#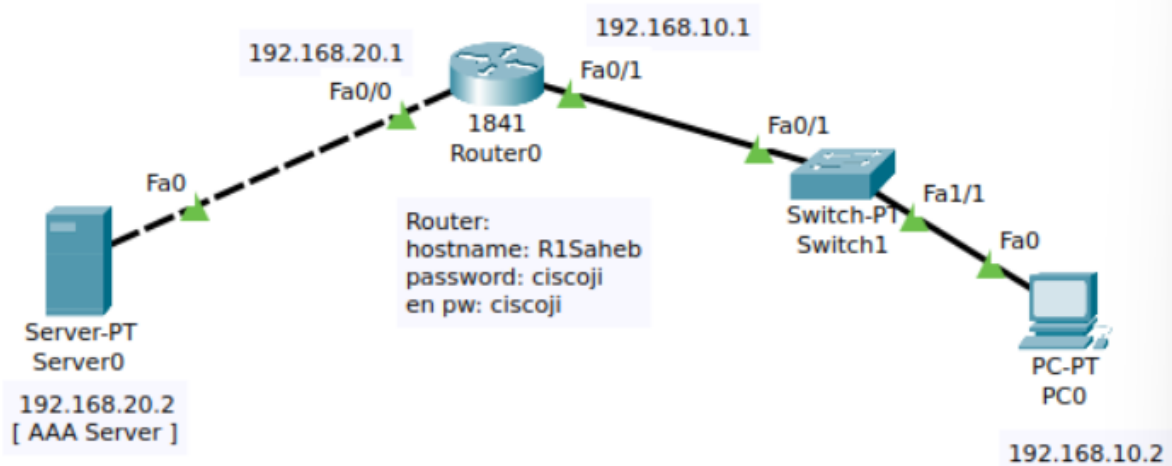 Configuration and verification of remote user authentication on a Cisco router using AAA server based username-password authentication with SSH.

Router:
hostname: R1Saheb
password: ciscoji
en pw: ciscoji

Server-PT
Server0
192.168.20.2
[AAA Server]

PC-PT
PC0
192.168.10.2


```
Router(config-if)#exit
Router(config)#hostname R1Saheb
R1Saheb(config)#enable password ciscoji
R1Saheb(config)#ip domain-name rajaji.com
R1Saheb(config)#username Admin password ciscoji
R1Saheb(config)#crypto key generate RSA
```

```
R1Saheb(config)#tacacs-server host 192.168.20.2
*Mar 1 0:12:22.996: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1Saheb(config)#tacacs-server key AliensReal
R1Saheb(config)#aaa new-model
R1Saheb(config)#aaa authentication login default group tacacs+ local
R1Saheb(config)#line vty 0 4
R1Saheb(config-line)#login authentication default
R1Saheb(config-line)#transport input ssh
R1Saheb(config-line)#line console 0
R1Saheb(config-line)#login authentication default
R1Saheb(config-line)#^Z
R1Saheb#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy   Paste

PC0   — □ ✕

Physical   Config   Desktop   Programming   Attributes

Command Prompt   X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l student 192.168.10.1

Password:
R1Saheb>en
Password:
R1Saheb#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1Saheb(config)#exit
R1Saheb#exit

[Connection to 192.168.10.1 closed by foreign host]
C:\>
```

☐ Top