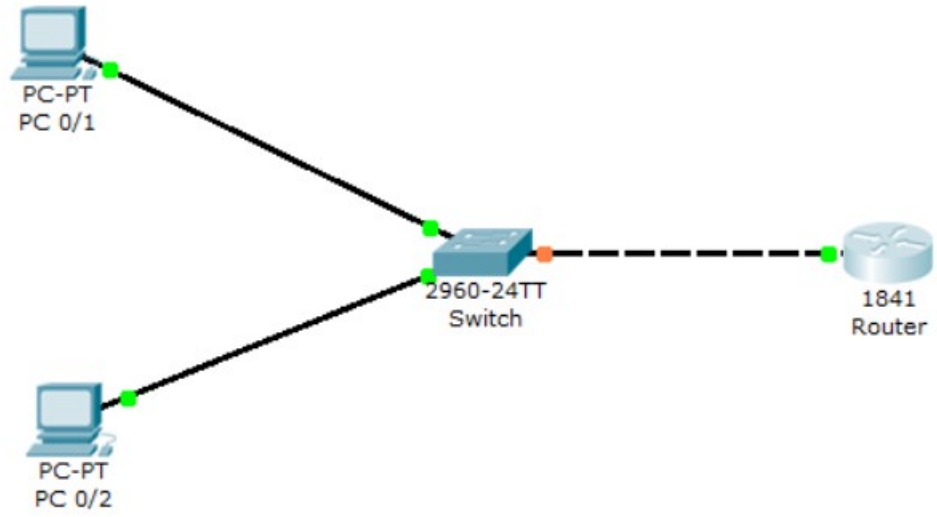
SSH CISCO

Le protocole **SSH** (**S**ecure **SH**ell) est un protocole qui permet de communiquer de manière sécurisée pour éviter que des informations sensibles (configuration, login, mot de passe, …) soient divulguées durant leur transport jusqu'à la console d'administration. Pour mettre en oeuvre ce protocole, nous allons nous appuyer sur le schéma ci-dessous :



I) Mise en place et configuration SSH

Tout d'abord, nous rendons sur le routeur et nous devons taper les commandes suivantes dans l'onglet « **CLI** » (**C**ommand **L**ine **I**nterface) :

Description des commandes pour le protocole SSH :

D'abord, nous devons définir une adresse IP sur une interface FastEthernet:
interface fasthernet 0/0.10

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0.10

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed stat
e to upRouter(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
```

Ensuite, nous devons définir un nouveau nom pour le routeur:
hostname R1

```
Router(config-subif)#exit
Router(config)#hostname R1
```

Ensuite, nous devons définir un mot de passe crypté au mode enable pour permettre la connexion au routeur (ici le mot de passe est: root) :

enable password root

```
R1(config)#enable password root
```

Ensuite, nous devons définir le nom de domaine sur lequel nous nous situons (Ici, le nom de domaine est « **thomas.local** ») :

ip domain-name thomas.local

```
R1(config)#ip domain-name thomas.local
```

Ensuite, cette commandes permet de définir un nouvel utilisateur en local (le nom d'utilisateur est « **thomas** » et son mot de passe est « **root** ») :

username thomas password 0 root

```
R1(config)#username thomas password 0 root
```

Ensuite, nous créons une clef cryptée RSA pour permettre à l'utilisateur d'accéder en Telnet ou en SSH à un matériel CISCO (switch et routeur) et nous pouvons taper directement sur « **Entrer** » pour définir le nombre de bits par défaut pour le module de la clef qui est « **512** ». Néanmoins, tel que cela est précisé, nous pouvons saisir entre **360** et 2**048** bits :

crypto key generate rsa

```
R1(config)#crypto key generate rsa
```

Ensuite, nous devons définir une fermeture de connexion au bout d'un certain temps (le temps est défini en secondes) pour des raisons de sécurité :

ip ssh time-out 120

```
R1(config)#ip ssh time-out 120
```

Ensuite, nous devons définir une certaine quantité de tentatives de connexion pour l'utilisateur :

ip ssh authentication-retries 3

```
R1(config)#ip ssh authentication-retries 3
```

Ensuite, nous devons désactiver Telnet :

line vty 0 4

```
R1(config)#line vty 0 4
```

Enfin, nous devons activer SSH :
transport input SSH

```
R1(config-line)#transport input SSH
```

II) Test et vérification du protocole SSH sur un ordinateur

Nous rendons sur un des deux **PC** pour vérifier que le ssh fonctionne en allant dans le **cmd**

Nous devons après cela taper la commande :
ssh –l nom_user @IP_routeur
Le nom d'utilisateur est « **thomas** » et l'adresse IP de l'interface du routeur est « **192.168.10.1** »).
L'utilisateur doit saisir son mot de passe (Ici, le mot de passe de l'utilisateur « **thomas** » est « **root** »).
Ensuite, nous saisissons le mot de passe secret crypté du routeur (Ici, le mot de passe du routeur est « **root** »).

Nous pouvons faire de même sur un switch : la procédure est exactement similaire mais nous devons définir une adresse IP pour le VLAN d'administration