ETTORI Bastien	BTS SIO 1ère année
08 avril 2015	Année scolaire : 2014/2015
Option : SISR	Version 1.0

SSH ROUTEUR CISCO

SOMMAIRE :

ETTORI Bastien	**BTS SIO 1ère année**
08 avril 2015	**Année scolaire : 2014/2015**
Option : SISR	**Version 1.0**

I) Objectif

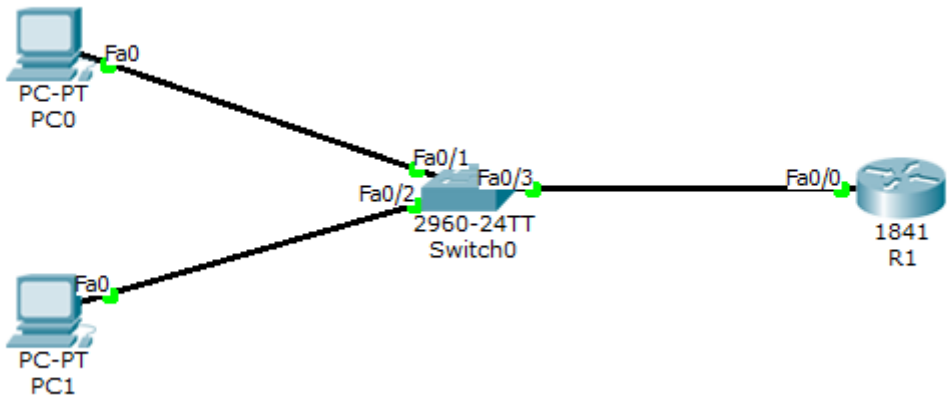
Ce tutoriel permet la mise en œuvre du protocole **SSH** en Cisco sur un routeur.

II) Prérequis

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

Nombre de postes	Nombre de Switch	Nombre de routeurs
2	**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)#in
Router(config)#interface f
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#en
Router(config-subif)#encapsulation d
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#ho
Router(config)#hostname R1
R1(config)#ena
R1(config)#enable pas
R1(config)#enable password cisco
R1(config)#ip domain-n
R1(config)#ip domain-name sio.local
R1(config)#aa
R1(config)#aaa n
R1(config)#aaa new-model
R1(config)#use
R1(config)#username ettori pas
R1(config)#username ettori password 0 cisco

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 ss
*mars 1 0:2:14.968:  RSA key size needs to be at least 768 bits for ssh version
2
*mars 1 0:2:14.968:  %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#ip ssh tim
R1(config)#ip ssh time-out 120
R1(config)#ip ss
R1(config)#ip ssh au
R1(config)#ip ssh authentication-retries 3
R1(config)#lin
R1(config)#line vt
R1(config)#line vty 0 4
R1(config-line)#tr
R1(config-line)#transport input SSH
```

V) Description des commandes saisies

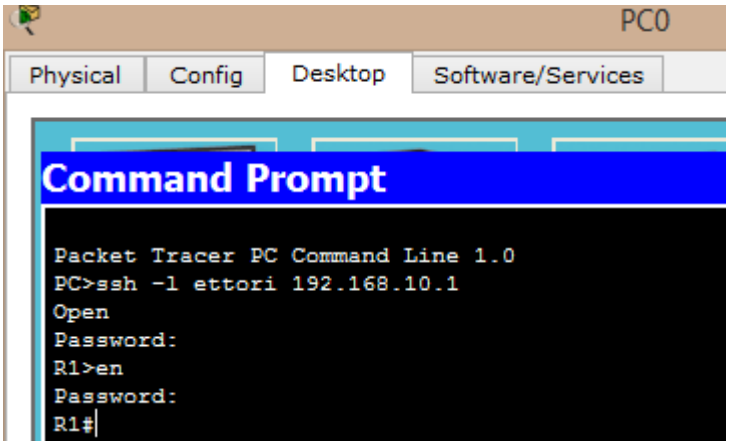
1) « **interface fasthernet 0/0.10** » : D'abord, nous devons définir une adresse IP sur une interface FastEthernet.
2) « **hostname R1** » : Ensuite, nous devons définir un nouveau nom de routeur et donc ne pas prendre le nom par défaut qui est « **Router** ».
3) « **enable password cisco** » : Ensuite, nous devons définir un mot de passe crypté au mode enable pour permettre la connexion au routeur CISCO.

4) « **ip domain-name sio.local** » : Ensuite, nous devons définir le 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** » : Ensuite, 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** » : Ensuite, nous créons une clé cryptée RSA pour permettre à l'utilisateur d'accéder en Telnet ou en SSH à un matériel CISCO (switch et routeur) et nous définissons 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.
7) « **ip ssh time-out 120** » : Ensuite, nous définissons une fermeture de connexion dans un temps défini (temps en secondes) pour des raisons de sécurité.
8) « **ip ssh authentication-retries 3** » : Ensuite, nous définissons une quantité de tentatives de connexion pour l'utilisateur.
9) « **line vty 0 4** » : Ensuite, nous désactivons Telnet.
10) « **transport input SSH** » : Enfin, nous activons SSH.

VI) Test et vérification du protocole SSH sur un poste

- Ensuite, nous devons taper la commande « **ssh –l nom_user @IP_routeur** » sur un poste (Ici, le nom d'utilisateur est « **ettori** » et l'adresse IP de l'interface du routeur est « **192.168.10.1** »).
- Ensuite, l'utilisateur doit saisir son mot de passe (Ici, le mot de passe de l'utilisateur « **ettori** » est « **cisco** »).
- Ensuite, nous saisissons le mot de passe secret crypté du routeur (Ici, le mot de passe du routeur est « **cisco** »).

Après avoir saisi toutes ces informations, voici ce que nous constatons :



Donc, nous voyons que l'utilisateur peut se connecter au routeur par l'invite de commandes de sa machine.

VII) Conclusion

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