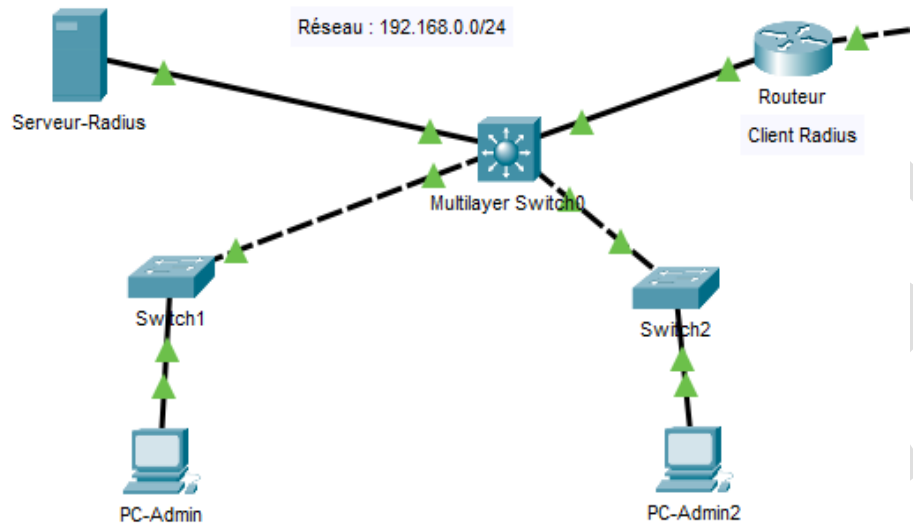
CONFIGURATION D'UN ACCES SSH SECURISE PAR UN SERVEUR RADIUS SUR CISCO

ES-SAIDI Naoufal

Sommaire

CONFIGURATION D'UN ACCES SSH SECURISE PAR UN SERVEUR RADIUS

MAQUETTE DE L'EXERCICE



PLAN D'ADRESSAGE

Compléter le tableau suivant :

Equipement	**Adresse IP/masque**
Interface routeur	192.168.0.254
Serveur Radius	192.168.0.10
Switch L3	192.168.0.1

OBJECTIFS

- Le but est de permettre aux administrateurs du réseau, depuis un PC, d'administrer à distance par SSH le routeur Cisco ;
- L'authentification ne sera pas réalisée par le routeur Cisco, mais par le serveur Radius ;
- Le routeur Cisco devra être configuré comme "**client Radius**".
- Le client Radius (routeur Cisco) et le serveur Radius doivent partager un secret pour qu'ils puissent mutuellement s'authentifier.

La base des comptes utilisateurs autorisés à administrer le routeur Cisco sera enregistrée sur le **serveur Radius**.

CONFIGURATION DU ROUTEUR CISCO (CLIENT RADIUS)

a. Configuration de l'accès SSH sur le routeur

```
Router(config)#hostname R1
R1(config)#ip domain-name sio.fr
R1(config)#crypto key generate rsa
R1(config)#ip ssh version 2
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
```

b. Configuration de l'authentification Radius sur le routeur

```
R1(config)#aaa new-model
R1(config)#radius-server host IP_seveur_Radius key 123456789
R1(config)#aaa authentication login SSH_LOGIN group radius local
```

123456789 est une chaîne de caractères correspondant à la clé secrète commune au client radius (Routeur R1) et au serveur Radius.

Remarque : une authentification locale est ajoutée dans le cas où le serveur Radius n'est pas accessible.

c. Application de l'authentification AAA sur les terminaux virtuels 0 à 15

```
R1(config)#line vty 0 15
R1(config-line)#login authentication SSH_LOGIN
```

Vous pouvez même configurer une authentification radius sur le compte privilégié lorsque vous tapez enable :

```
Router(config)# aaa authentication enable default group radius local
```

CONFIGURATION DU SERVEUR RADIUS

La configuration se fait en 2 étapes :

- Enregistrer le client Radius ainsi que la clé secrète partagée (ici 123456789).
- Enregistrer les utilisateurs autorisés à administrer le routeur Cisco.

Attention : Packet Tracer ne permet pas que le mot de passe d'un utilisateur de la base de comptes Radius soit identique à son nom.

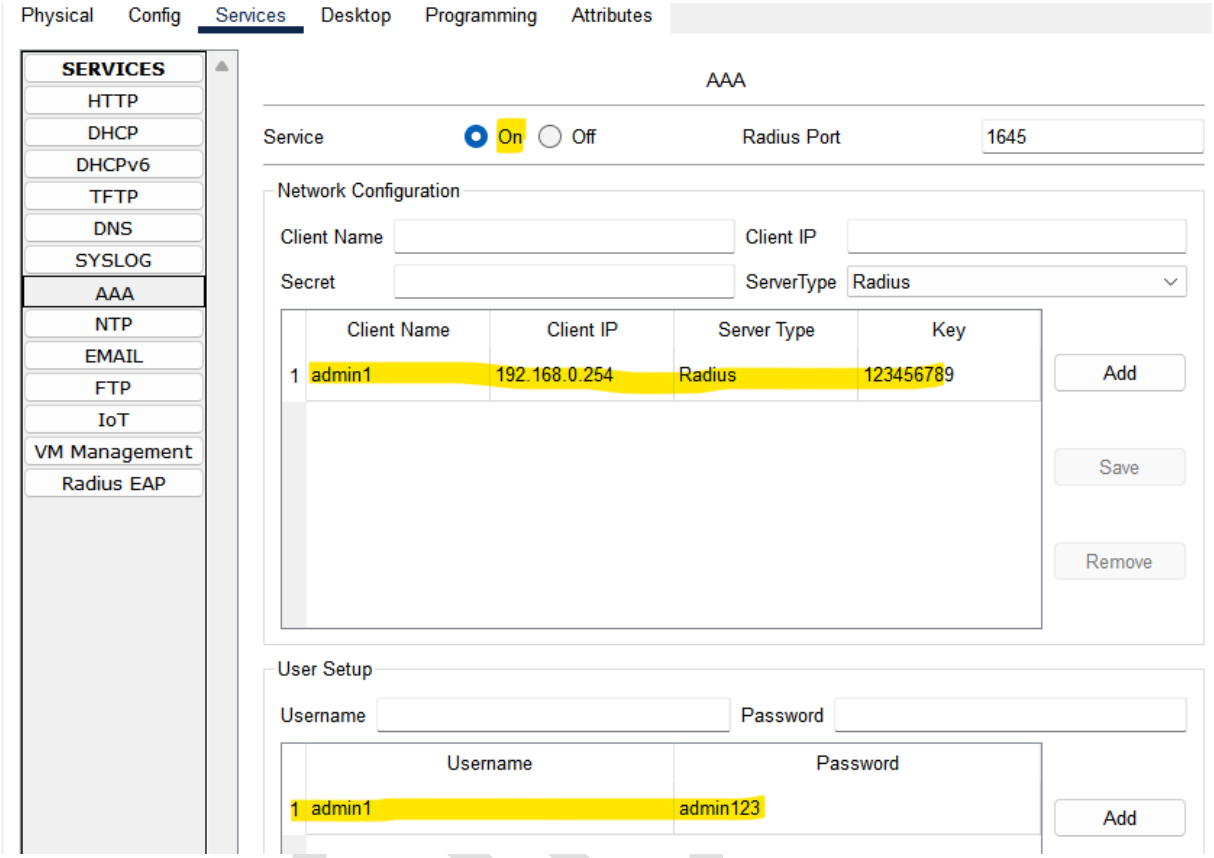
Copie d'écran de la configuration du service Radius :

TESTS

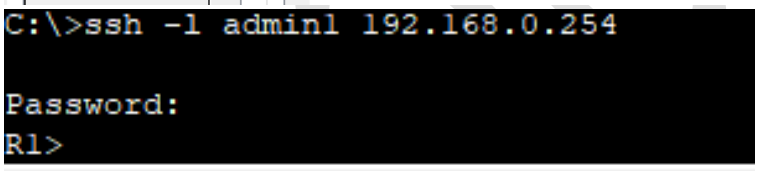
- Vérifier que l'accès SSH au routeur se fait avec l'utilisateur et le mot de passe associé déclarés sur le serveur RADIUS.
  A partir d'un PC tapez la commande suivante :

ssh –l **nom-utilisateur** ***IP-routeur***

- Ajouter un autre utilisateur sur le serveur Radius et tester son accès au routeur en ssh.



-



-
- Visualiser et analyser les trames échangées entre le routeur et le serveur d'authentification RADIUS.
- Utiliser le mode « debug » sur le routeur :

debug aaa authentication

- Connectez-vous en ssh à partir d'un client.
- Observer le résultat sur le routeur.
- Quitter le mode « debug » :

no debug aaa authentication

FONCTIONNEMENT DE L'AUTHENTIFICATION RADIUS :

a. **Demande d'accès** : L'utilisateur tente de se connecter à un service ou réseau protégé par RADIUS (par exemple, un VPN, Wi-Fi, serveur, routeur, …).

b. **Echange du secret partagée** entre le client RADIUS (ex : point d'accès, routeur, serveur, …) et le serveur RADIUS.

c. **Demande d'authentification** : Le client RADIUS envoie les informations d'identification (nom d'utilisateur, mot de passe) de l'utilisateur vers le serveur RADIUS.

d. **Vérification et réponse** : Le serveur RADIUS valide les informations d'identification, vérifie les droits d'accès et envoie une réponse :
    - **Accès accordé** : L'utilisateur peut accéder aux ressources réseau.
    - **Accès refusé** : L'utilisateur est bloqué.

e. **Comptabilisation** : Le serveur peut également enregistrer l'activité de l'utilisateur pendant la session (durée, quantité de données, etc.).

f. **Fin de session** : Lorsque l'utilisateur se déconnecte, une notification de fin de session est envoyée pour la comptabilisation.

AVANTAGES DU SERVEUR RADIUS :

- **Centralisation de la gestion des accès** : Les informations d'identification et les politiques d'accès sont gérées de manière centralisée.
- **Sécurité** : RADIUS utilise des méthodes de chiffrement et de hachage pour protéger les informations d'identification pendant le processus d'authentification.
- **Extensibilité** : RADIUS peut s'intégrer à d'autres systèmes comme LDAP, Active Directory et des bases de données externes pour l'authentification et l'autorisation.