**I - 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. NetworkingCompany est une société partenaire Cisco Premier Partner. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d’une grande expérience dans ce secteur.

Pour créer la conception de haut niveau, NetworkingCompany a tout d’abord interrogé le personnel du stade et décrit un profil de l’organisation et des installations.

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 technologiques 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.

**1.3 Enseignements sur le système informatique de l’organisation :**

**Organisation de StadiumCompany :**

**Téléphones et PC de StadiumCompany :**

Tous les dirigeants et responsables de StadiumCompany utilisent des PC et téléphones connectés à un PABX vocal numérique. À l’exception des préposés au terrain à temps plein et des gardiens, tous les salariés utilisent également des PC et des téléphones.

Cinquante téléphones partagés sont répartis dans le stade pour le personnel de sécurité. On compte également12 téléphones analogiques, certains prenant également en charge les télécopies et d’autres offrant un accès direct aux services de police et des pompiers. Le groupe sécurité dispose également de 30 caméras de sécurité raccordées à un réseau distinct.

**Installations existantes et prises en charge :**

StadiumCompany propose des installations et une prise en charge de réseau pour deux équipes de sports (Équipe A et Équipe B), une équipe « visiteurs », un restaurant et un fournisseur de concessions.

Le stade mesure environ 220 mètres sur 375. Il est construit sur deux niveaux. En raison de la taille des installations, plusieurs locaux techniques connectés par des câbles à fibre optique sont répartis sur l’ensemble du stade. Les vestiaires des équipes A et B et les salons des joueurs sont situés au premier niveau de la partie sud du stade. Les bureaux des équipes occupent une surface d’environ 15 mètres par 60 au deuxième niveau.

Le bureau et le vestiaire de l’équipe « visiteuse » sont également situés au premier niveau.

Les bureaux de StadiumCompany se trouvent dans la partie nord du stade, répartis sur les deux niveaux.

L’espace des bureaux occupe environ 60 mètres par 18 au premier niveau et 60 mètres par 15 au deuxième niveau.

Les équipes A et B sont engagées dans des compétitions sportives différentes, organisées à des dates différentes. Elles sont toutes les deux sous contrat avec StadiumCompany pour leurs bureaux et services au sein du stade.

**Organisation de l’équipe A :**

L’équipe A compte 90 personnes :

· 4 dirigeants

· 12 entraîneurs

· 14 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et

assistants financiers)

· 60 joueurs

L’équipe A dispose de 15 bureaux dans le stade pour ses employés non joueurs. Cinq de ces bureaux sont partagés. 24 PC et 28 téléphones sont installés dans les bureaux. L’équipe A dispose également d’un vestiaire des joueurs, d’un grand salon pour les joueurs et d’une salle d’entraînement. Les employés non joueurs utilisent les locaux toute l’année. Les joueurs ont accès au vestiaire et aux équipements d’entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones. Des rumeurs indiquent que l’équipe A aurait récemment installé un concentrateur sans fil dans le salon des joueurs.

**Organisation de l’équipe B :**

L’équipe B compte 64 personnes :

· 4 dirigeants

· 8 entraîneurs

· 12 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et

assistants financiers)

· 40 joueurs

L’équipe B dispose de 12 bureaux dans le stade pour ses employés autres que les joueurs. Trois de ces bureaux sont partagés. 19 PC et 22 téléphones sont installés dans les bureaux. L’équipe B dispose également d’un vestiaire des joueurs et d’un grand salon pour les joueurs. Les employés non joueurs utilisent les locaux toute l’année. Les joueurs ont accès au vestiaire et aux équipements d’entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

**Accueil de l’équipe « visiteuse » :**

L’équipe « visiteuse » dispose d’un vestiaire et d’un salon équipés de 10 téléphones. Chaque équipe « visiteuse » demande des services provisoires le jour du match et quelques jours auparavant. Les équipes « visiteuses » passent également un contrat avec StadiumCompany pour les bureaux et services au sein du stade.

**Fournisseur de concessions :**

Un fournisseur de concessions gère les services proposés lors des matchs et événements. Il compte 5 employés à temps plein. Ils occupent deux bureaux privés et deux bureaux partagés équipés de cinq PC et sept téléphones. Ces bureaux se trouvent dans la partie sud du stade, entre les bureaux des équipes A et B. Deux employés à temps partiel prennent les commandes auprès des loges au cours des événements. Le concessionnaire de services emploie des intérimaires saisonniers pour gérer 32 stands permanents et autres services répartis sur l’ensemble du stade. Il n’y a actuellement aucun téléphone ni PC dans les zones de vente.

**Organisation du restaurant de luxe :**

Le stade propose un restaurant de luxe ouvert toute l’année. En plus des salles et des cuisines, le restaurant loue des bureaux auprès de StadiumCompany. Les quatre dirigeants ont chacun un bureau privé. Les deux employés en charge des questions financières et comptables partagent un bureau. Six PC et téléphones sont pris en charge. Deux téléphones supplémentaires sont utilisés en salle pour les réservations.

**Prise en charge des loges de luxe :**

Le stade compte 20 loges de luxe. StadiumCompany équipe chaque loge d’un téléphone permettant de passer des appels locaux et d’appeler le restaurant et le concessionnaire de services.

**Prise en charge de la zone de presse :**

StadiumCompany propose un espace presse avec trois zones partagées :

· La zone presse écrite accueille généralement 40 à 50 journalistes au cours d’un match. Cette zone partagée est équipée de 10 téléphones analogiques et de deux ports de données partagés. On sait qu’un journaliste stagiaire apporte un petit point d’accès sans fil lorsqu’il couvre un match.

· La zone de presse pour les radios peut accueillir 15 à 20 stations de radio. Elle estéquipée de 10 lignes téléphoniques analogiques.

· La zone de presse télévisée accueille généralement 10 personnes. Elle est équipée de 5 téléphones.

**Prise en charge de site distant :**

StadiumCompany compte actuellement deux sites distants : une billetterie en centre-

ville et une boutique de souvenirs dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local. Le stade est connecté au FAI local à l’aide de FAI1, un routeur de services gérés qui appartient au FAI. Les deux sites distants sont connectés au même FAI par les routeurs FAI2 et FAI3, fournis et gérés par le FAI. Cette connexion permet aux sitesdistants d’accéder aux bases de données situées sur les serveurs dans les bureaux de StadiumCompany. StadiumCompany dispose également d’un routeur de périmètre, nommé Routeur de périphérie, connecté au routeur FAI1 du stade.

**En résumé :**

Nombre de serveurs : 9 dont : (web, DHCP, commerce électronique, comptabilité(x3), paie)

Utilisateurs :

- 35 dirigeants

- 135 employés

- environs 80 intérimaires

- équipe A (90 personnes : 4 dirigeants, 12 entraineurs, 14 employé, 60 joueurs)

- équipe B

- équipe visiteurs

- restaurant

- fournisseur de concessions

- équipe B (4 dirigeants, 8 entraineurs, 12 employé, 40 joueurs)

- équipe visiteurs :

- fournisseur de concessions 5 employé 2 employé a temps partiel : intérimaire non défini

- restaurant de luxe : 4 dirigent, 2 employé,

- 20 loges de luxe

- 2 sites distants

Services : DNS, DHCP, web

- dirigeants : PC et téléphones connecter à un PABX

- personnel et sécurité : 50 téléphones et PC réparti dans le stade

- 12 téléphones analogiques répartis dans le stade qui prennent en charges la

télécopie, et d’autres offrant un accès direct aux services de police et pompier.

- locaux connecté par fibre optiques

- équipe A : 15 bureaux dont 5 partagé 24 PC et 28 téléphones dans ces bureaux ; vestiaire 5 téléphone, salon des joueurs : 15 téléphones

- équipe B : 12 bureaux dont 3 partagé, 19 PC et 22 téléphones, vestiaires 5 téléphones, salon des joueurs 15 téléphones

- équipe visiteur : salon et vestiaire doté de 10 téléphones

- fournisseur de concession : 2 bureau privée 5 PC et 7 téléphones, 32 stand permanent non équipé pour le moment.

- restaurant de luxe : 4 bureau privé, 6 téléphones + 2 utilisé en salle pour les réservations

- 20 loges de luxe : 20 téléphones

- zone de presse : 10 téléphones analogique, 2 ports de données réseaux + Wireless AP

- 2 sites distant : connecter Via VPN (router FAI x3 pour gérer la connexion StadiumCompany dispose d’un routeur de périmètre

Pas d’information sur les processus, contrats et chartes informatiques.

**II - Cahier des charges :**

Cette année, vous allez intégrer la division du stade de StadiumCompany. Vous

serez chargé de la maintenance des systèmes et réseaux informatiques.

StadiumCompany est composé de plusieurs sites :

Site 1 : Stade (hébergement informatique, siège social et centre administratif)

Site 2 : Billetterie (vente des billets)

Site 3 : Magasin (vente des souvenirs)

Les différentes solutions retenues pour l’étude du projet d’un point de vue général de

StadiumCompany pourront faire l’objet de documentations techniques suivant la

complexité de la mise en œuvre.

**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.

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).

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 oeuvre 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

**III - Solutions & Choix**

### Test et comparaison des solutions :

Pour assurer la sécurité 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 le réseau des visiteurs médicaux, 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.

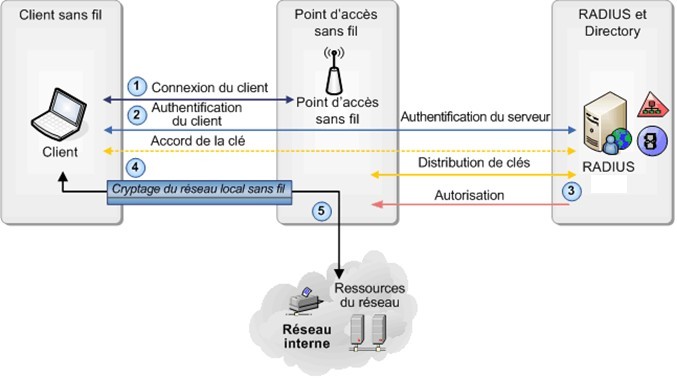
Pour s’authentifier, le poste utilisateur transmet une requête d’accès à un client RADIUS pour entrer sur le réseau, ce dernier se charge de demander les informations identifiant l’utilisateur (utilisateur & mot de passe). Le client RADIUS génère une requête d’accès qu’il transmet au serveur RADIUS, ce dernier préalablement couplé avec le service d’annuaire 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.

Le réseau Wi-Fi utilisera donc la sécurité suivante : WPA2 Enterprise 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 :



Références

Illustrations des modèles

Descriptions

D-LINK DAP-2590

-Interface

gestion sécurisée

- Ligne

de

de

commande (telnet

et SSH)

* WPA2 AES
* Filtre MAC
  + RADIUS
* SSID Caché
* Multi-SSID
  + PoE

- 802.11a/b/g/n

* + VLAN 802.1Q

|  |  |  |
| --- | --- | --- |
| HP E-MSM430 |  | * Interface de gestion sécurisée * Ligne de commande (telnet et SSH) * WPA2 AES * Filtre MAC   + RADIUS * SSID Caché * Multi-SSID   + PoE   - 802.11a/b/g/n   * + VLAN 802.1Q |
| CISCO Aironet 1042 N |  | * Interface de gestion sécurisée * Ligne de commande (telnet et SSH) * WPA2 AES * Filtre MAC   + RADIUS * SSID Caché * Multi-SSID   + PoE   - 802.11a/b/g/n   * + VLAN 802.1Q |

### Choix de solutions :

Suite cette comparaison nous avons choisi le point d’accès Aironet de Cisco qui est le plus adaptés à nos besoins. Elle est compatible avec toutes les contraintes de sécurisation besoin, son avantage par rapport aux autres points d’accès est la garantie matérielle à vie. De plus notre réseau étant essentiellement formé de matériel du constructeur Cisco, cette borne respectera l’homogénéité matérielle.

### Objectifs et but du projet :

L’objectif de ce projet est la mise en place d’une architecture sans fil accessible et propre à chaque vlan avec un accès visiteur. Cette architecture doit avoir StadiumCompany veut proposer une solution d’accès Wifi pour le Vlan Wifi (stade- wifi) et pour les visiteurs du stade. Le groupe souhaite que les point d’accès sans fil soient compatible avec la technologie PoE pour des raisons esthétiques et éviter des pertes des chargeurs électriques. L’architecture wifi doit permettreune authentification des salariés via le réseau sans fil grâce à la mise en place d’un serveur d’authentification de type Radius. Le plan de sécurité de l’architecture doit permettre l’accès des visiteurs uniquement à internet.

# Annexe

**Procedure :**

### Configuration de l’AP

Activation du pont entre les interfaces wifi et le FastEthernet

AP#configure terminal AP(config)#bridge irb AP(config)#bridge 1 route ip

### Configuration de l’adresse IP de l’AP :

AP#configure terminal AP(config)#interface BVI 1

AP(config-if)#ip address 172.20.2.10 255.255.255.128 AP(config-if)#no shutdown

AP(config-if)#end

### Activation de l’interface graphique

AP(config)#ip http secure-server AP(config)#end

### Configuration de la passerelle par défaut

AP(config)#ip default-gateway 172.20.0.1

*Configuration des différents SSID*

AP(config)#dot11 vlan-name administration vlan 10 AP(config)#dot11 vlan-name equipes vlan 20 AP(config)#dot11 vlan-name vlan 20 AP(config)#dot11 vlan-name VIP-Presse vlan 30 AP(config)#dot11 vlan-name fournisseur vlan 40 AP(config)#dot11 vlan-name restaurant vlan 50 AP(config)#dot11 vlan-name wifi vlan 100 AP(config)#dot11 vlan-name camera vlan 200

AP(config)#dot11 ssid administration AP(config-ssid)#vlan 10

AP(config-ssid)#authentication open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid equipes AP(config-ssid)#vlan 20

AP(config-ssid)#authentication open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid VIP-Presse AP(config-ssid)#vlan 30

AP(config-ssid)#authentication open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid fournisseur AP(config-ssid)#vlan 40

AP(config-ssid)#authentication open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid restaurant AP(config-ssid)#vlan 50

AP(config-ssid)#authentication open AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid wifi AP(config-ssid)#vlan 100 AP(config-ssid)#authentication open AP(config-ssid)#mbssid guest-mode AP(config-ssid)#exit

AP(config-ssid)#dot11 ssid camera AP(config-ssid)#vlan 200

AP(config-ssid)#authentication open AP(config-ssid)#exit

### Configuration de l’interface radio

AP(config)#interface Dot11Radio0 AP(config-if)#mbssid

AP(config-if)#encryption vlan 10 mode wep mandatory AP(config-if)#encryption vlan 10 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 20 mode wep mandatory AP(config-if)#encryption vlan 20 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 30 mode wep mandatory AP(config-if)#encryption vlan 30 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 40 mode wep mandatory AP(config-if)#encryption vlan 40 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 50 mode wep mandatory AP(config-if)#encryption vlan 50 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 100 mode wep mandatory AP(config-if)#encryption vlan 100 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#encryption vlan 200 mode wep mandatory AP(config-if)#encryption vlan 200 key 1 size 128bit 7 01234567890123456789abcdef

AP(config-if)#ssid administration AP(config-if)#ssid equipes AP(config-if)#ssid VIP-Presse AP(config-if)#ssid fournisseur AP(config-if)#ssid restaurant AP(config-if)#ssid wifi AP(config-if)#ssid camera AP(config-if)#no shutdown AP(config-if)#exit

* + 1. **Prise en charge du protocole 802.q**

AP#conf terminal AP(config)#interface Dot11Radio0.10

AP(config-subif)#encapsulation dot1Q 10

AP(config-subif)#bridge-group 10 AP(config-subif)#no sh AP(config-if)#exit

AP(config-subif)#encapsulation dot1Q 20

AP(config-subif)#bridge-group 20 AP(config-subif)#no sh AP(config-if)#exit

AP(config-subif)#encapsulation dot1Q 30

AP(config-subif)#bridge-group 30 AP(config-subif)#no sh AP(config-if)#exit

AP(config-subif)#encapsulation dot1Q 40

AP(config-subif)#bridge-group 40 AP(config-subif)#no sh AP(config-if)#exit

AP(config-subif)#encapsulation dot1Q 50

AP(config-subif)#bridge-group 50 AP(config-subif)#no sh AP(config-if)#exit

AP(config-subif)#encapsulation dot1Q 100

AP(config-subif)#bridge-group 100 AP(config-subif)#no sh

AP(config-if)#exit

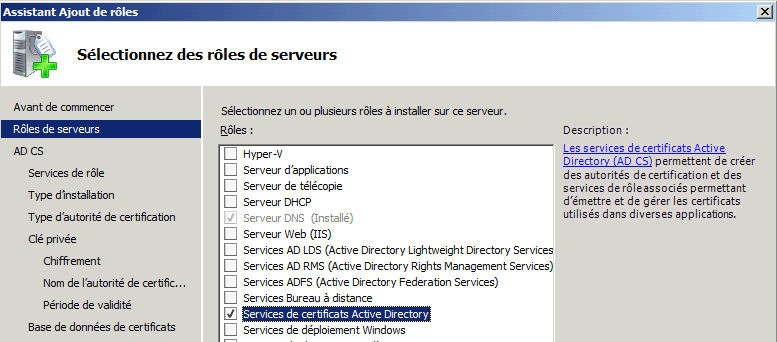
AP(config-subif)#encapsulation dot1Q 200

AP(config-subif)#bridge-group 200 AP(config-subif)#no sh

AP(config-if)#exit

### Configuration du serveur Radius

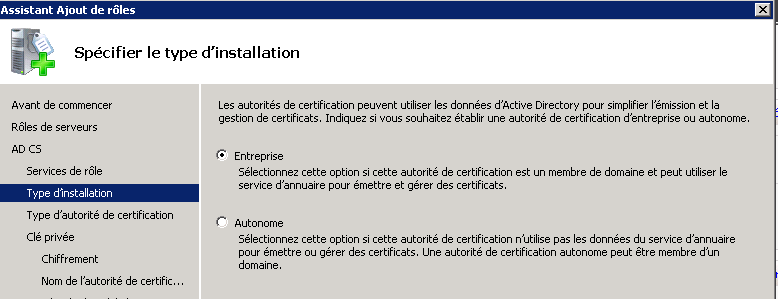
### Ajout du rôle « Services de certificats Active Directory »



### Installation d’une autorité de certification.



### On choisit une installation du type Autorité de certification d'entreprise



### On spécifie un type d’autorité de certification (racine) :



### Création d’une nouvelle clé privée



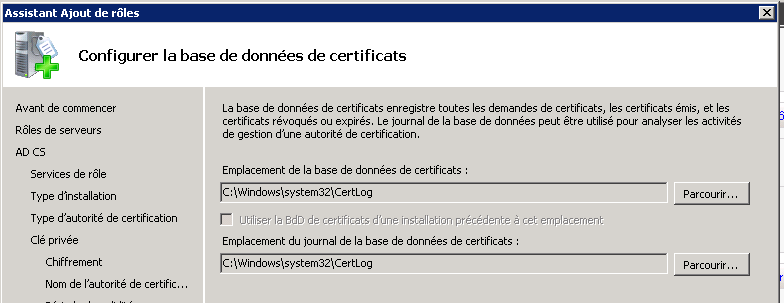
### On choisit la méthode de chiffrement par défaut :

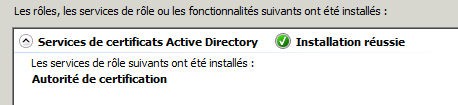


### Choix d’une période de validité du certificat



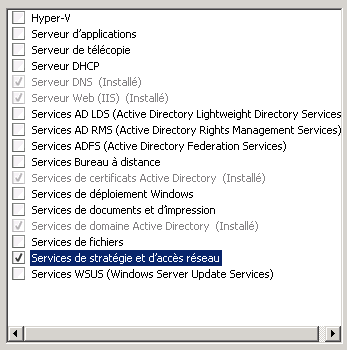
### Configuration de l'emplacement d'installation de la base de données de certificats

Fin de l’installation :

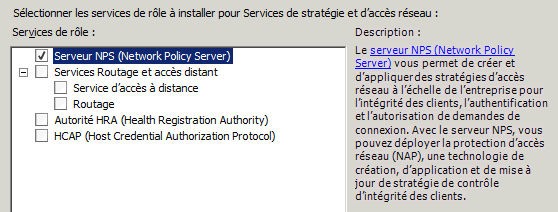


### Installation du serveur RADIUS - NPS (Network Policy Server)

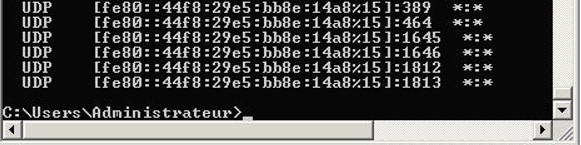
Dans l'assistant de gestion des rôles, choisir "Services de stratégie et d'accès réseau".



### Installation du rôle serveur NPS



Pour vérifier le bon fonctionnement du service NPS sur le serveur et afficher les ports en écoute sur celui-ci utilisé la commande **netstat -a**



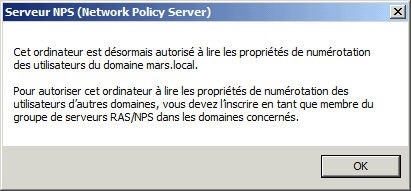
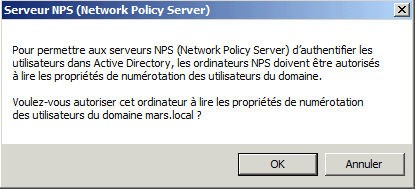
NPS écoute sur les ports suivants par défaut :

* + - * + 1812, 1645 pour l'authentification.
        + 1813,1646 pour la gestion.

### CONFIGURATION DU SERVEUR RADIUS NPS

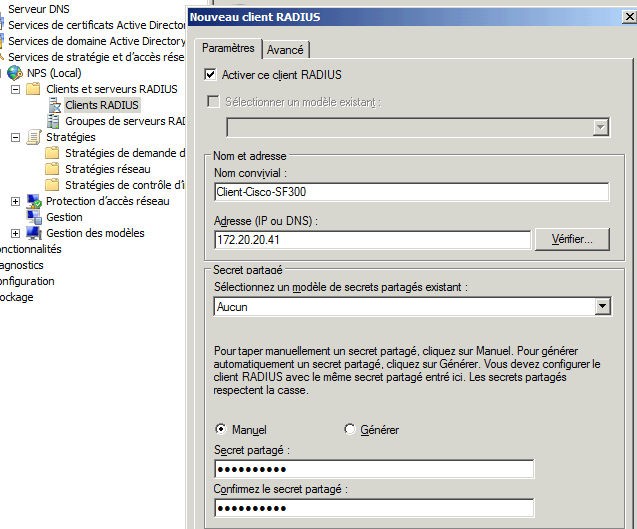
### Inscrire NPS dans Active Directory pour lui permettre d'interroger la base des utilisateurs.

Dans Menu à Action

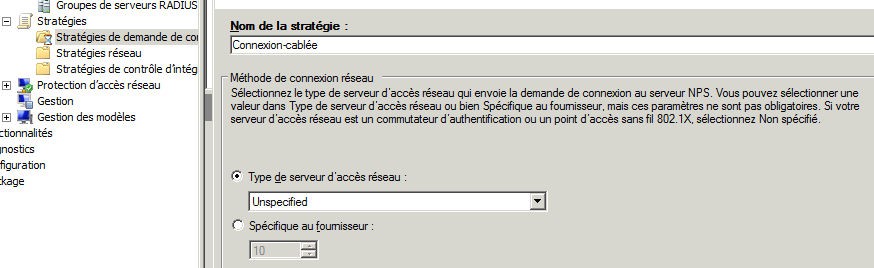


### Déclaration d'un client RADIUS

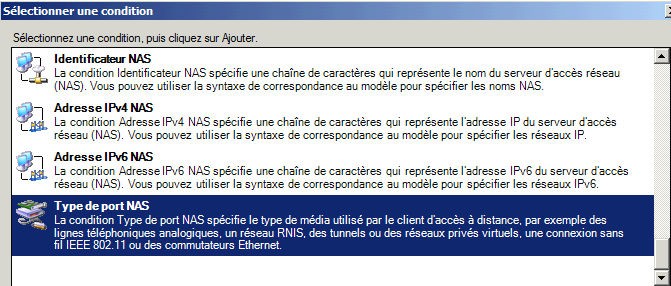
Sur l'entrée *Clients RADIUS*, clic droit è Nouveau Client RADIUS

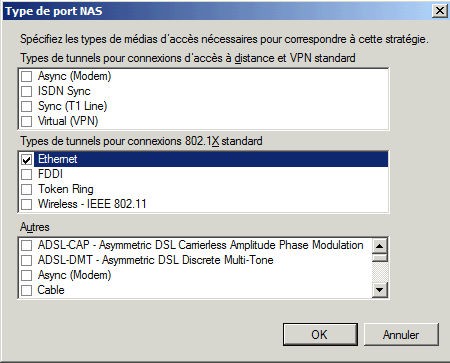


### Déclaration d'une stratégie de demande de connexion



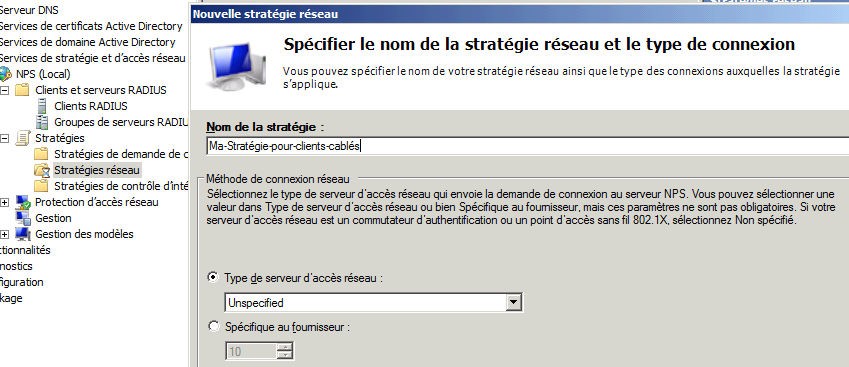
### Choisir un type de port NAS

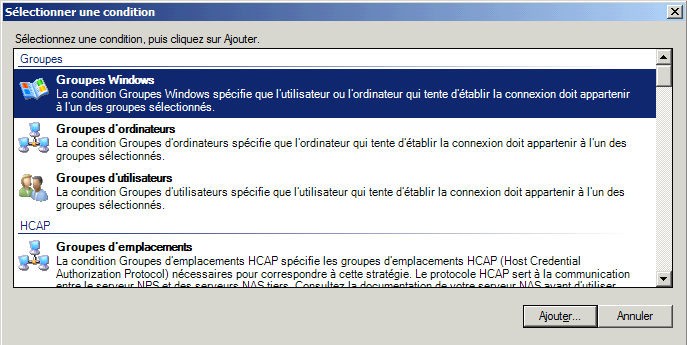


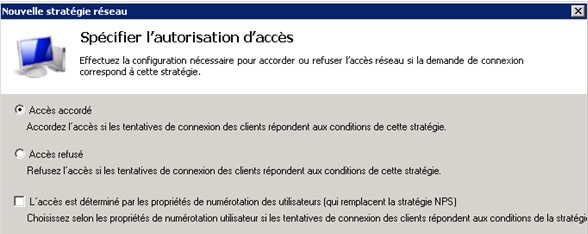
On choisit ici Ethernet

### Déclaration d'une stratégie réseau (stratégie d'accès au réseau)

Sur l'entrée Stratégie Réseau, faire un clic droit è Nouvelle Stratégie réseau

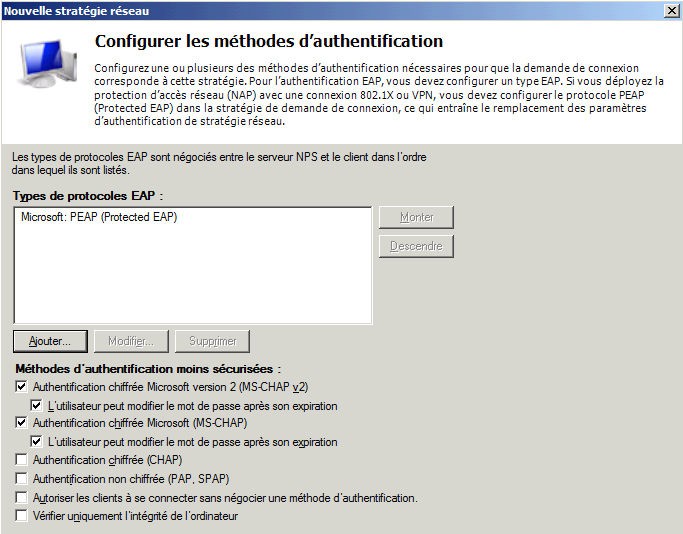


Condition à la validation de la stratégie : l'utilisateur doit être membre d'un groupe AD

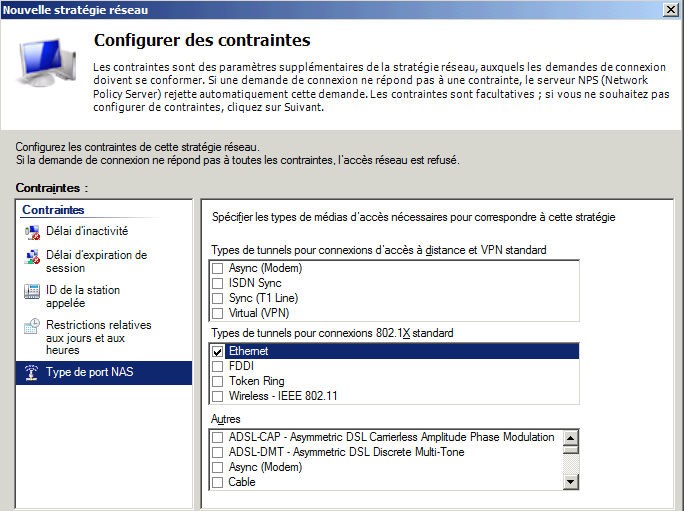
Condition à la validation de la stratégie : l'utilisateur doit être membre d'un groupe AD

Spécifier l’autorisation d’accès :

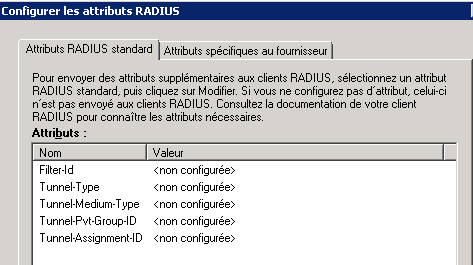
### Déclaration des protocoles EAP et PEAP



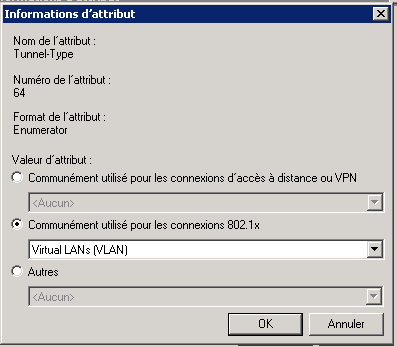
On accepte les Types de ports NAS Ethernet :



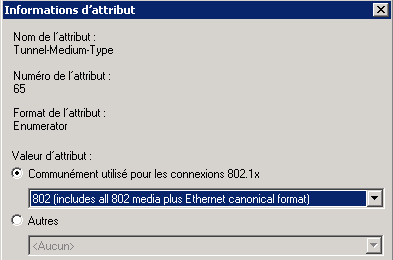
### Ajout des attributs de contrôle de trafic

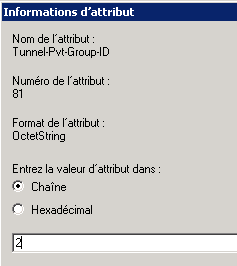


### Modification des attributs Tunnel-Type, Tunnel-Medium-Type et Tunnel-Pvt-Group- ID



### Modification des attributs Tunnel-Type, Tunnel-Medium-Type et Tunnel-Pvt-Group- ID

Tunnel-Medium-Type

Tunnel-Pvt-Group-ID :

Écran récapitulatif de la configuration :

