2022-2023

MISSION 6 : SOLUTION D'ACCES WIFI SANS FIL

Sofiane AININE, Daniel GOLGI, , Yvan-loic SOH , Alexandre AUBERMAS, Lina HAOUAS

2022-2023

Sommaire

Introduction

1. Contexte :

1.1 Présentation de l'entreprise :

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme. Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe.

StadiumCompany fournit l'infrastructure réseau et les installations sur le stade.

StadiumCompany emploie 170 personnes à temps plein :

- 35 dirigeants et responsables
- 135 employés

Environ 80 intérimaires sont embauchés en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.

À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide de faire appel à des consultants réseau pour prendre en charge la conception, la gestion du projet et sa mise en œuvre.

Ce projet sera mis en œuvre suivant trois phases. La première phase consiste à planifier le projet et préparer la conception réseau de haut niveau. La deuxième phase consiste à développer la conception réseau détaillée. La troisième phase consiste à mettre en œuvre la conception.

1.2 Présentation du prestataire informatique :

Après quelques réunions, StadiumCompany charge NetworkingCompany, une société locale spécialisée dans la conception de réseaux et le conseil, de la phase 1, la conception de haut niveau.

Créée en 1989, NetworkingCompany est une société spécialiste en infrastructures systèmes et vente de matériel informatique pour professionnels de la vidéo. Employant aujourd'hui 20 ingénieurs réseau, l'activité de NetworkingCompany s'établit à 1,8 millions d'euros de chiffre d'affaires. Son cœur de métier se situe au niveau de l'infrastructure informatique afin de garantir les besoins des activités « métiers ». NetworkingCompany est l'une des seules sociétés de services informatique qui accompagne réellement et jusqu'au bout ses clients dans le choix et la mise en œuvre de solutions.

NetworkingCompany intervient en mode Projet (Engagement de résultats), Régie (Engagement de moyens) et Infogérance des environnements Windows. Son outil de compétitivité et de productivité réside dans la capitalisation de son savoir-faire, le haut niveau de certification de ses partenariats ainsi qu'une veille technologique active.

NetworkingCompany a développé une expertise forte dans les domaines de la virtualisation, les infrastructures d'accès (Application delivery), l'industrialisation du poste de travail (Itil, Supervision, Télédistribution), les annuaires et la gestion de l'identité.

Reconnu depuis 25 ans comme une entreprise innovante, et avec aujourd'hui plus de 300 collaborateurs, cette société répond avec flexibilité et efficacité à tous les besoins, qu'ils émanent de PME ou de grands comptes. Enfin, NetworkingCompany est en partenariat avec de nombreux gros groupes du monde de l'informatique, tout comme Microsoft, CISCO, HP, Huawei ou encore DELL, pour ne citer que les plus importants.

1.4 Contexte du projet WiFi

Actuellement, le stade possède un accès aux différentes ressources de StadiumCompagny (fichiers, impression, internet, bases de données,). Mais cet accès n'est possible qu'à travers une liaison filaire. La direction du stade souhaite étendre aux services équipés d'un terminal Wifi.

StadimCompagny a fait l'acquisition de plusieurs Switchs compatibles PoE et des AP Cisco. Vous êtes chargé d'implémenter une solution d'accès sans fil pour les salariés du stade ainsi qu'aux visiteurs. Ces derniers n'auront accès qu'à la ressource internet mais d'une façon sécurisée (obligation légale).

1.5 Cahier des charges :

Chaque service dispose d'un point d'accès 802.11 b/g/n PoE. Il y a un SSID non diffusé par VLAN sauf le Vlan visiteur.

La confidentialité est assurée par la norme WPA2 Enterprise sauf pour le dernier dans première temps, puis un renforcement de l'authentification dans un deuxième temps.

La confidentialité est assurée par la norme WPA2 Enterprise sauf pour le dernier dans un premier temps, puis un renforcement de l'authentification dans un deuxième temps.

Modification à opérer :

- Proposer une solution d'accès Wifi pour le Vlan Wifi (stade-wifi)
- Intégrer et configurer le ou les switchs PoE
- Intégrer et configurer les AP Wifi

1.6 Solutions & Choix

Test et comparaison des solutions :

Pour assurer la securité du réseau nous allons utiliser le Wi-Fi Protected Access 2 (WPA2 – IEEE 802.11i), en implémentant différents protocoles qui permettront de répondre aux exigences de sécurité et de transparence auprès des utilisateurs.

Authentification des utilisateurs :

Pour gérer l'authentification des utilisateurs, nous allons utiliser un serveur Radius. Radius (Remote Authentifiacation Dial-in User Service) est un protocole client-serveur permettant de centraliser les données d'authentification.

Pour s'authentifier, le poste utilisateur transmet une requête d'accès à un client RADIUS pour entrer sur le réseau, ce dernier se charge de demander les identifiants de l'utilisateur (utilisateur & mot de passe).

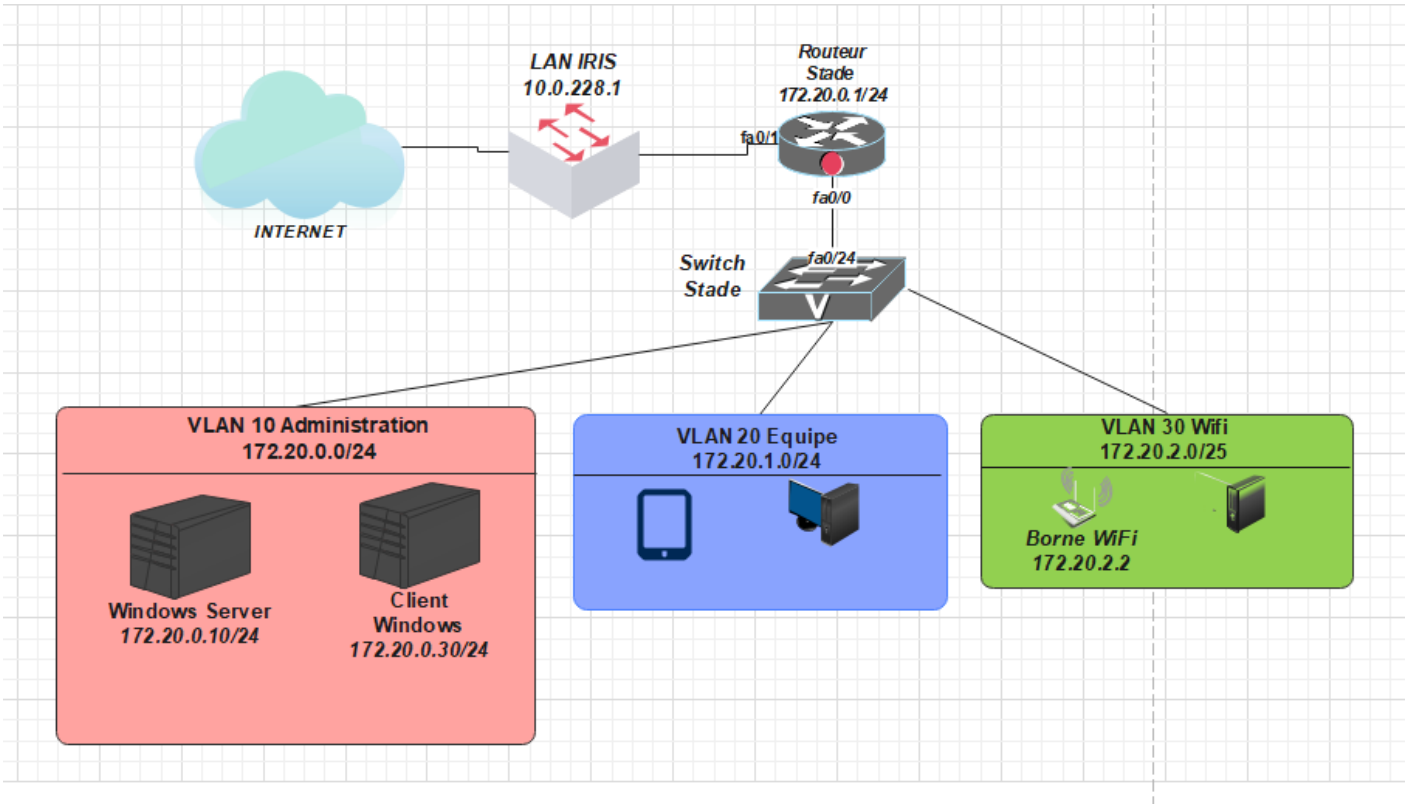
Le client RADIUS génère une requête d'accès qu'il transmet au serveur RADIUS, ce dernier, préalablement couplé avec le service d'annuaire (serveur Active Directory) va pouvoir aller vérifier les informations envoyées par le client et ainsi valider ou bien refusé l'accès.

Sécurité des communications :

Pour sécuriser les communications sur le réseau WPA2 offre deux types de chiffrements :

- Temporal Key Integrity Protocol (TKIP) : il permet l'authentification et la protection des données transitant sur le réseau. C'est une méthode de cryptage. Qui génère une clé de paquets, mélange les paquets du message, puis remet les paquets dans l'ordre pour retrouver l'intégrité du message grâce à un mécanisme de triage.
- Advanced Encryption Standard (AES) : c'est une méthode de chiffrement symétrique (chiffrement avec une clé secrète). TKIP est donc initialement mis en place pour pallier aux différents problèmes du chiffrage WEP, il repose sur la même base de chiffrement qui a révélé ses limites. AES quant à lui est une méthode de chiffrement complètement à part qui n'a pour l'instant pas été cassé. De plus TKIP générant dynamiquement (quelques minutes d'intervalle entre chaque génération de clés) des clés de chiffrement peuvent diminuer les performances alors que l'AES n'a besoin que de très peu de ressources.

1.7 Schéma réseau



2. Configuration des équipements

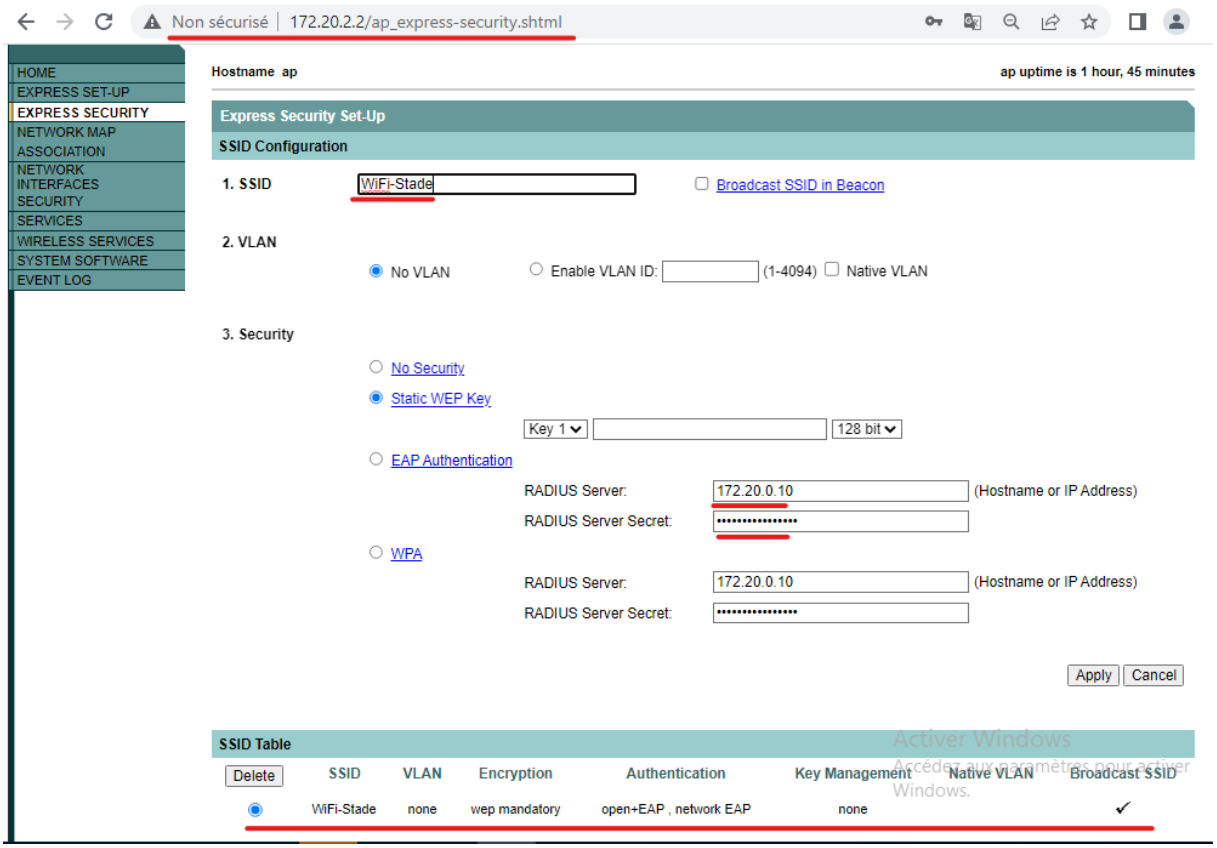
2.1 Configuration de la borne WiFi

On commence par configurer la borne wifi en lui attribuant une adresse IP :

```
!
interface BVI1
 ip address 172.20.2.2 255.255.255.0
 no ip route-cache
!
```

Après avoir configuré l'adresse IP de la borne, on va pouvoir la configurer depuis l'interface web en la renseignant dans la barre de recherche d'un moteur de recherche. On renseigne ainsi le SSID (Service Set IDentifier), qui est tout simplement le nom d'un réseau WiFi, composé au maximum de 32 caractères alphanumériques. Il permet donc d'identifier le réseau sur lequel on veut se connecter. On y renseigne aussi l'adresse IP du serveur Active Directory qui héberge le serveur Radius, via le protocole EAP (Extensible Authentication Protocol), qui est une infrastructure architecturale qui fournit une extensibilité pour les méthodes d'authentification pour les technologies d'accès réseau protégées couramment utilisées, telles que l'accès sans fil basé sur IEEE 802.1 X ou l'accès câblé IEEE 802.1 X.

On coche également la case « Broadcast SSID » (en bas à droite) afin que le réseau soit visible de tous.



2.2 Configuration du routeur

On configure le port fa0/0 qu'on relie au switch 1, avec le système d'encapsulation Dot1Q, au nombre de trois, dont les adresses IP sont :

- 172.20.0.1
- 172.20.1.1
- 172.20.2.1

Configuration du NAT

```
Rl-stade#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rl-stade(config)#int fa0/0
Rl-stade(config-if)#int fa0/0.20
Rl-stade(config-subif)#ip address 172.20.1.1 255.255.255.0
Rl-stade(config-subif)#no shutdown
Rl-stade(config-subif)#exit
Rl-stade(config)#int fa0/0.30
Rl-stade(config-subif)#encapsul
Rl-stade(config-subif)#encapsulation dot1Q 30
Rl-stade(config-subif)#ip address 172.20.2.1 255.255.255.0
Rl-stade(config-subif)#no shut
Rl-stade(config-subif)#no shutdown
```

Le NAT pour **N**etwork **A**ddress **T**ranslation est unmécanisme mis en place sur les routeurs afin de remplacer l'adresse IP privée source d'une machine par l'adresse IP publique du routeur dans un paquet réseau lorsqu'une machine tente de communiquer avec un serveur situé sur Internet.

Il existe deux types de NAT, le NAT statique, qui traduit une adresse IP privée en une adresse IP publique et le NAT dynamique, qui lui peut associer plusieurs adresses privées à une adresse IP publique.

Dans notre cas, on définit les différentes interfaces où l'interface va rendre disponible (public) le réseau que l'on souhaite apparaître.

On souhaite que le réseau public passe par notre routeur, donc c'est tout naturellement que l'on va configurer ses interfaces.

On configure notre port fa0/1 de sorte à ce qu'il soit en DHCP afin de récupérer une adresse IP de manière automatique avec ces commandes :

interface FastEthernet0/1

no shut

ip address dhcp

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

```
Rl-stade(config)#int fa 0/0.10
Rl-stade(config-subif)#ip nat inside

*Jan 20 15:46:30.511: %LINEPROTO-5-UPDOWN: Line protocol o
Rl-stade(config-subif)#
Rl-stade(config-subif)#
Rl-stade(config-subif)#
Rl-stade(config-subif)#exit
Rl-stade(config)#int fa/0.20
                   ^
% Invalid input detected at '^' marker.

Rl-stade(config)#int fa0/0.20
Rl-stade(config-subif)#ip nat inside
Rl-stade(config-subif)#exit
Rl-stade(config)#int fa0/0.30
Rl-stade(config-subif)#ip nat inside
Rl-stade(config-subif)#exit
```

La commande {**ip nat inside**} permet d'avoir accès au réseau, en configurant l'interface réseau sur un routeur comme une interface d'intérieur pour la traduction d'adresse de réseau.

Après que l'on a fait cela on va spécifier les interfaces qui vont vers la source et qui seront soumis à la traduction d'adresse IP (le fait de changer une adresse privée en adresse IP publique, ici celles qui correspondent aux VLANS avec les list), pour cela on va mettre les commandes suivantes :

ip nat inside source list 10 interface FastEthernet0/1 overload

ip nat inside source list 20 interface FastEthernet0/1 overload

ip nat inside source list 30 interface FastEthernet0/1 overload

ip route 0.0.0.0 0.0.0.0 10.0.228.1

!

access-list 10 permit 172.20.0.0 0.0.0.255

access-list 20 permit 172.20.1.0 0.0.0.255

access-list 30 permit 172.20.2.0 0.0.0.127

2.3 Switch

Dans un premier temps, on y configure les VLANS où les ordinateurs des différents services seront présents.

```
swl-srv(config)#VLAN 10
swl-srv(config-vlan)#name administration
swl-srv(config-vlan)#exit
swl-srv(config)#VLAN 20
swl-srv(config-vlan)#name equipe
swl-srv(config-vlan)#exit
swl-srv(config)#VLAN 30
swl-srv(config-vlan)#name WIFI
swl-srv(config-vlan)#exit
swl-srv(config)#
swl-srv(config)#
swl-srv(config)#int range gi0/1-6
swl-srv(config-if-range)#switchport acces vlan 10
swl-srv(config-if-range)#switchport mode access
swl-srv(config-if-range)#no shut
swl-srv(config-if-range)#exit
swl-srv(config)#int range gi0/7-14
swl-srv(config-if-range)#switchport acces vlan 20
swl-srv(config-if-range)#switchport mode access
swl-srv(config-if-range)#no shut
swl-srv(config-if-range)#exit
swl-srv(config)#int range gi0/15-21
swl-srv(config-if-range)#switchport acces vlan 30
swl-srv(config-if-range)#switchport mode acces
swl-srv(config-if-range)#no shut
swl-srv(config-if-range)#exit
```

On y constate que les VLAN sont bien créer :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/22, Gi0/23, Gi0/24
10   administration                    active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                 Gi0/5, Gi0/6
20   equipe                            active    Gi0/7, Gi0/8, Gi0/9, Gi0/10
                                                 Gi0/11, Gi0/12, Gi0/13, Gi0/14
30   WIFI                              active    Gi0/15, Gi0/16, Gi0/17, Gi0/18
                                                 Gi0/19, Gi0/20, Gi0/21
```

2.4 Vérification de la fonctionnalité du routage

Pour cela, on ping la passerelle du routeur avec la borne WiFi, qu'on a branché sur VLAN 30 du switch, au nom de Wifi.

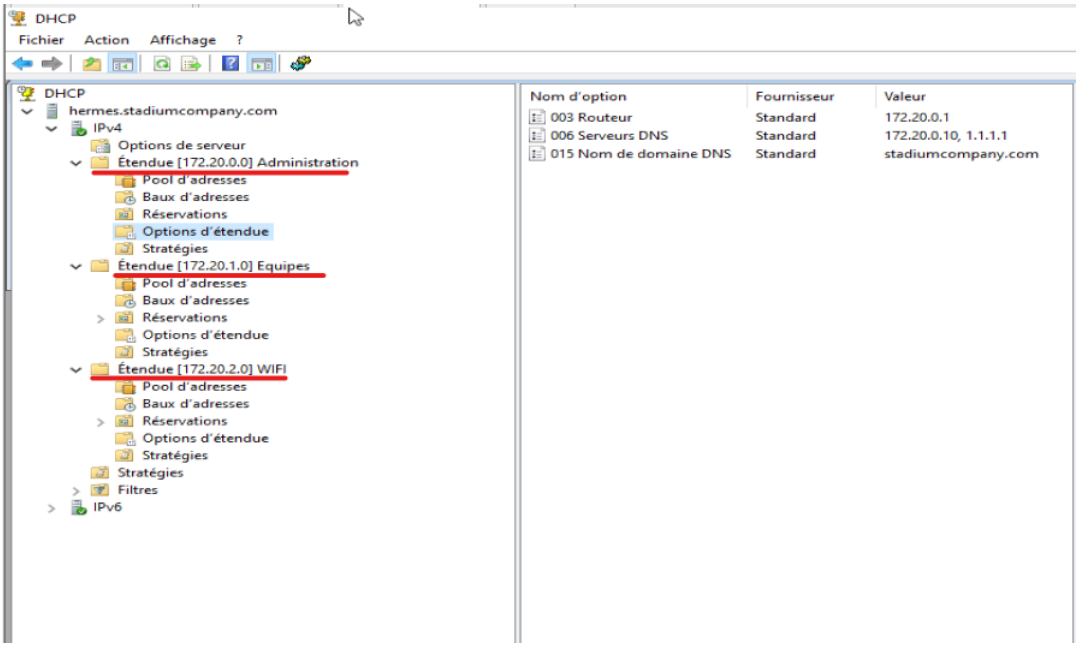
```
ap#ping 172.20.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1001 ms
ap#
```

On voit que ce a bien marché.

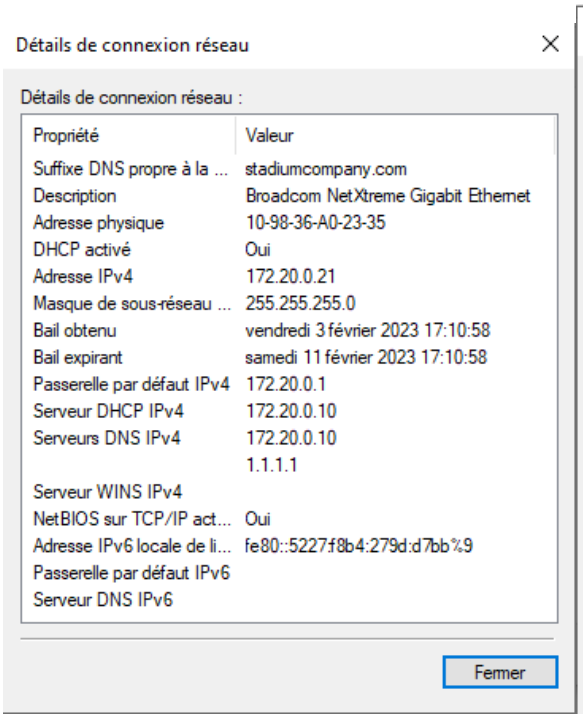
3. Configuration du serveur Radius

3.1 Configuration des VLANS sur le serveur AD :

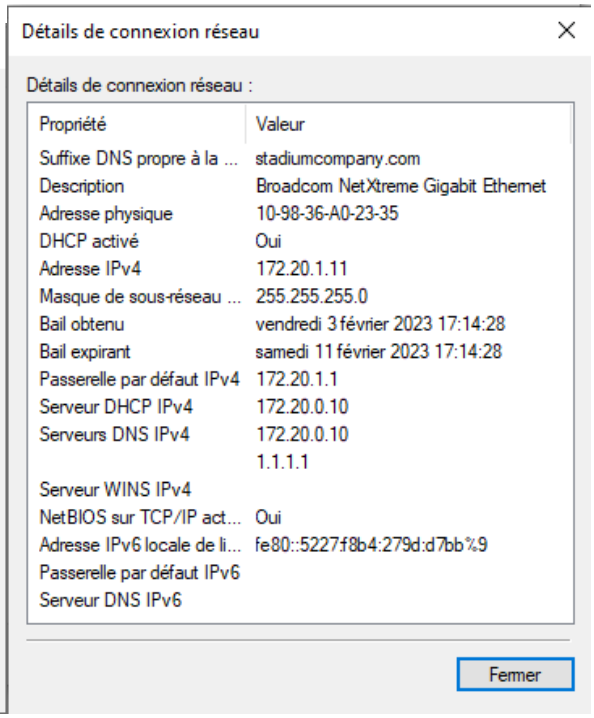
On configure d'abord les étendues, au nombre de trois et qui correspondent aux VLAN Administration, Equipes et WiFi, ainsi que leur passerelle (ici 172.20.0.1) et les adresses DNS.



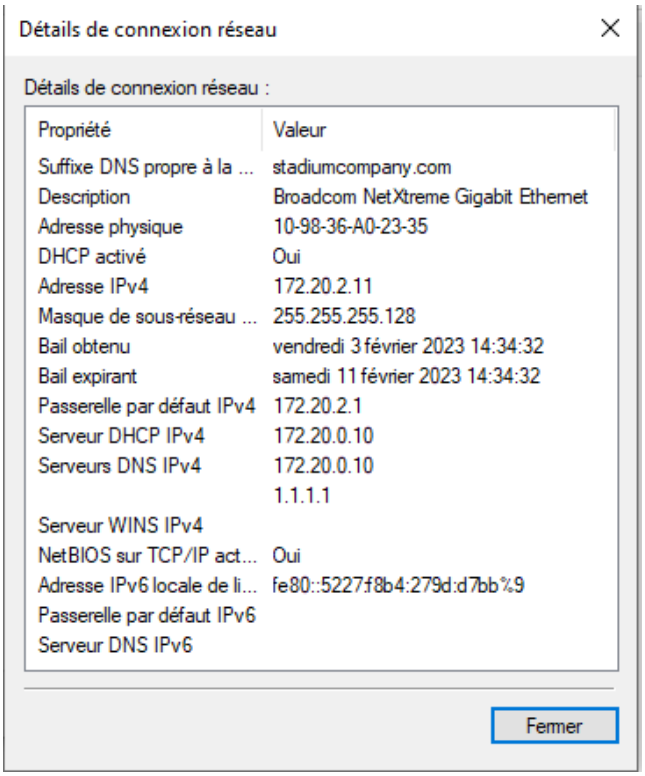
VLAN 10 :



VLAN 20 :



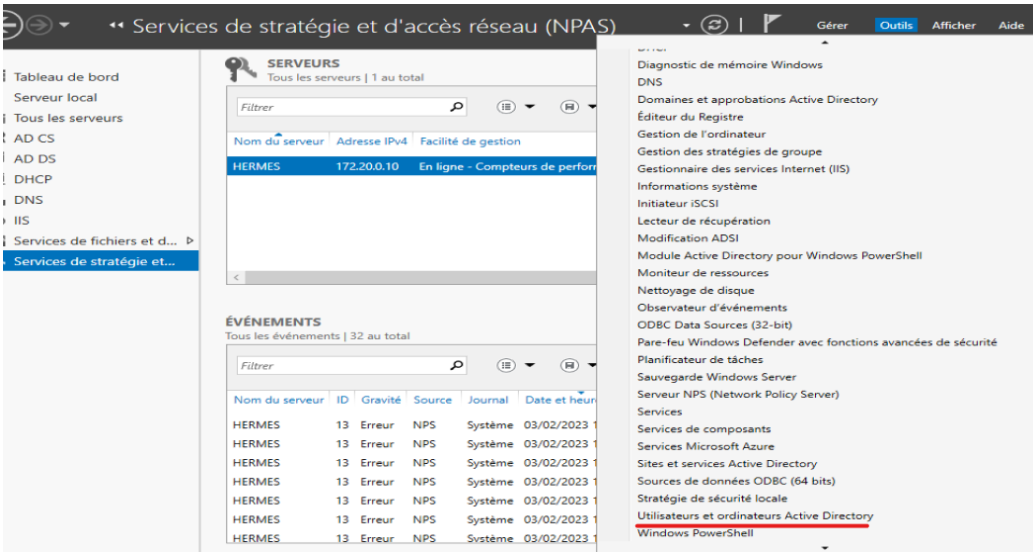
VLAN 30 :



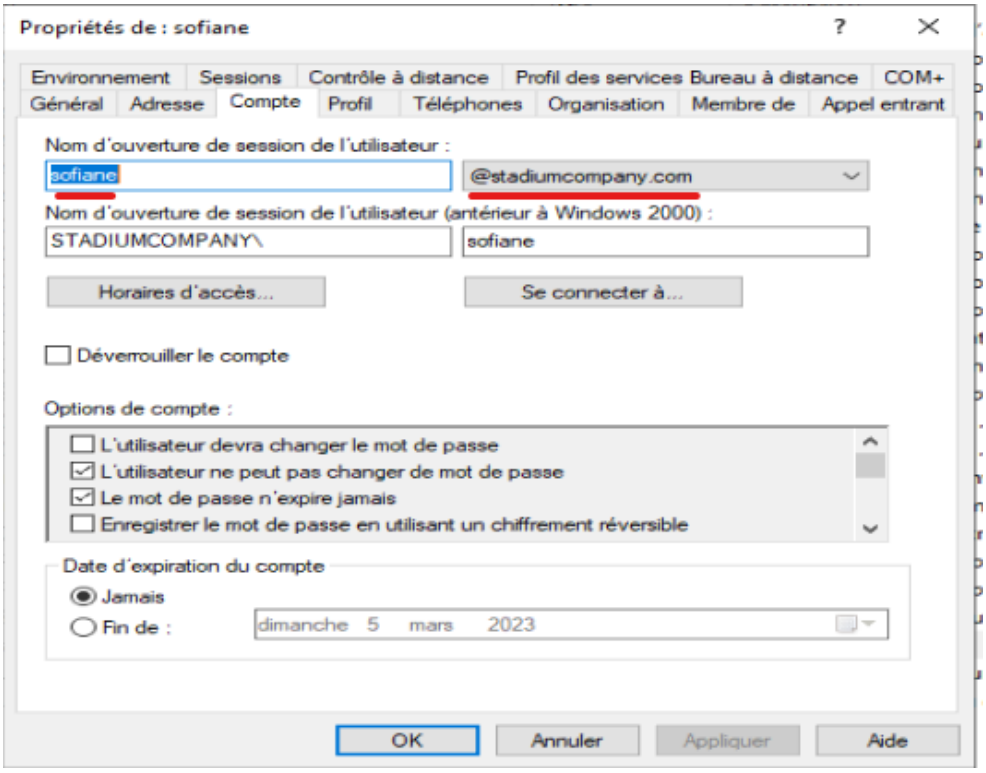
Pour récupérer ces fiches d'information réseau, on s'est connecté à partir d'un ordinateur vers les VLANS des switchs qu'on a configuré précédemment. On voit que toutes les informations sont bien remontées (passerelle par défaut, serveur DHCP et DNS et adresse IP), de même que les configurations des VLANS via le service DHCP du serveur Active Directory (avec les adresses IP qu'on a exclus par exemple).

3.2 Configuration des utilisateurs dans l'Active Directory

Tout d'abord, on créé un nouveau utilisateur qui servira de test pour l'authentification.

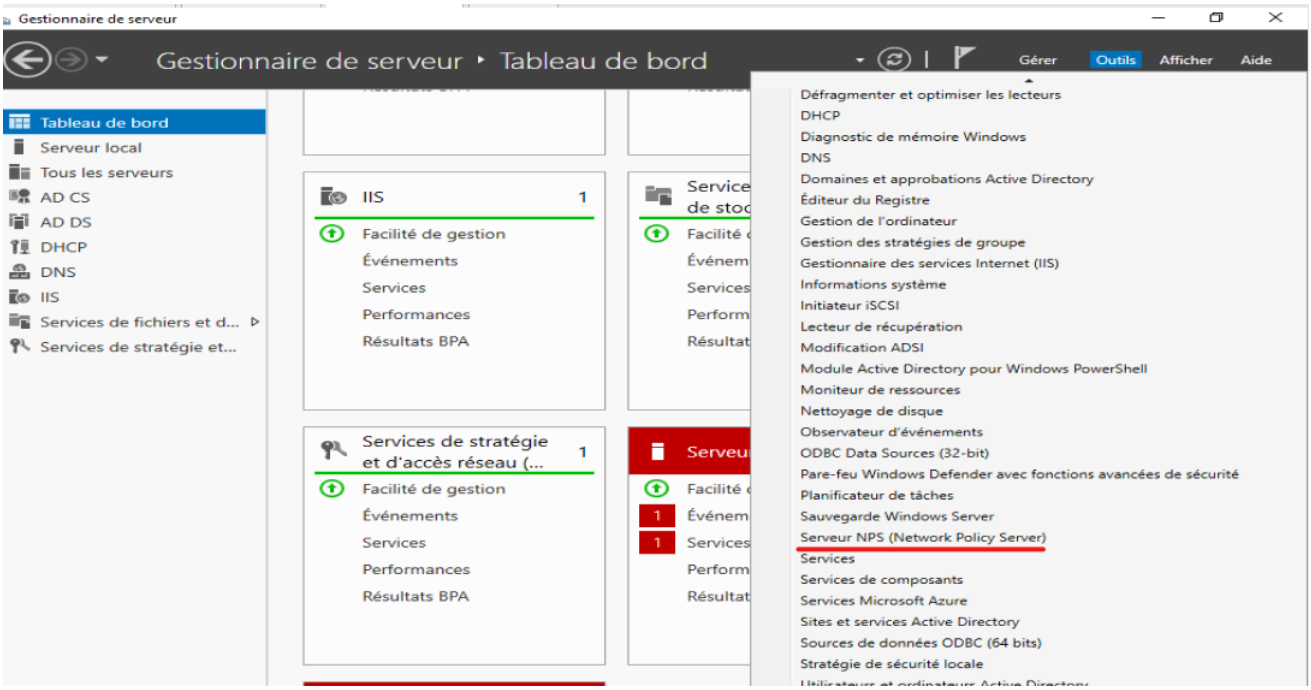


On renseigne le nom d'utilisateur : *sofiane@stadiumcompany.com*

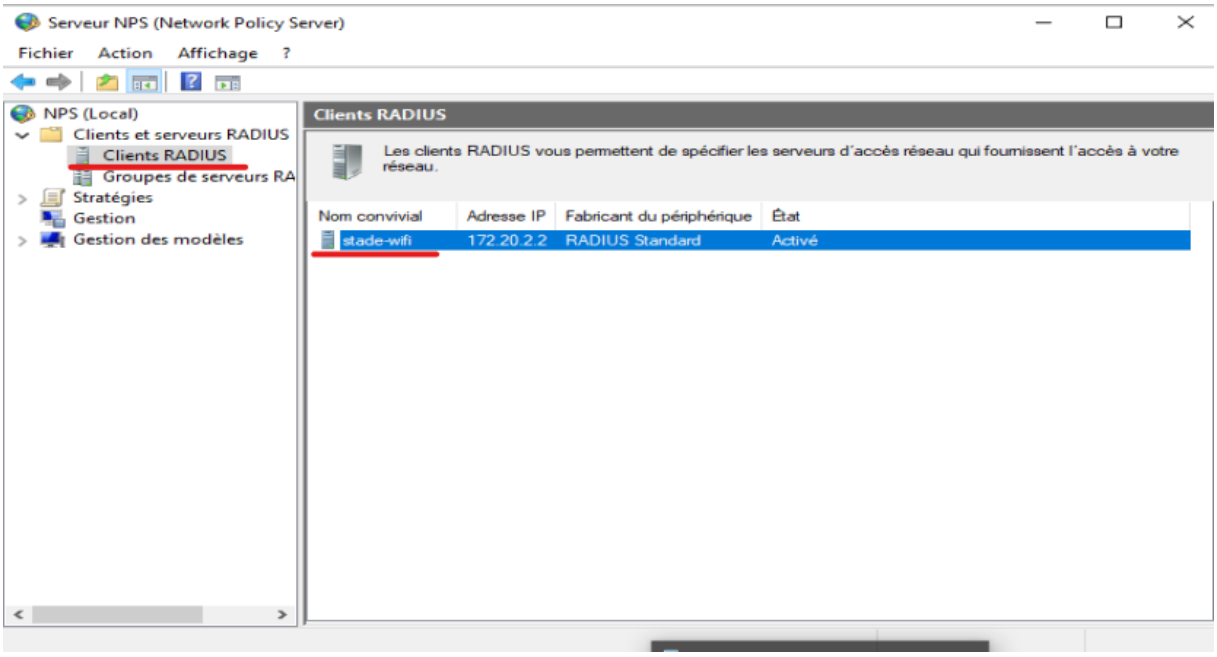


3.3 Configuration du service d'authentification Radius

Après avoir installé l'outil NPS (Network Policy Server), ou le selectionne afin de configurer le serveur Radius.

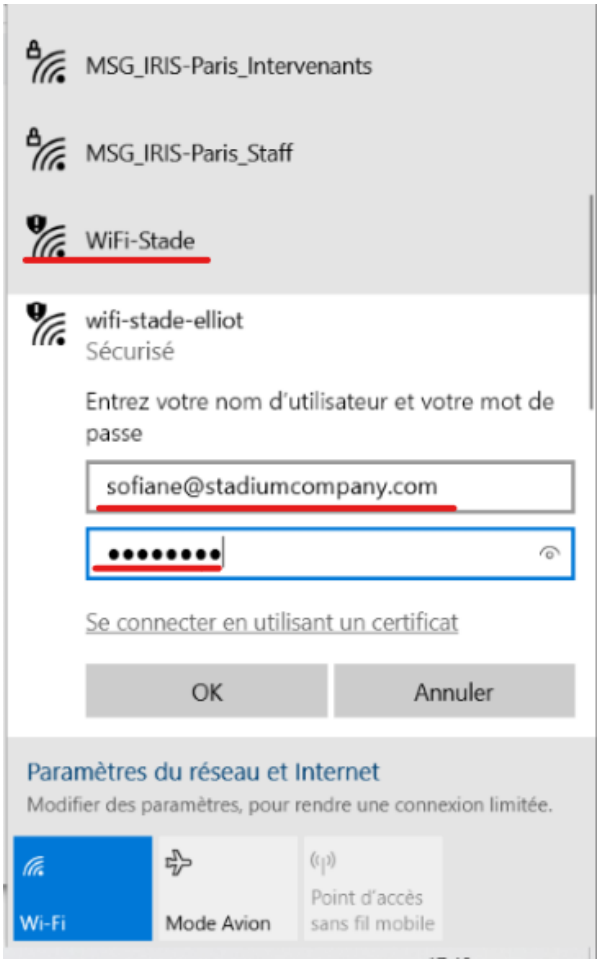


On fait un clic droit sur « Client RADIUS » pour configurer un client Radius.



On renseigne le nom du wifi, puis son adresse IP, ainsi que le mot de passe.

Pour tester que l'authentification via Radius marche bien, on tente de se connecter :



On voit bien que l'on s'est bien connecté :

Après avoir vu que ça marche bien, on va analyser l'authentification avec WireShark, qui est un **outil de capture et d'analyse de paquets**. Il capture le trafic du réseau local pour permettre leur analyse.

On va donc le lancer au moment où l'on tente de se connecter au wifi avec le compte utilisateur précédemment créé.

Comme on le voit ci-dessus, une requête est envoyé par l'utilisateur qui tente de se connecter au serveur radius, qui porte comme adresse IP : 172.20.0.10.

Le serveur accepte cette requête car on voit sur WireShark, « Acces-Accept » (cf ce qui est surligné ci-dessous.