Contrôle d'accès centralisé avec un serveur RADIUS (AAA)

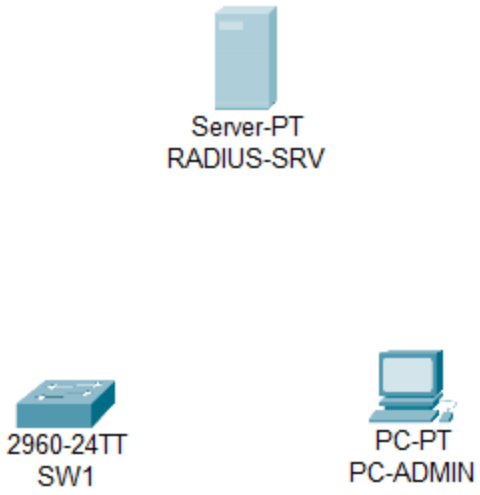
Dans une entreprise il faut centraliser les comptes et les badge afin de réduire le temps pour accorder des droits, supprimer des droits aux employés. Le protocole RADIUS est un des standards les plus fréquemment utilisé pour permettre cela
Le modéle AAA pour:

- Authentification (Authentication): Qui êtes-vous? avec la combinaison de connexion
- Autorisation (Authorization): Qu'avez-vous le droit de faire? (Administrateur ou simple utilisateur)
- Comptatibilité (Accounting): Qu'avez vous fait? (Journalisation des commandes et des connexions)

Préparation du Laboratoire

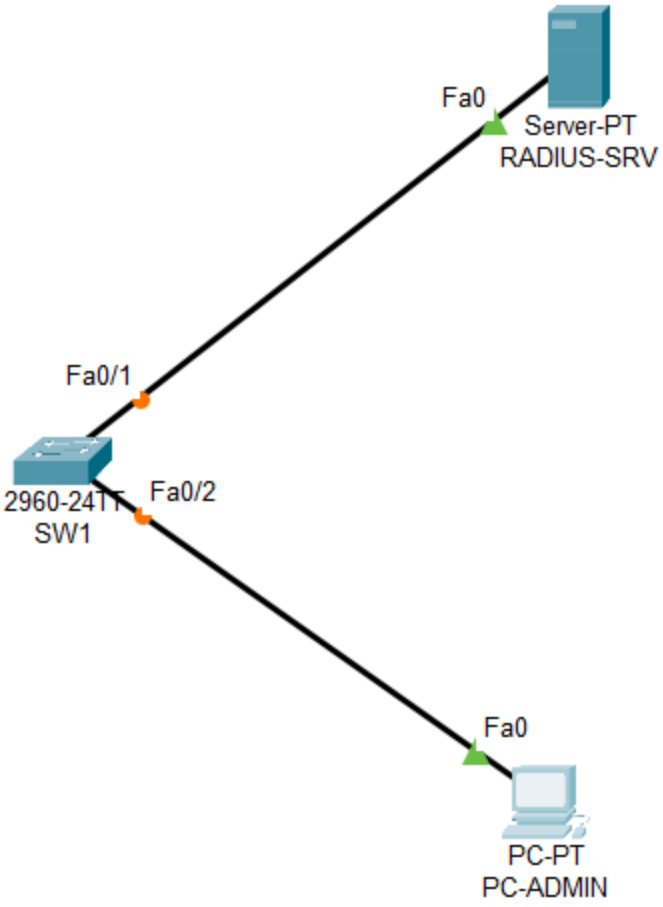
Liste d'équipement

1 commutateur nommé SW1 modèle 2960
1 server RADIUS-SRV
1 PC PC-ADMIN



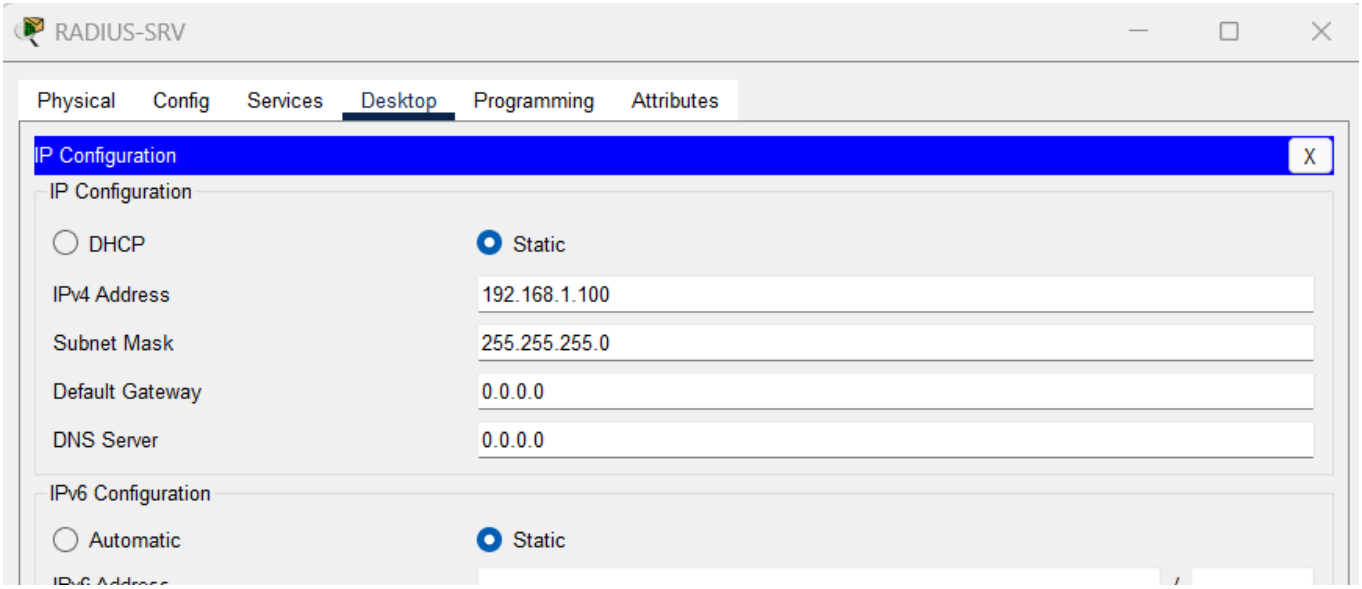
Topologie

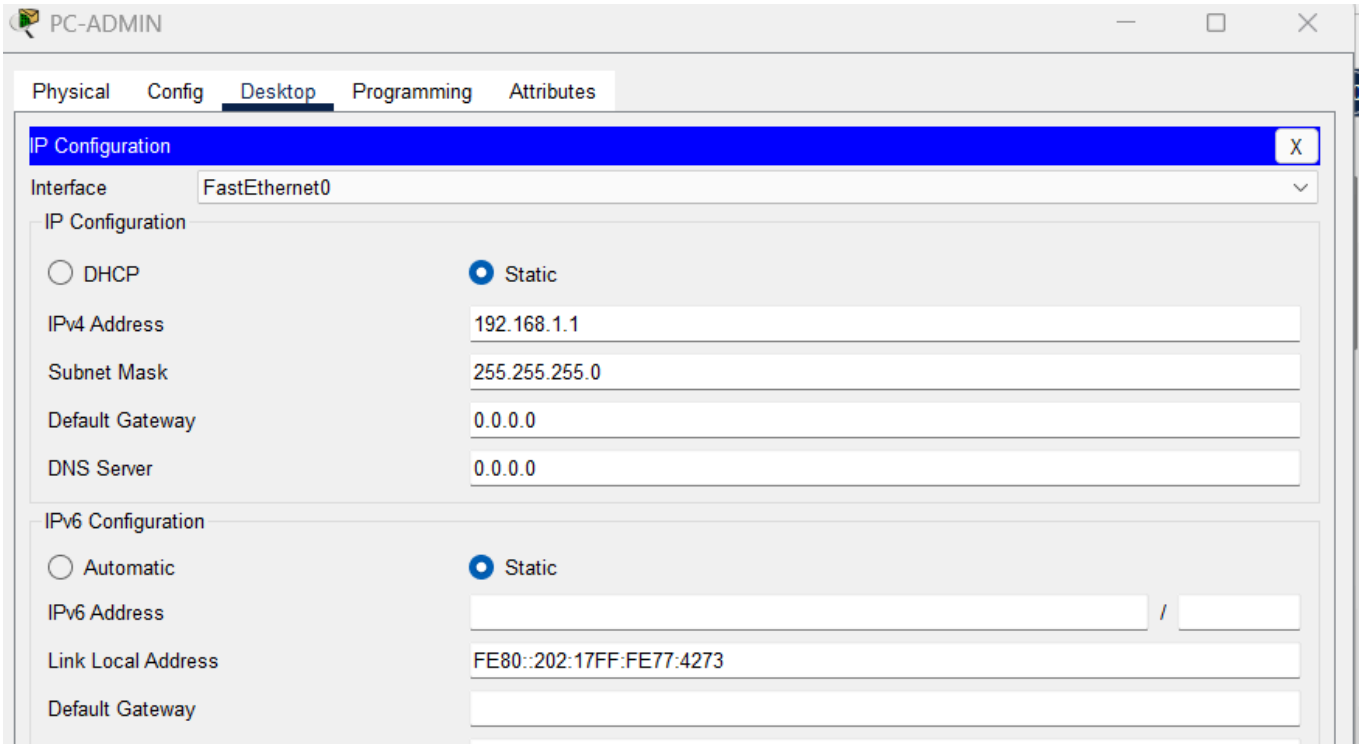
Relié SW1 (Fa0/1) à RADIUS-SRV
SW1(Fa0/2) à PC-ADMIN



Adrressage IP

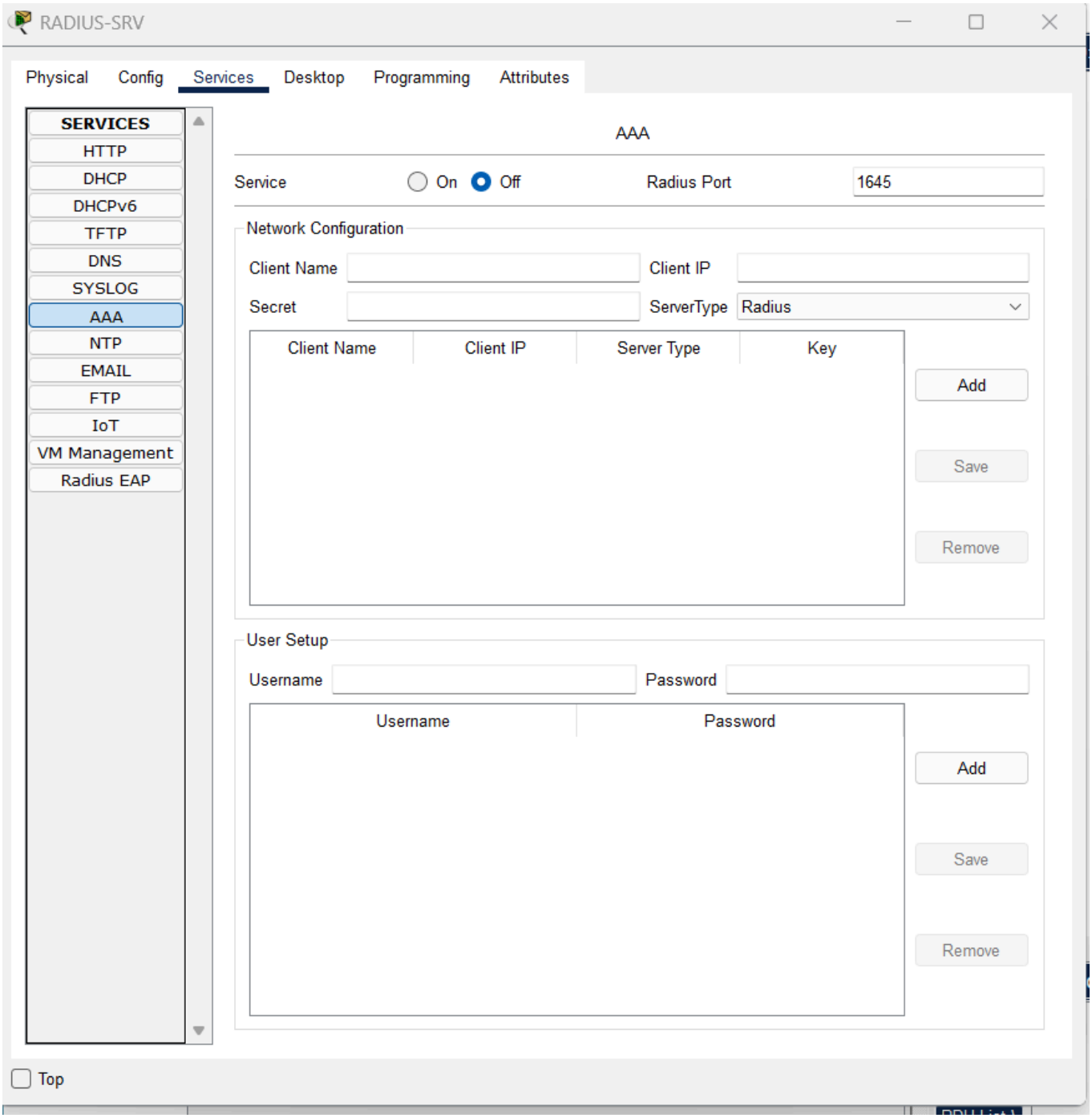
équipement	IP	masque de sous-réseaux
RADIUS-SRV	192.168.1.100	255.255.255.0
PC-ADMIN	192.168.1.10	255.255.255.0
SW1	192.168.1.1	255.255.255.0

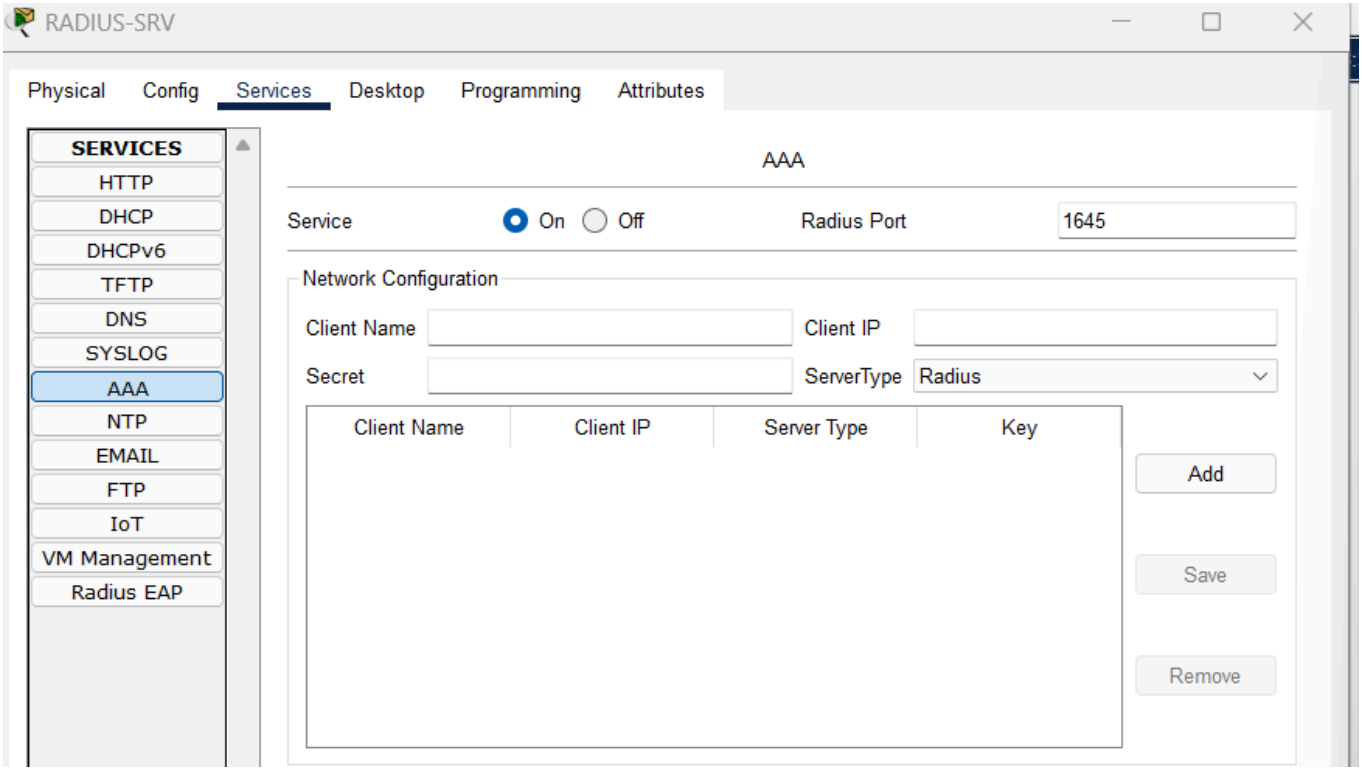


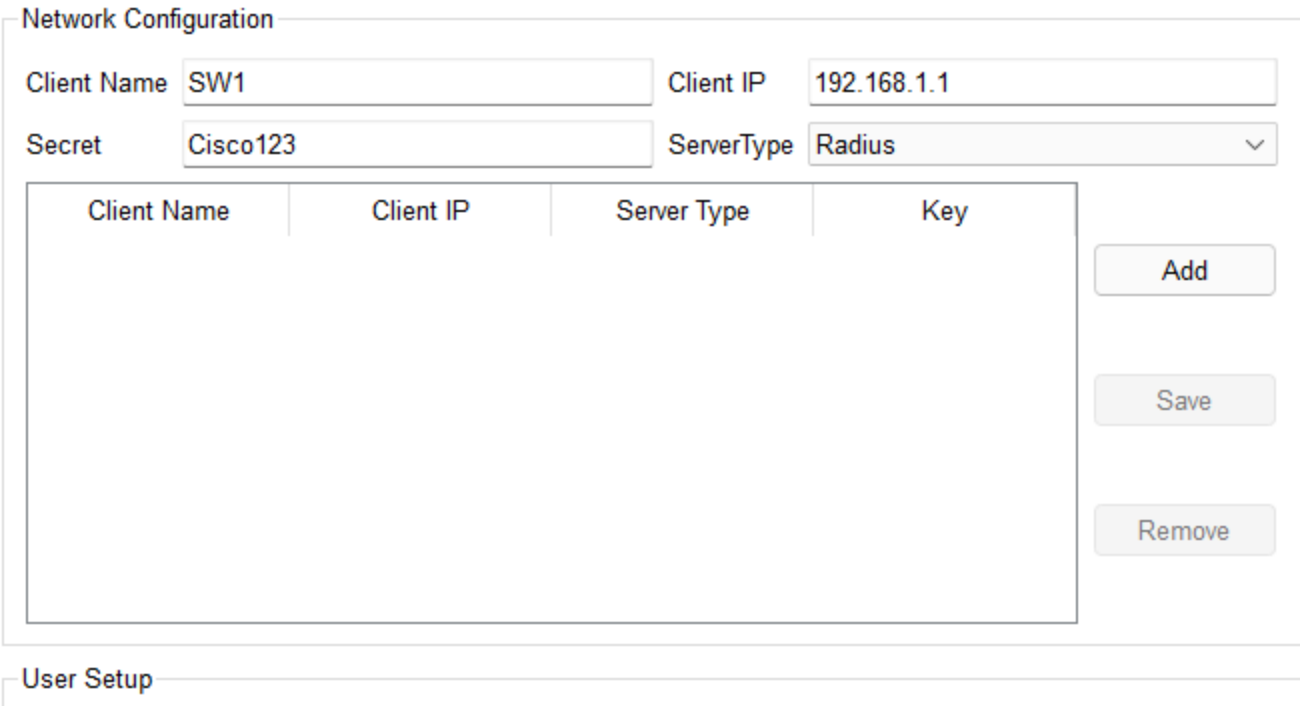


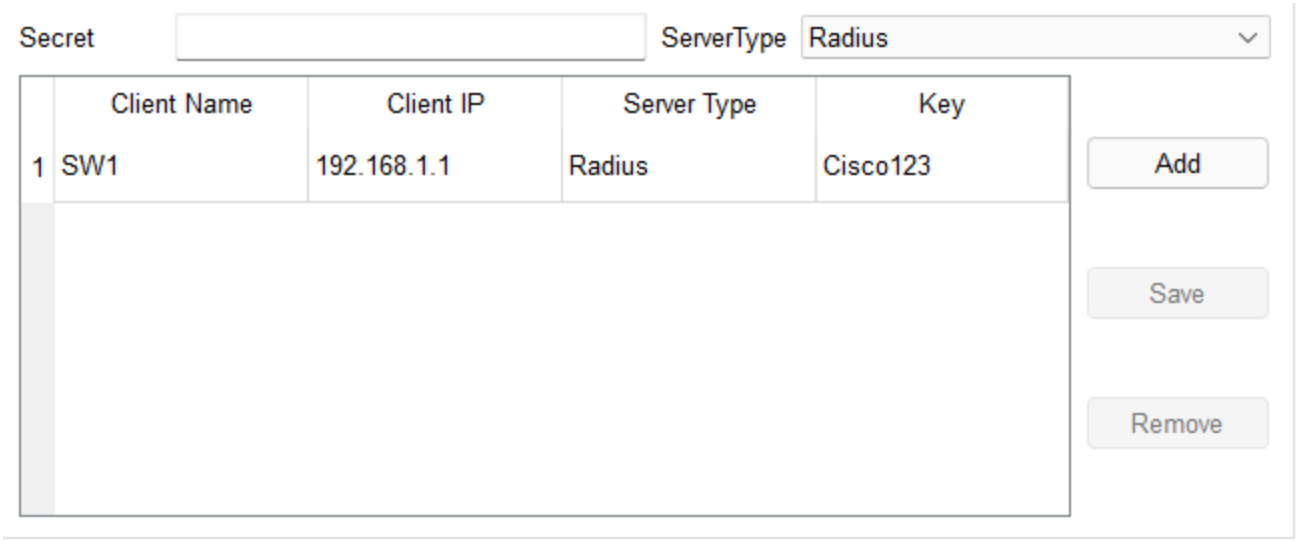

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
```

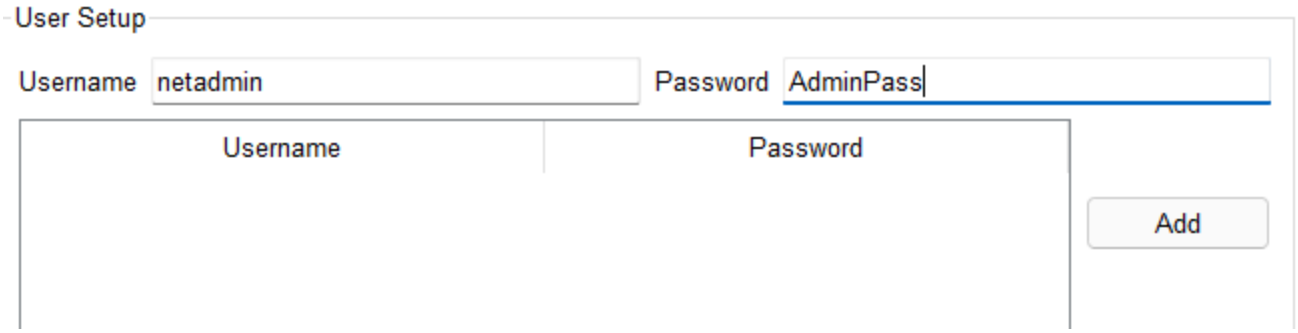
Configuration du serveur RADIUS

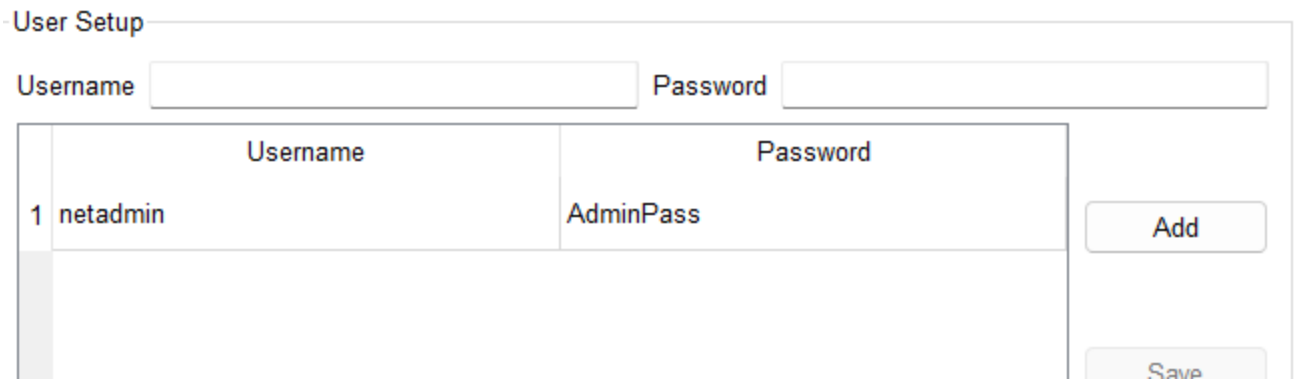

RADIUS-SRV
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius
Client Name
Client IP
Server Type
Key
Add
Save
Remove
User Setup
Username
Password
Username
Password
Add
Save
Remove
Top


RADIUS-SRV
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius
Client Name
Client IP
Server Type
Key
Add
Save
Remove


Network Configuration
Client Name
SW1
Client IP
192.168.1.1
Secret
Cisco123
ServerType
Radius
Client Name
Client IP
Server Type
Key
Add
Save
Remove
User Setup







Configuration du SW1

Configuration de l'accès à distance SSH

```
ip domain-name noob2pro.lab
crypto key generate rsa
1024
ip ssh version 2
```

Configuration du modèle AAA

```
#Activer le modèle AAA
aaa new-model
#Déclaré le serveur Radius
```

```
radius server RADIUS-SRV
address ipv4 192.168.1.100
key Cisco123
#Configuration d'une liste de méthode d'authentification
aaa authentication login default group radius local
#Création d'un utilisateur local de secours
username backupadmin secret BackupPass
#Applicquer la liste de méthode aux ligne d'accès à distance
line vty 0 15
transport input ssh
login authentication VTY-LOGIN #lie la liste de méthode au connexion telnet et SSH
```

```
SW1(config)#aaa new-model
SW1(config)#radius server RADIUS-SRV
SW1(config-radius-server)#address ipv4 192.168.1.100
SW1(config-radius-server)#key Cisco123
 WARNING: Command has been added to the configuration using a type 0 password. However, type 0 passwords will soon be deprecated. Migrate to a supported password type
*Nov 02 21:37:37.024: %AAAA-4-CLI_DEPRECATED: WARNING: Command has been added to the configuration using a type 0 password. However, type 0 passwords will soon be deprecated. Migrate to a supported password type
SW1(config-radius-server)#exit
SW1(config)#aaa authentication login default group radius local
SW1(config)#username backupadmin secret BackupPass
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login authentication VTY-LOGIN
 AAA: Warning authentication list VTY-LOGIN is not defined for LOGIN
SW1(config-line)#exit
SW1(config)#
```

vérification

ssh -l netadmin 192.168.1.1 avec le Password AdminPass

ssh -l backupadmin 192.168.1.1 avec le Password BackupPass