**MISSION 6 : SOLUTION D'INFRASTRUCTURE RÉSEAUX ET SYSTÈME PERMETTANT D'ASSURER L'ACCÈS SANS FIL**

**I-)** Contexte

a) **Presentation de stadium company**

Stadium Company est une société qui s'occupe de la gestion des stades , qui souhaite moderniser l'infrastructure réseau de son stade , la rendre scalable au fur et à mesure que ses ambitions augmentent . Elle emploie 170 personnes à plein temps et 80 à temps partiels . Elle projette ajouter des fonctions haute technologie afin de pouvoir prendre en charge l'organisation des concerts . La direction de Stadium Company n'étant pas compétente en matière d'Infrastructure réseau décide de faire appel à une entreprise de consultants réseaux qui s'en occupera de la conception à la mise en oeuvre en passant par la gestion du projet . Il sera mis en oeuvre en trois phases à savoir :

- La planification du projet et la préparation de la conception réseau haut niveau
- Le développement de la conception reseau détaillée
- La mise en oeuvre de la conception

b) **Presentation NetworkingCompany**

Le prestataire désigné pour l'exécution de ce projet est la société Networking Company, une firme locale spécialisée dans la conception d'infrastructure réseau et le conseil . C'est une société Cisco Premier Partner qui emploie 20 ingénieurs réseaux certifiés et expérimentée dans ce secteur.

Dans le but de concevoir le nouveau plan de l'infrastructure de haut niveau , Networking Company a décrit un profil de l'organisation et des installations sur la base des études menées par ses experts notamment en interrogeant le personnel.

**Mission 6 :**

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.
StadiumCompagny 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).
Éléments du cahier des charges concernant les accès Wifi.
A chaque service est disposé 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.
Prérequis :
- Le système d'information d'AP est opérationnel.
Modification à opérer :
- Proposer une solution d'accès Wifi pour le Vlan Wifi (stade-wifi)
- Proposer une solution d'accès Wifi pour les visiteurs
- Intégrer et configurer le ou les switchs PoE
- Intégrer et configurer les AP Wifi
- Authentification des salariés via le réseau sans fils
- Accès des visiteurs à internet seulement.

**Phase 1 :**

- Proposer une solution d'infrastructure réseau et système permettant d'assurer l'accès sans fils aux salariés et aux visiteurs dans tous les locaux sans interruption de service.

- Proposer un schéma réseau logique et physique et la démarche à mettre en œuvre avec l'ordonnancement des tâches pour assurer cette extension sans fils.

**Phase 2 :**

- Configurer le matériel et les systèmes nécessaires pour mener à bien cette extension d'accès sans fil
- Proposer la batterie de tests nécessaires pour valider votre infrastructure.
- Documentation technique sur les switchs et les AP
- Documentation technique sur le cryptage des données

**Test et comparaison de solution**

Pour assurer la sécurité du réseau on utilisera le **Wi-Fi Protected Access 2** (WPA2 -IEEE 802.11i) en implémentant different protocole qui permettront de répondre aux exigences de sécurité et de transparence auprès des clients.

**Authentification des utilisateurs :**

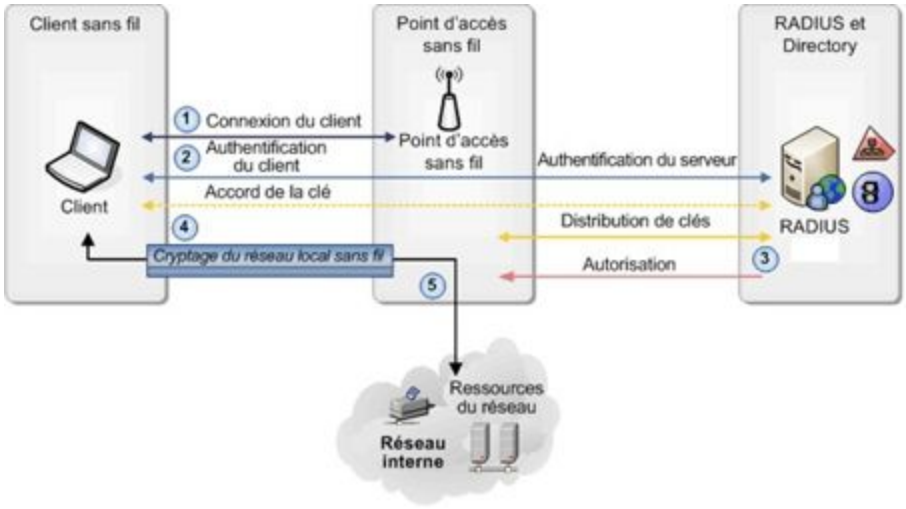
Nous utiliserons un serveur Radius ( **Remote Authentication Dial-in User** ) protocole client -serveur centralisant les données d'authentification .
Pour s'authentifier , l'utilisateur transmet une requête d'accès à un client **RADIUS** pour entrer sur le réseau , ce dernier se charge de demander les informations 'identifiant l'utilisateur (identifiant et mot de passe). Le client RADIUS génère une requête d'accès qu'il transmet au serveur RADIUS , ce dernier préalablement couple avec le service d'annuaire va pouvoir pour aller vérifier les informations envoyés par le client et ainsi valider ou refuser l'accès

**Securite 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 . Elle génère une clé de paquets , mélange les paquets du message , puis remet les paquets dans l'ordre pour retrouver l'intégrité du message , puis remets les paquets dans l'ordre pour retrouver l'intégrité du message grâce à un mécanisme de tri .
- Advanced Encryption Standard (AES): c'est une méthode de chiffrement symétrique (chiffrement 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 relevé 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 minute 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.

Le réseau Wi-Fi utilisera donc la sécurité suivante : WPA2 Entreprise AES. Les bornes Wi-Fi devront être référencées sur le serveur d'authentification afin d'assurer la provenance des connexions. On renseigne un code secret qui ne sera connu que par le point d'accès et le serveur .




**Étude du matériel :**

Pour la mise en place du réseau Wi-Fi nous avons étudié trois bornes :