin2pa55
```

Step 2 : Verify the TACACS+ Server Configuration.

Click on TACACS+ Server → Go to Services tab → From services option click on AAA → Enable the Services option → And accordingly change as per requirement:

Name :Harsh Kadu Roll No : 33



Step 3 : Configure the TACACS+ Server specifics on R2.

Click on Router R2 → Go to CLI tab → And the following commands :

```
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspa55
```

Step 4 : Configure AAA login authentication for console access on R2.

Click on Router R2 → Go to CLI tab → And the following commands :

```
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
```

Step 5 : Configure the line console to use the defined AAA authentication method.

Name :Harsh Kadu Roll No : 33

Click on Router R2 → Go to CLI tab → And the following commands :

```
R2(config)#line console 0
R2(config-line)#login authentication default
```

Step 6 : Verify the AAA authentication method.

Verify the user EXEC login using the AAA TACACS+ server.

Click on Router R2 → Go to CLI tab → And the following commands :

```
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

Authorized access are only allowed. After exiting from the privilege mode it will ask for user access verification. Give proper username and password :

```
User Access Verification

Username: Admin2
Password:
R2>
```

Part 4 : Configure Server-Based AAA Authentication Using RADIUS in R3.

Step 1 : Configure a backup local database entry called Admin.

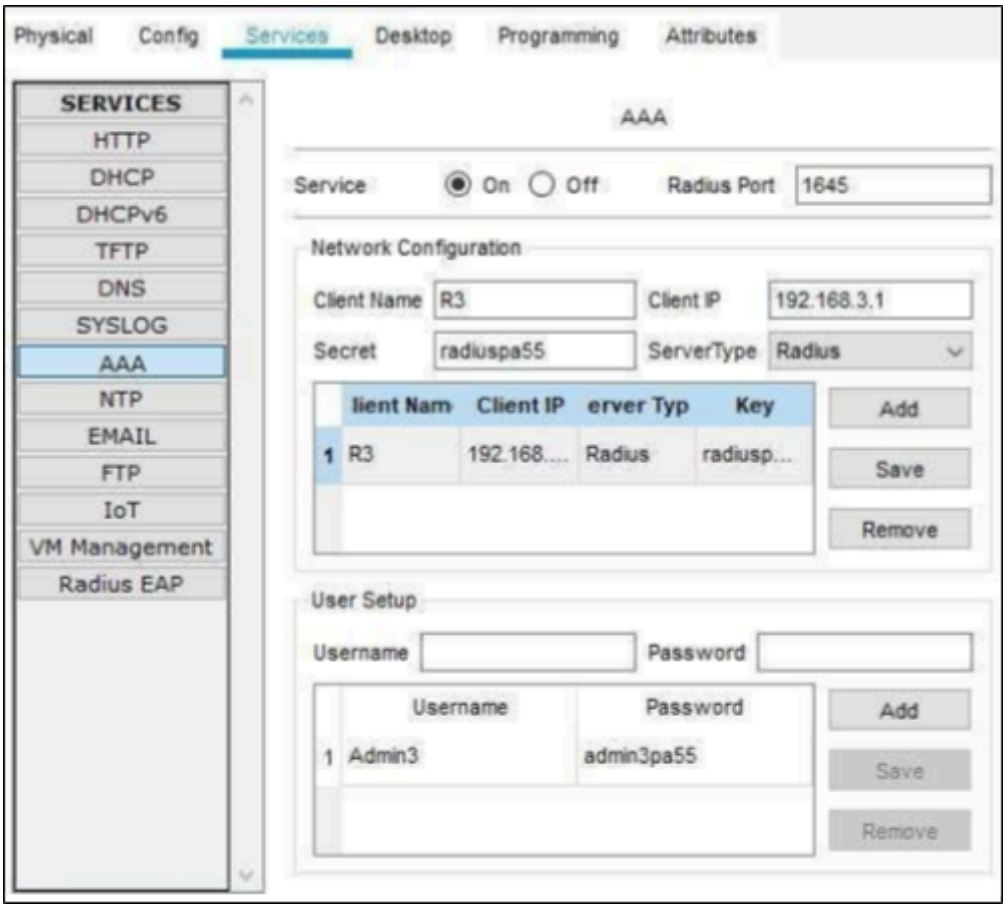
Click on Router R3 → Go to CLI tab → And the following commands :

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username Admin3 secret admin3pa55
R3(config)#
```

Step 2 : Verify the RADIUS Server configuration.

Name :Harsh Kadu Roll No : 33

Click on RADIUS+ Server → Go to Services tab → From services option click on AAA → Enable the Services option → And accordingly change as per requirement:



Step 3 : Configure the RADIUS Server specifics on R3.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspa55
```

Step 4 : Configure AAA login authentication for console access on R3.

Click on Router R3 → Go to CLI tab → And the following commands :

Name :Harsh Kadu Roll No : 33

```
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
```

Step 5 : configure the line console to use the defined AAA authentication method.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3(config)#line console 0
R3(config-line)#login authentication default
```

Step 6 : Verify the AAA authentication method.

Verify the user EXEC login using the AAA RADIUS server.

Click on Router R3 → Go to CLI tab → And the following commands :

```
R3(config-line)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Authorized access are only allowed. After exiting from the privilege mode it will ask for user access verification. Give proper username and password :

```
User Access Verification

Username: Admin3
Password:
R3>
```