ETTORI Bastien	BTS SIO 1ère année
08 Avril 2015	Année scolaire : 2014/2015
Option : SISR	Version 1

SSH ROUTEUR CISCO

SOMMAIRE :

ETTORI Bastien	**BTS SIO 1ère année**
08 Avril 2015	**Année scolaire : 2014/2015**
Option : SISR	**Version 1**

I) Objectif

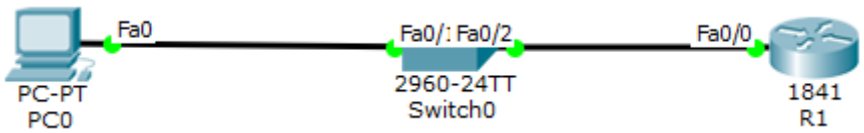
Dans cette procédure, nous allons montrer comment mettre en œuvre le protocole **SSH** en Cisco sur un routeur.

II) Prérequis

Pour mettre en place cette procédure, nous avons besoin des équipements suivants :

Nom du poste	Nombre de Switch	Nombre de routeurs
PC0	**1 Switch Cisco 2960**	**1 routeur Cisco**

Pour mettre en œuvre ce protocole, nous allons nous appuyer sur le schéma ci-dessous :



III) Définition

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.

IV) Mise en place et configuration SSH sur un routeur Cisco

- 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) :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#hostname R1
R1(config)#enable password cisco
R1(config)#ip domain-name sio.local
R1(config)#aaa new-model
R1(config)#use ettori password 0 cisco
R1(config)#

R1(config)#crypto key generate rsa
The name for the keys will be: R1.sio.local
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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

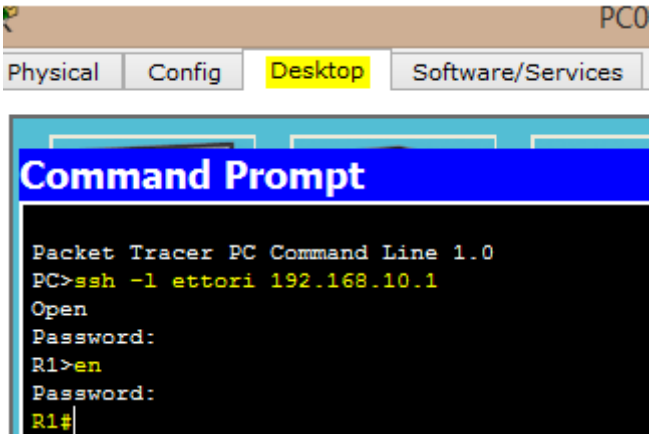
```
R1(config)#ip ssh time-out 120
R1(config)#ip ssh authentication-retries 3
R1(config)#line vty 0 4
R1(config-line)#transport input SSH
R1(config-line)#
```

V) Description des commandes saisies de manière chronologique

1) « **interface fasthernet 0/0.10** » : Attribution d'une adresse IP sur une interface FastEthernet.
2) « **hostname R1** » : Modification du nom du routeur.
3) « **enable password cisco** » : Définition et activation d'un mot de passe crypté pour permettre la connexion au routeur.
4) « **ip domain-name sio.local** » : Intégration d'un nom de domaine sur lequel nous nous situons (Ici, le nom de domaine est « **sio.local** »).
5) « **aaa new-model** » et « **username ettori password 0 cisco** » : Ces 2 commandes permettent de définir un nouvel utilisateur en local (nom d'utilisateur « **ettori** » et son mot de passe « **cisco** »).
6) « **crypto key generate rsa** » : Création d'une clé cryptée **RSA** pour permettre à l'utilisateur d'accéder en Telnet ou en SSH au routeur et définissons le nombre de bits par défaut pour le module de la clef qui est « **512** ». De plus, nous pouvons saisir entre « **360** » et « **2048** » bits.
7) « **ip ssh time-out 120** » : Définition d'une fermeture de connexion dans un temps défini (temps en secondes) pour des raisons de sécurité.
8) « **ip ssh authentication-retries 3** » : Attribution d'une quantité de tentatives de connexion pour l'utilisateur.
9) « **line vty 0 4** » : Désactivation du service **Telnet**.
10) « **transport input SSH** » : Activation du service **SSH**.

VI) Tests et vérifications du protocole SSH sur un poste client

- Maintenant, nous nous rendons sur le poste client, cliquons sur l'onglet « **Desktop** », saisissons les commandes suivantes (en jaune) et constatons que l'utilisateur peut se connecter au routeur par l'invite de commandes de sa machine :



Description des commandes saisies :

- « **ssh –l nom_user @IP_routeur** » : saisie du nom d'utilisateur qui est « **ettori** » et l'adresse IP de l'interface du routeur qui est « **192.168.10.1** ») sur le poste client.
- Premier « **Password** » : saisie du mot de passe qui est « **cisco** ».
- « **en** » : accès à la configuration et à l'administration du routeur.
- Deuxième « **Password** » : saisie du mot de passe secret crypté du routeur qui est « **cisco** ».

VII) Conclusion

En conclusion, nous pouvons constater que le protocole **SSH** fonctionne correctement et que l'utilisateur peut se connecter au routeur pour l'administrer à distance.