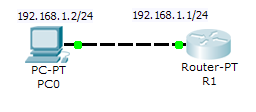
**TP:2 Réalisation de la communication ssh**

Réaliser le montage sur Packet Tracer :



**Sur le routeur faire la configuration suivante :**

Router(config)#hostname R1

R1(config)#ip domain-name cisco

R1(config)# username admin password cisco

R1(config)# enable secret cisco

R1(config)# line con 0

R1(config-line)# password cisco

R1(config-line)# login

R1(config)# line vty 0 4

R1(config-line)# password cisco

R1(config-line)# login local

R1(config-line)#no transport input all

R1(config-line)# transport input ssh

R1(config-line)# exit

R1(config)# interface FastEthernet0/0

R1(config-if)# ip address 192.168.1.1 255.255.255.0

R1(config-if)# no shut

R1(config-if)# exit

R1(config)# crypto key generate rsa

R1(config)# ip ssh time-out 15

R1(config)# ip ssh authentication-retries 2

**Tester la communication depuis le PC :**

PC>ssh -l admin 192.168.1.1

Open

Password:

**Conclusion :** l’Objectif de ce TP est de pouvoir montrer aux étudiants qu’un administrateur réseaux doit pouvoir configurer les équipements afin de communiquer en sécurité même dans un réseau local.