**République Algérienne Démocratique et Populaire**

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**Université Abderrahmane. Mira de Béjaia**

**Faculté des Sciences exactes**

**Département Informatique**


*Mémoire de fin de cycle*

**En vue de l'obtention du diplôme de Master professionnel en Informatique**

**Option : Administration et sécurité des réseaux**

# Thème

# *Mise en place d'une solution d'authentification RADIUS Cas :Cevital de Bejaia*

**Présenté par :**

$M^{lle}$ **Tighilt Dihia**

$M^{lle}$ **Hamoudi Asma**

**Devant le jury composé de :**

| | |
|---|---|
| **Président** | $M^{lle}$ **Hamza Lamia** |
| **Examinateur** | $M^{r}$ **Baadache Abderrahmane** |
| **Examinateur** | $M^{lle}$ **Ikan Sonia** |

**Promoteur** $M^r$ **Sider Abderrahmane**
**Co-Promoteur** $M^r$ **Atsi Djebbar**

**Années universitaire 2012-2013**

# Remerciements

**Louange A Dieu, le miséricordieux, sans Lui rien de tout cela n'aurait pu être.**

***N***ous tenons tout d'abord à remercier $M^r$ SIDER Abderrahmane pour l'honneur qu'il nous a fait en acceptant de nous encadrer. Ses conseils précieux ont permis une bonne orientation dans la réalisation de ce modeste travail.

***n***ous remercions également $M^r$ ATSI Djebbar pour son grand intérêt porté à ce travail, son suivi, patience et remarques constructives qui nous ont beaucoup aidé.

***U***n grand merci pour l'organisme d'accueil CEVITAL, qui nous a accepté comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel.

***N***ous exprimons également notre gratitude au président $M^{lle}$ HAMZA Lamia et au membre de jury $M^r$ BADAACHE Abderrahmane et $M^{lle}$ BATTAT Nadia qui nous ont honorés en acceptant de juger notre travail et consacrer leurs temps à la lecture et à la correction de ce mémoire.

***N***os remerciements s'adressent aux enseignants et aux personnels administratifs de département Informatique.

***N***os remerciements les plus vifs vont tout particulièrement à nos parents,nos familles et à tous nos amis.

# Dédicaces

***O***n tient à dédier ce modeste travail à notre raison de vivre,d'espérer, à notre source de courage, à ceux qu'on a de plus chères, nos parents,pour leurs encouragements et leurs sacrifices sans limite, pour que nous puissions franchir tout obstacle durant toutes nos années d'étude que le dieu nous les gardent en très bonne santé.

***A*** nos trés chèrs frères et soeurs : Sieffddine,Younes,Kherddine,Wahiba,Nadjet,Silia,Milissa Wissam que nous estimont beaucaup.

***A*** nos chèrs grands parents.

***A*** nos tantes et oncles.

***A*** tous nos cousins et cousines.

***A*** nos enseignants pour leurs patience, leurs soutien,leurs encouragements et à nos amis Pour leur témoigner une amitié et fidélité indéfinies.

***A*** tous les étudiants en $2^{eme}$ master informatique de l'université de Béjaia.

***Asma , Dihia***

# Table des matières

**Liste des figures** **i**

**Glossaire** **iv**

**Introduction générale** **1**

**1 Généralités sur les réseaux et sécurité informatique** **3**

1.1 Définition d'un réseau . . . . . 4

1.2 Modèle OSI . . . . . 4

1.3 Le modèle Client/serveur . . . . . 5

1.3.1 Notions de base . . . . . 5

1.3.2 Définition . . . . . 6

1.3.3 Présentation de l'architecture Client/serveur . . . . . 6

1.3.4 Fonctionnement d'un système Client /serveur . . . . . 6

1.4 Les attaques . . . . . 7

1.5 La Sécurité informatique . . . . . 8

1.5.1 Définition . . . . . 8

1.5.2 Notions sur la cryptographie . . . . . 8

1.5.3 Les services de la sécurité informatique . . . . . 8

1.5.4 Outils et systèmes d'authentification . . . . . 9

1.5.5 Fonction de hachage . . . . . 12

1.5.6 Signature numérique . . . . . 13

1.5.7 La politique de sécurité . . . . . 14

1.5.8 Les outils de sécurité . . . . . 16

1.6 Les VLAN(Virual Local Area Network) . . . . . 17

1.6.1 Présentation de VLAN . . . . . 17

1.6.2 Types de VLAN . . . . . 17

1.6.3 Les avantages de VLAN . . . . . 18

**2 Présentation de l'organisme d'acceuil 19**

2.1 Présentation de l'organisme d'acceuil . . . . . 20
2.2 Organigramme de l'entreprise . . . . . 21
2.3 Activités de CEVITAL . . . . . 23
2.4 Mission et objectifs . . . . . 23
2.5 Architecture actuelle du réseau LAN de CEVITAL de Bejaia . . . . . 24
2.6 Problématique . . . . . 24
2.7 Solutions proposée . . . . . 25

**3 Etude des solutions proposées 27**

3.1 Expression de la politique de sécurité . . . . . 28
3.2 Les équipements réseau . . . . . 28
3.3 Le protocole RADIUS . . . . . 29
3.3.1 Historique . . . . . 29
3.3.2 Présentation de protocole RADIUS . . . . . 29
3.3.3 Rôles de protocole RADIUS . . . . . 29
3.3.4 Principes de protocole RADIUS . . . . . 29
3.3.5 Eléments d'authentification RADIUS . . . . . 30
3.3.6 Le fonctionnement de protocole RADIUS . . . . . 33
3.3.7 RADIUS et Les protocoles de mots de passe . . . . . 36
3.3.8 Le protocole RADIUS et la couche de transport UDP . . . . . 36
3.4 Le Protocole 802.1x . . . . . 36
3.4.1 Présentation . . . . . 36
3.4.2 Principe Général de 802.1x . . . . . 37
3.4.3 Mécanisme Général . . . . . 39
3.4.4 Authentification basée sur le contrôle des ports . . . . . 39
3.4.5 Méthode d'authentification 802.1x . . . . . 39
3.5 Objectifs de l'authentification 802.1x . . . . . 48

**4 Mise en oeuvre et réalisation 50**

4.1 les composantes nécessaires : . . . . . 51
4.2 Les outils utilisés . . . . . 51
4.2.1 Virtualisation . . . . . 51
4.2.2 Windows Server 2008 R2 . . . . . 51
4.2.3 GNS3(Graphical Network Simulator) . . . . . 56

4.3 Présentation des VLANs utilisés . . . . . 56
4.4 Présentation de l'architecture réseau . . . . . 57
4.5 **Configuration de la partie réseau :** . . . . . 57
4.5.1 Création des vlans . . . . . 57
4.5.2 Configuration des interfaces des Vlan(Attribution d'adresses et Activation) . . . . . 59
4.5.3 Configuration de l'interface fa0/0 . . . . . 62
4.5.4 Création des sous interface logiques (Encapsulation des vlan) . 62
4.5.5 Activation du routage . . . . . 63
4.5.6 Configuration du commutateur en tant que serveur DHCP . . 66
4.5.7 Configuration de l'authentification . . . . . 71
4.6 **Configuration de serveur :** . . . . . 75
4.6.1 Attribution d'une adresse Ip statique au serveur . . . . . 75
4.6.2 Création des groupes et des utilisateurs dans l'Active Directory 76
4.6.3 Installation de service "Network Policy and Access Services"( Services de Stratégie et d'accés réseau) . . . . . 82
4.6.4 configuration de "NPS" en tant que serveur RADIUS . . . . . 84
4.7 **Configuration de client d'accès (Windows XP)** . . . . . 95
4.8 Tests . . . . . 98
4.8.1 Authentification RADIUS 802.1x . . . . . 98
4.8.2 Authentification RADIUS . . . . . 105

**Conclusion** **110**

**Bibliographie** **112**

# Liste des figures


1.1 Modèle OSI . . . . . 5
1.2 Modèle Client/Serveur . . . . . 7
1.3 les étapes d'authentification de protoccole PAP . . . . . 10
1.4 les étapes d'authentification de protoccole CHAP . . . . . 11
1.5 la signature numérique . . . . . 13

2.1 Plan de masse du complexe CEVITAL . . . . . 21
2.2 La direction Système d'informations . . . . . 22
2.3 Architecture actuelle du réseau LAN de CEVITAL de Bejaia . . . . . 24
2.4 Schéma global de la solution proposée . . . . . 25

3.1 principe de protocole RADIUS . . . . . 30
3.2 L'authentification Radius . . . . . 32
3.3 L'identifiant . . . . . 33
3.4 fonctionnement de protocole RADIUS . . . . . 34
3.5 Format des paquets RADIUS . . . . . 35
3.6 Acteurs principaux de 802.1x . . . . . 37
3.7 Accès avant authentification . . . . . 38
3.8 Accès après authentification . . . . . 38
3.9 Principe des ports contrôlés et non contrôlés . . . . . 40
3.10 Types EAP . . . . . 41
3.11 Trame EAP . . . . . 41
3.12 Les couches EAP . . . . . 42
3.13 Echange des messages EAP . . . . . 45
3.14 Étape " identité externe " d'EAP . . . . . 47
3.15 Étape " Négociation de protocole " d'EAP . . . . . 48

4.1 Ajout de services de domaine Active Directory . . . . . 53
4.2 Installation de Active Directory . . . . . 54
4.3 Installation de Active Directory en mode avancé . . . . . 55
4.4 Création de domaine "cevital.local" . . . . . 56
4.5 Nom NetBIOS de domaine et le niveau fonctionnel de la forêt . . . . 57
4.6 l'emplacement des fichiers Active Directory et Introduction de mot de passe. . . . . 58
4.7 l'installation de services de domaine Active directory . . . . . 59
4.8 Fin d'installation de domaine Active Directory . . . . . 60
4.9 présentation des différents VLANs . . . . . 60
4.10 Nomination et adressage des VLANs . . . . . 61
4.11 Présentation de l'architecture réseau . . . . . 61
4.12 Création des différents vlans . . . . . 62
4.13 Vérification des différents vlans . . . . . 63
4.14 Configuration des interfaces des Vlans . . . . . 64
4.15 Attribution d'une adresse à l'interface fa0/0 . . . . . 64
4.16 Encapsulation des vlan . . . . . 65
4.17 Activation du routage . . . . . 66
4.18 Test de routage . . . . . 66
4.19 Activation du DHCP . . . . . 67
4.20 Création des pools d'adresses . . . . . 68
4.21 Création des pools d'adresses . . . . . 69
4.22 Exclusion des pools d'adresses . . . . . 69
4.23 Attribution automatique d'adresse IP . . . . . 70
4.24 Attribution automatique d'adresse IP . . . . . 70
4.25 Activer le modèle AAA . . . . . 71
4.26 L'authentification . . . . . 71
4.27 L'autorisation . . . . . 72
4.28 configuration de l'adresse IP de serveur RADIUS . . . . . 72
4.29 activation de protocole 802.1x au niveau de Client-RADIUS . . . . . 72
4.30 activation de protocole 802.1x sur le port de l'utilisateur . . . . . 73
4.31 Debug AAA . . . . . 73
4.32 Authentification RADIUS . . . . . 74
4.33 Authentification RADIUS . . . . . 75
4.34 Attribution d'une adresse statique au serveur . . . . . 76

4.35 Création de groupe IT . . . . . 77
4.36 Création d'un utilisateur . . . . . 78
4.37 introduction de mot de passe de utilisateur . . . . . 79
4.38 Permission d'accés au réseau . . . . . 80
4.39 Associer l'utilisateur atsi au groupe IT . . . . . 81
4.40 Selection de service "Network Policy Server" . . . . . 82
4.41 Console d'administration NPS . . . . . 83
4.42 Inscrire le serveur NPS dans le domaine . . . . . 84
4.43 Inscription du serveur NPS dans le domaine . . . . . 85
4.44 création de client RADIUS . . . . . 86
4.45 NPS pour les connexions 802.1x câblés et sans fil . . . . . 87
4.46 type de connexion 802.1X . . . . . 88
4.47 Vue d'ensemble de la stratégie . . . . . 88
4.48 Ajout de client RADIUS . . . . . 89
4.49 Spécification de groupe d'utilisateurs pour la connexion 802 .1x câblée 90
4.50 Conditions de stratégie réseau . . . . . 91
4.51 Choix de méthodes d'authentification . . . . . 91
4.52 Ajout d'un attribut spécifique au fournisseur . . . . . 92
4.53 Ajout d'attributs spécifique au fournisseur . . . . . 93
4.54 Ajout d'attributs . . . . . 94
4.55 Ajout d'un attribut spécifique au fournisseur . . . . . 95
4.56 Démarrage de service " Configuration automatique de réseau câblé" . 96
4.57 Sélection de méthode d'authentification " EAP-MSCHAP v2 " . . . . 97
4.58 l'ajout de la machine au domaine . . . . . 98
4.59 Membres de vlan IT . . . . . 99
4.60 Test d'authentification 802.1x . . . . . 100
4.61 Utilisateur n'appartenant pas au vlan IT . . . . . 101
4.62 Test d'authentification 802.1x . . . . . 102
4.63 Wireshark sous GNS3 . . . . . 103
4.64 Aalyse de transactions de l'authentification 802.1x . . . . . 103
4.65 Access-Request . . . . . 104
4.66 Access-Accept . . . . . 105
4.67 Activer le protocole SSH . . . . . 106
4.68 l'accès au switch avec un client SSH . . . . . 107
4.69 L'accès avec login et password . . . . . 107

4.70 l'accès au switch avec un client telnet . . . . . 108
4.71 L'accés avec Username et password . . . . . 109
4.72 L'accès avec Username et password . . . . . 109

# Glossaire

**AAA :** Authentication Authorization Accounting.

**CHAP :** Challenge Handshake Authentification Protocol.

**DHCP :** Dynamic Host Configuration Protocol.

**DNS :** Domain Name Server.

**DRH :**Direction de Ressources Humaines.

**EAP :**Extensible Authentication Protocol.

**EAP-MD5 :** Extensible Authentication Protocol Message Digest 5.

**EAPOL :** Extensible Authentication Protocol Over Lan.

**EAP-FAST :** Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling.

**EAP-TLS :** Extensible Authentication Protocol- Transport Layer Security.

**EAP-TTLS :** Extensible Authentication Protocol -Tunneled Transport Layer.

**ETCD :** Equipement Terminal de Circuit de Données.

**FAI :**Fournisseur d'Accés Internet.

**GNS3 :**Graphical Network System 3.

**IANA :** Internet Assigned Numbers Authority.

**ID :** Identifiant.

**IEEE :** Institute of Electrical and Electronics Engineers.

**IETF :** Internet Engineering Task Force.

**IGC :** Infrastructure de Gestion de Clés.

**IOS :** Internetwork Operating System.

**IP :** Internet Protocol.

**IT :** Informatique Technologie.

**LAN :** Local Area Network.

**LLC :** Logical Link Control.

**MAN :** Metropolitain Area Network.

**MAC :** Media Access Control.

**MD5 :** Message Digest 5.

**MS-CHAP :** Microsoft Challenge Handshake Authentification Protocol.

**MS-CHAPv2 :** Microsoft Challenge Handshake Authentification Protocol Version 2.

**MD2 :** Message Digest 2.

**MD4 :** Message Digest 4.

**MGT :** Management.

**NPS :** Network Policy Server.

**NetBIOS :** Network Basic Input Output System.

**NAS :** Network Access Server.

**OSI :** Open Systems Interconnexion.

**PAP :** Password Authentication Protocol).

**PPP :** Point to Point Protocol.

**PEAP :** Protected Extensible Authentication Protocol.

**PAE :** Port Access Entity.

**PKI :** Public Key Infrastructure.

**RADIUS :** Remote Access Dial In User Service.

**RFC :** Request For Comment.

**SI :** Système Informatique.

**SSH :** Secure shell.

**SP3 :** Service Pack 3.

**SYSVOL :**Système Volume.

**SHA-1 :** Secure Hash Algorithm 1.

**SHA-2 :** Secure Hash Algorithm 2.

**SQL :** Structured Query Language.

**TCP :** Transmission Control Protocol.

**TTLS :** Tunneled Transport Layer Security.

**UDP :** User Datagram Protocol.

**VLAN :** Virtual Local Area Network.

**VPN :** Virtuel Private Network.

**WAN :** Wide Area Network.

**WiFi :** Wireless Fidelity.

**WPA :** Wi-Fi Protected Access.

# Introduction générale

Avec l'évolution rapide de l'informatique et les systèmes de communication, le réseau des entreprises est devenu de plus en plus exposé à des éventuelles attaques menées par des intrus au système , la preuve lorsque un utilisateur essaye d'accéder aux services réseau dont il a besoin, il doit s'y connecter physiquement ou par une borne wifi, ce qui menace la sécurité de ressources matérielles et logicielles de l'entreprise, alors pour faire face à ces risques, l'administrateur réseau doit mettre en place des stratégies de sécurité performantes pour le contrôle des accès au réseau de son entreprise assurant à la fois : un niveau de sécurité élevé, une simplicité pour l'utilisateur et une fiabilité de services.

Notre objectif donc est de prévoir une solution d'authentification permettant de sécuriser l'accès des utilisateurs au réseau de l'entreprise CEVITAL de Bejaia.

Pour atteindre cet objectif, nous avons à notre disposition, plusieurs solutions d'authentification parmi lesquelles, on a choisi celle basée sur le protocole d'authentification RADIUS (Remote Access Dial In User Service) qui s'appuie à la fois sur le standard 802.1X et le protocole EAP (Extensible Authentication Protocol) , ainsi cette solution nécessite une combinaison de plusieurs outils, notamment un annuaire (Active Directory) pour contenir l'ensemble des utilisateurs, un serveur RADIUS intégré sous Windows server 2008 pour authentifier les utilisateurs.

Notre mémoire est articulé autour de quatres chapitres :

Le premier chapitre décrit les notions théoriques de base sur les réseaux et la sécurité informatiques qui nous introduit au domaine de l'authentification.

Le deuxième chapitre porte sur la présentation d'organisme d'accueil Cevital avec la problématique posée de son réseau ainsi la solution proposée pour la résoudre.

Le troisième chapitre traite l'étude de la solution proposée pour l'entreprise en se basant sur la présentation de protocole d'authentification RADIUS, ses principes son fonctionnement, ainsi les protocoles sur lesquels il est épaulé, tel que la norme 802.1X et le standard EAP.

Le quatrième chapitre est consacré à la mise en oeuvre de service d'authentification RADIUS pour le réseau de CEVITAL de Bejaia, il présente les différents moyens et outils déployés pour l'implémentation de cette solution (Windows server 2008, l'annuaire Active Directory, le simulateur GNS3,...), ainsi les étapes de configuration mises en place pour pouvoir tester l'authentification des utilisateurs par le mécanisme de sécurité retenu.

Enfin,notre travail se clôture par une conclusion générale, décrivant les éléments essentiels qui ont été développés dans ce mémoire, ainsi quelques perspectives pour ce projet.

# 1

# Généralités sur les réseaux et sécurité informatique

# Introduction

La nécessité de communication et du partage des informations en temps réel, impose aujourd'hui aux entreprises la mise en réseau de leurs équipements informatiques en vue d'améliorer leurs rendements, et quelque soit la taille de ce réseau, la sécurisation des données informatique doit être une véritable stratégie de l'entreprise. L'objectif de ce chapitre est de présenter quelques concepts de bases sur les réseaux informatiques et leurs sécurités, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de l'adressage IP, le routage, ainsi que la sécurité et ces objectifs.

## 1.1 Définition d'un réseau

Un réseau informatique, est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (équipements, programmes,...). Ces équipements peuvent être éloignés ou rapprochés. Suivant l'éloignement entre ces équipements, on distingue les réseaux suivants :

- **Le LAN** (Local Area Network) : il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue est Ethernet).
- **Le MAN**(Metropolitain Area Network) : les MAN interconnectent plusieurs LAN géographique proche (au maximum quelque dizaines de KM) à des débits importants(de 1 à 100 Mbits/s). Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits(en générale une fibre optique).
- **Le WAN**(Wide Area Network) : Un WAN interconnecte plusieurs LANs à travers de grandes distances géographiques(plus de 1000 kilomètres). Le plus connu des WAN est internet. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un noeud de réseau.

## 1.2 Modèle OSI

le modèle OSI(Open Systems Interconnexion) est l'interconnexion des systèmes ouverts,il décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau, il est organisé en 7 couches successives.[10]


**Figure 1.1 – Modèle OSI**

**L'architecture en 7 couches du modèle OSI**

Le modèle OSI est constitué de 7 couches successives. Chacune de ces 7 couches est spécialisée dans une tâche bien précise. Les données de l'ordinateur émetteur traversent chacune de ces 7 couches (de haut en bas) avant d'être transmises (sous la forme de trames) au support de communication, puis, arrivées à la destination.

- **Couche 7 Application** :cette couche comprend les programmes d'application avec leurs conventions d'échange et de coopération .C'est la seule couche qui s'occupe de la sémantique des données transférées .on y trouvera des protocoles spécifiques à certains types d'applications (par exemple : application bancaires, réservation de place, messagerie électronique, terminal virtuel, prises de commande,...)

- **Couche 6 Présentations** : ce niveau est responsable de la présentation des données sous un format (une syntaxe) lisible par l'application.

- **Couche 5 Session** : cette couche fournit une interface permettant de gérer la synchronisation de la communication entre processus distant.

- **Couche 4 Transport** : ce niveau est responsable du contrôle du transport de bout en bout. Elle fournit l'interface permettant à l'utilisateur de paramétrer

la qualité de l'acheminement des données. C'est le premier niveau permettant de gérer les erreurs dues au passage à travers plusieurs liens (réseaux). Elle fournit deux principaux types de service : avec connexion (circuit virtuel) ou sans connexion (paquets indépendants).

- **Couche 3 Réseau** : cette couche réalise l'interface utilisateur avec le réseau, et gère l'adressage et le transfert des données vers la machine destinataire à travers le ou les réseaux connectés.

- **Couche 2 Liaison de donnée** : cette couche est responsable de l'échange de blocs d'informations sur une ligne (détection, correction d'erreurs, adressage). Elle est subdivisée en deux sous-couches dans la norme IEEE 802(sous-couches MAC et LLC).

- **Couche 1 Physique** : cette couche définit les caractéristiques physiques des signaux et des supports utilisés pour l'interconnexion des systèmes. Elle est également responsable de l'activation du maintien, et de la désactivation des circuits de l'ETCD, ainsi que des signaux d'horloge.[9]

## 1.3 Le modèle Client/serveur

### 1.3.1 Notions de base

- **Client** :Processus demandant l'exécution d'une opération à un autre processus par envoi de message contenant le descriptif de l'opération à exécuter et attendant la réponse de cette opération par un message en retour.
- **Serveur** : processus accomplissant une opération sur demande d'un client, et lui transmettant le résultat.
- **Requête** :message transmis par un client à un serveur décrivant l'opération à exécuter pour le compte du client.
- **Réponse** : message transmis par un serveur à un client suite à l'exécution d'une opération, contenant le résultat de l'opération.

### 1.3.2 Définition

Un client/serveur est un modèle informatique basé sur le traitement distribué selon lequel un utilisateur lance un logiciel client à partir d'un ordinateur relié à un réseau déclenchant simultanément le lancement d'un logiciel serveur situé dans un autre ordinateur possédant les ressources souhaitées par l'utilisateur (client).[10]

### 1.3.3 Présentation de l'architecture Client/serveur

L'architecture client/serveur désigne un modèle de communication entre plusieurs ordinateurs d'un réseau qui distingue plusieurs postes clients qui contactent avec un serveur (une machine généralement très puissante en termes de capacités d'entrée/sortie) qui leurs fournit des services. Ces services sont des programmes fournissant des données telles que l'heur, des fichiers, une connexion... Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes.[10]

### 1.3.4 Fonctionnement d'un système Client /serveur

- Le client provoque le dialogue en émettant une requête vers le serveur grâce à son adresse IP et le port, qui désigne une demande de service particulier du serveur.
- Le serveur réalise ce service et renvoie le résultat au client.

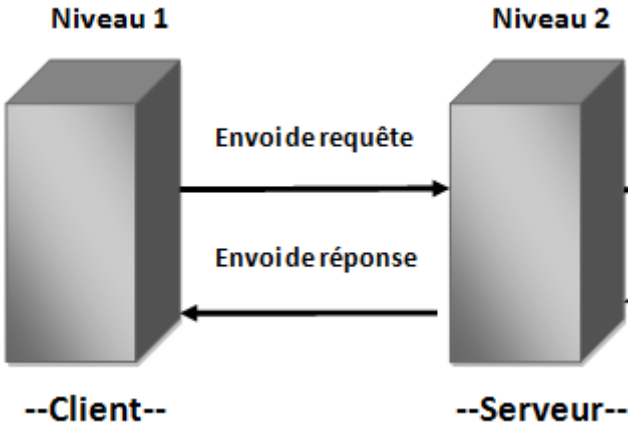


**FIGURE 1.2 – Modèle Client/Serveur**

## 1.4 Les attaques

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident. Ces événements seront appelés des " attaques ".[9]

Il existe quatre catégories principales d'attaques

- **L'accès**

  Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

- **La modification**

  Une attaque de type " modification " consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

- **Le déni de service**

  Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. Cette technique est assez simple à réaliser et jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.

- **La répudiation**

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

**Buts des attaques**

- **Interruption** : vise la disponibilité des informations.
- **Interception** : vise la confidentialité des informations.
- **Modification** : vise l'intégrité des informations.
- **Fabrication** : vise l'authenticité des informations.[9]

Comment se protéger contre ces attaques ?

## 1.5 La Sécurité informatique

### 1.5.1 Définition

La sécurité informatique est les mécanismes utilisés pour la protection de l'information contre les menaces et les attaques informatiques.

### 1.5.2 Notions sur la cryptographie

- **Chiffrement** : est la fonction qui consiste à transformer des données afin de les rendre incompréhensibles par un une entité.
- **Déchiffrement** : est l'opération inverse de chiffrement, consiste à rendre la donnée chiffrée compréhensible.
- **Cryptogramme (Texte chiffré)** : est le résultat de chiffrement d'une donnée.
- **Clé** :C'est le paramètre impliqué dans les opérations de chiffrement (respectivement de déchiffrement).
- **Cryptographie** :c'est la science qui permet de rendre inintelligible un message 'a ceux qui ne sont pas habilités a en prendre connaissance.

### 1.5.3 Les services de la sécurité informatique

- **La confidentialité**

  C'est la propriété qui permet de limiter la diffusion des données aux seules entités autorisées.

– **L'intégrité**

C'est le mécanisme qui permet d'assurer que les informations ne sont pas altérées lors de leur transmission entre les entités.

– **La non-répudiation**

Empêche l'expéditeur que le destinataire de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le récepteur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut montrer que le message a bien été reçu par le récepteur prétendu.

– **La disponibilité**

Cet objectif s'agit d'assurer l'accessibilité des entités authentifiées du système d'information aux ressources de ce système.

– **L'authentification**

C'est le moyen qui consiste à vérifier l'identité d'un utilisateur avant de lui donner l'accès à une ressource, Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a dotée. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

### 1.5.4 Outils et systèmes d'authentification

Authentifier des utilisateurs permet de vérifier l'identité des utilisateurs avant de leurs autoriser l'accès aux ressources d'une application, donc pour sécuriser l'accès à ses services, on doit mettre en place un système d'authentification qui est associés à un ou plusieurs annuaires et protocoles.

**1. Les annuaires**

**a. Définition**

Un annuaire est une base de données permettant d'offrir des services particuliers comme la sécurité d'accès aux données, la recherche, le classement et l'organisation des informations par certains critères simples et puissants pour faciliter la recherche, par exemple le critère d'index alphabétique pour la recherche des noms,...[1]

**b. Caractéristiques d'un annuaire**

- **L'aspect dynamique**

  Un annuaire électronique permet de gagner de temps lors de la recherche par rapport à un annuaire au format papier qui mis à jour une fois par ans, par contre l'annuaire électronique enregistre immédiatement toutes les modifications d'adresse, de numéro de téléphone, ainsi qu'il permet de déléguer les responsabilités de la mise à jour aux propriétaires mêmes des informations.
- **La flexibilité**

  La flexibilité des annuaires en ligne permet de rajouter un nouvelle donnée par exemple un numéro de téléphone mobile ou un numéro de téléphone sur IP (adresse IP) sans altérer les informations existantes pour le reste de l'annuaire.
- **La sécurité**

  Les annuaires en ligne permettent de contrôler les informations affichées en fonction de différents critères, comme l'identité de l'utilisateur ou simplement sa localisation géographique. Un mécanisme d'authentification, à l'aide d'un nom et d'un mot de passe par exemple, permet d'interdire l'accès à un sous-ensemble de l'annuaire ou à certains attributs, par exemple le numéro de téléphone personnel.
- **La personnalisation**

  En basant sur l'exemple des listes rouges, on peut dire que les annuaires traditionnels ne permettent pas de personnaliser le contenu. En effet, nous avons soit la possibilité d'apparaître pour tous dans l'annuaire, soit d'être en liste rouge et de n'apparaître pour personne, sans aucune alternative par contre les annuaires en ligne, il est possible de décider à quelles informations il a accès à partir de l'identité de l'utilisateur qui le consulte, mais aussi de ne lui montrer que ce qui l'intéresse en priorité et de reléguer sur un second plan le reste des informations.[1]

**c. Exemple d'annuaire**

L'annuaire LDAP (Light Wight Directory Access Protocol) né de la nécessaire adaptation du protocole DAP (protocole d'accès au service d'annuaire X500 de l'OSI) à l'environnement TCP/IP. Initialement frontal d'accès à des annuaires X500, LDAP est devenu en 1995, un annuaire natif, ce type d'annuaire permet de partager des bases d'informations sur le réseau interne ou externe. Ces bases peuvent contenir toute sorte d'information que ce soit

des coordonnées de personnes ou des données systèmes. [2]

**2. Définition d'un domaine Windows**

Un domaine est l'ensemble d'objets ordinateurs, utilisateurs et groupes définis par un administrateur réseau. Ces objets partagent une base de données d'annuaire, des stratégies de sécurité.[3]

**3. Les protocoles d'authentification**

**a. Le protocole PAP (Password Authentication Protocol)**

Le protocole PAP (Password Authentication Protocol) est un protocole d'authentification, utilisé avec le Protocole PPP(Point to Point Protocol), permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau.Après une phase de synchronisation entre le client et le serveur pour définir l'utilisation du Protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

- Le client envoie son nom PAP ainsi que son mot de passe en clair.
- Le serveur qui détient une table de noms d'utilisateurs et de mots de passe vérifie que le mot de passe correspond bien à l'utilisateur et valide ou rejette la connexion.[4]

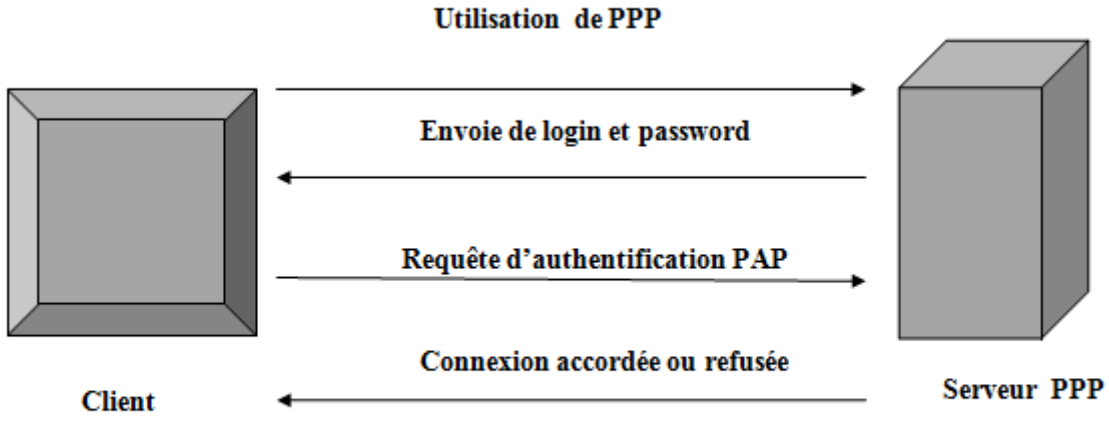


**Figure I.3 : les étapes d'authentification de protocole PAP**

**Figure 1.3 – les étapes d'authentification de protoccole PAP**

### b. Le protocole CHAP(Challenge Handshake Authentification Protocol)

CHAP (Challenge Handshake Authentification Protocol) est un protocole permettant une authentification sécurisée par hachage MD5 (Message Digest 5) d'où MD5 est une fonction de hachage cryptographique permettant d'obtenir l'empreinte numérique d'un message à partir de laquelle il est impossible de retrouver le message original. Ainsi, en envoyant l'empreinte du mot de passe au serveur, le client peut montrer qu'il connaît bien le mot de passe sans avoir à réellement l'envoyer sur le réseau .Après le même type de synchronisation que pour le Protocole PAP, le mécanisme d'authentification est basé sur un CHALLENGE en 3 étapes :

- Le serveur envoie au client un nombre aléatoire de 16bits ainsi qu'un compteur incrémenté à chaque envoi.
- Le client génère une empreinte MD5 de l'ensemble constitué reçu puis il envoie cette empreinte.
- Le serveur calcule également de son coté l'empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l'empreinte envoyée par le client. Si les deux empreintes sont identiques, le client est bien identifié et la connexion peut s'effectuer sinon, elle est rejetée.
- Le client génère une empreinte MD5 de l'ensemble constitué reçu puis il envoie cette empreinte.
- Le serveur calcule également de son coté l'empreinte MD5 grâce au mot de passe du client stocké localement puis il compare son résultat à l'empreinte envoyée par le client. Si les deux empreintes sonte identiques, le client est bien identifié et la connexion peut s'effectuer sinon, elle est rejetée.

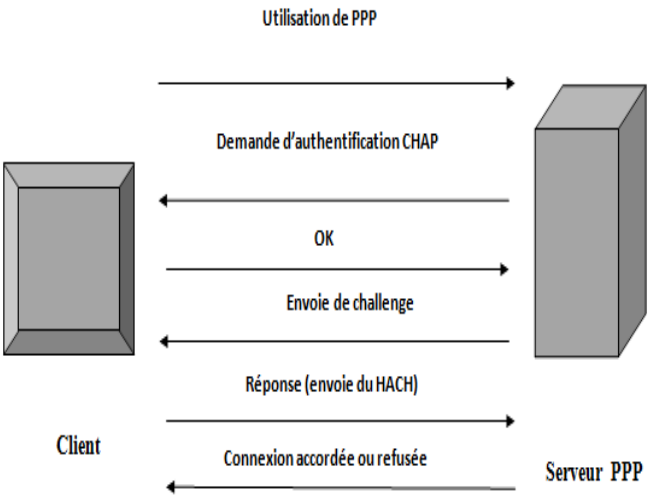


**FIGURE 1.4 – les étapes d'authentification de protoccole CHAP**

**c. Le protocole MS-CHAP(MicroSoft Challenge Handshake Authentification Protocol)**

MS-CHAP (Microsoft Challenge Handshake Authentification Protocol) est la version Microsoft de protocole CHAP. Plus qu'une simple version prioritaire, MS-CHAP apporte des améliorations à CHAP. Un des principaux inconvénients de CHAP est que le serveur doit détenir les mots de passe des utilisateurs en clair pour pouvoir vérifier l'empreinte MD5 envoyée par les clients, ce qui constitue une vulnérabilité potentielle en cas de compromission du serveur. Pour remédier à cette faiblesse, le Protocole MS-CHAP intègre une fonction de hachage propriétaire permettant de stocker sur le serveur un hash intermédiaire du mot de passe.

**d. Le protocole MS-CHAP v2(MicroSoft Challenge Handshake Authentification Protocol version 2)**

MS-CHAPv2 est un protocole d'authentification conçu par Microsoft, il est la deuxième version de protocole MS-CHAP, ce protocole a apporté des solutions pour deux principales faiblesses de MS-CHAP, la première le client ne puisse pas vérifier l'authentification du serveur sur lequel il veut se connecter

et la deuxième s'agit de la vulnérabilité de l'algorithme de hachage propriétaire à des attaques par brute-force. Voici le fonctionnement du processus d'authentification mutuelle fournit par MS-CHAP-v2 :

- Le serveur d'accès distant envoie une demande de vérification au client contenant une identification de session I et une chaîne C1 générée aléatoirement.
- Le client envoie alors une réponse contenant : son nom d'utilisateur, une chaîne aléatoire C2 et un hash de l'ensemble formé par la chaîne C1, l'identificateur de session I et son mot de passe.
- Le serveur vérifie la réponse du client et il renvoie une réponse contenant : une chaîne indiquant le succès ou l'échec de l'authentification, et un hash de l'ensemble formé par 3 éléments : la chaîne C2, l'identificateur de session I et son mot de passe.
- Le client vérifie à son tour la réponse d'authentification et établit la connexion en cas de réussite.[4][5]

### 1.5.5 Fonction de hachage

Une fonction de hachage date de la fin des années 1980 (algorithme MD2) mais l'idée est plus ancienne, c'est une méthode permettant de caractériser une information, une donnée dans le but de réduire sa taille. En effet la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de celles-ci, ce condensé est de taille fixe dont la valeur diffère suivant la fonction utilisée.

**Fonctions de hachage usuelles**

- **MD4 et MD5 (Message Digest)** :furent développées par Ron Rivest,MD5 produit des hachés de 128bits en travaillant les données originales par blocs de 512bits.
- **SHA-1(Secure Hash Algorithm 1)**,comme MD5,est base sur MD4.il fonctionne également à partir de blocs de 512bits de données,et produit par contre des condensés de 160bits en sortie.il nécessite donc plus de ressources que MD5.
- **SHA-2(Secure Hash Algorithm 2)** :est destiné à remplacer SHA-1 ,les différences principales résident dans les tailles de hachés possibles :256 ,384 ou 512 bits.
- **IPEMD-160(Ripe Message Digest)** :est la dernière version de l'algorithme RIPEMD.la version précédente produisait des condensés de 128bits mais présentait des failles de sécurité importantes.elle produit comme son nom l'indique

des condensés de 160bits

– **Tiger** :Tiger est une fonction de hachage cryptographique conçue par Ross Anderson et Eli Biham en 1996.Tiger fournit une empreinte sur 192bits mais des versions sur 128 et 160 bits existent aussi.[9]

### 1.5.6 Signature numérique

La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un message électronique autrement dit de prouver qu'un message provient bien d'un expéditeur donné,à l'instar d'une signature sur un document papier.son principe est par exemple que A veut signer numériquement un message destiné à B.pour ce faire ,A utilise sa clé privée pour chiffrer le message,puis il envoie le message accompagné de sa clé publique,étant donné que la clé publique de A est la seule clé qui puisse déchiffrer ce message,le déchiffrement constitue une vérification de signature numérique.[6]

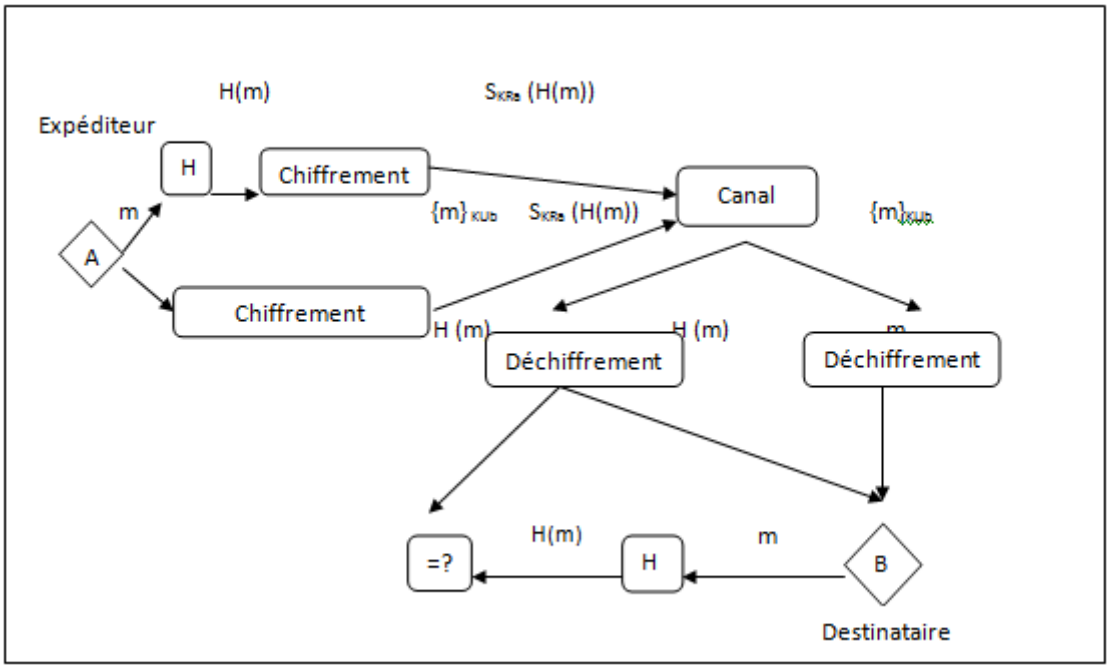


**Figure 1.5 – la signature numérique**

### 1.5.7 La politique de sécurité

**1. Définition**

Une politique de sécurité est l'ensemble de lois, de règles et de pratiques à suivre afin de protéger les informations sensibles et les ressources d'une organisation. Considérons un exemple simple : Une population d'une entreprise reçoit une habilitation de niveau confidentiel. Un ensemble de documents est également classé confidentiel. La politique de sécurité indique :
-l'ccès à des documents classés confidentiel n'est autorisé qu'aux personnels disposant d'une habilitation à ce niveau ou à un niveau supérieur ;
-la durée d'utilisation des documents classés de type confidentiel est enregistrée ; -les documents classés confidentiel sont uniquement accessibles en lecture seule ; -les documents classés confidentiel sont consultables à distance uniquement au travers d'un canal chiffré sur les réseaux de type LAN ou WAN.[7].
Cet exemple illustre la relation entre une population, une ressource, un niveau de confidentialité et la politique de sécurité.[7]

**2. Éléments d'une politique de sécurité**

**i. Structure de la politique de sécurité**

Les politiques de sécurité s'articulent généralement autour des six grandes sections suivantes :

- contexte ;
- objectifs ;
- respect de la politique ;
- portée ;
- principes directeurs ;
- rôles et responsabilités.

**ii. Les sections de la politique** Cette partie présente chacune des sections que l'on retrouve généralement dans une politique de sécurité.

**a. Section contexte**

- **Objectif de la section "contexte"**

L'objectif de cette première section est de positionner le contexte de la politique. La section, que l'on présente parfois sous l'appellation " préambule ", vise à identifier les éléments de haut niveau ayant donné naissance au besoin d'élaborer une politique.[8]

**b. Section "Objectifs"**

- **"Objectif de la section "Objectifs"**

  La section " Objectifs" a pour but d'exprimer les objectifs de l'établissement en matière de sécurité de l'information. Les objectifs de la politique doivent permettre au lecteur de rapidement saisir les intentions de l'établissement en matière de sécurité de l'information.

- **"Suggestion"**

  Certaines politiques présentent un objectif de très haut niveau sans l'accompagner de sous-objectifs plus précis, les objectifs de l'établissement en matière de sécurité de l'information sont :
  d'assurer la disponibilité, l'intégrité et la confidentialité à l'égard de l'utilisation des réseaux informatiques, du Réseau de télécommunication et d'Internet, de l'utilisation des actifs informationnels et de télécommunications, et des données corporatives ;
  d'assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs aux usagers et au personnel du réseau de l'établissement ;
  d'assurer la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations de l'établissement.

**c. Section "Respect de la politique "**

- **Objectif de la section**

  L'objectif de cette section est de préciser qui est responsable de l'application de la politique. La section indique aussi le processus disciplinaire en cas de non-respect de la politique.

**d. Section "Portée"**

- **Objectif de la section**

  La section " Portée " est très importante puisqu'elle définit le champ d'application de la politique. La portée comporte généralement trois dimensions, soit :

  les personnes visées par la politique ;

  les actifs visés par la politique ;

  les activités encadrées par la politique.

**e. Section "Principes directeurs "**

- **Objectif de la section**

  La section " Principes directeurs " est le cIJur de la politique. L'objectif de cette section est d'énoncer les grands principes que l'établissement se donne en matière de gestion de la sécurité de l'information.

- **Meilleures pratiques**

  Les principes directeurs sont des orientations de haut niveau qui permettront d'assurer les trois grands objectifs de la sécurité de l'information, soit :

  la disponibilité ;

  l'intégrité ;

  la confidentialité, incluant la protection des renseignements personnels.

**f. Section "Rôles et responsabilités"**

- **Objectif de la section**

  C'est dans cette section de la politique que les rôles et responsabilités de chacun des intervenants concernés sont définis.

- **Meilleures pratiques**

  Les rôles et responsabilités présentés dans la politique devraient être de niveau général et éviter les détails spécifiques qui s'apparentent à des tâches qui devraient être plutôt définies dans les procédures de sécurité.

### 1.5.8 Les outils de sécurité

Le système de sécurité d'une entreprise se construit à l'aide de nombreux outils complémentaires et techniques existant sur le marché. Un seul ne suffit pas : la sécurité est assurée par une utilisation correcte d'un ensemble d'outils à choisir, paramétrer et/ou développer en fonction de l'objectif de sécurité fixé.

**1. Encryption, signature électronique et certificats**

L'utilisation des techniques d'encryptions, de signature électronique et des certificats sont la base d'un commerce électronique sécurisé :

- **L'encryption**

  Elle consiste à transformer les informations électroniques au moyen d'un algorithme mathématique afin de les rendre inintelligibles, sauf pour celui qui

possède le moyen (une clé) de les décoder. L'encryption des informations qui transitent par le réseau est utilisée pour assurer la confidentialité, l'intégrité et l'authenticité des transactions et du courrier électronique. A titre d'exemple, le logiciel d'encryption gratuit Pretty Good Privacy (PGP) est très largement employé pour protéger le courrier électronique ;

- **La signature électronique**
  c'est un code digital (une réduction du document électronique à envoyer) qui, associé aux techniques d'encryption, garantit l'identité de la personne qui émet le message et assure la non-répudiation et l'intégrité de l'envoi ;

- **Le certificat** document électronique (carte d'identité) émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique d'encryption et fournit des informations de gestion complémentaires sur le certificat et le détenteur.

2. **L'authentification et l'autorisation**
   - **Une personne peut être authentifiée par la combinaison d'une identification et d'un mot de passe (code secret personnel)**
     Le mot de passe doit posséder certaines caractéristiques : non trivial, difficile à deviner, régulièrement modifié, secret, etc. Des outils logiciel ou hardware de génération de mots de passe existent.

   - **L'authentification précède généralement l'autorisation**
     L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser et dans quelle mesure (par exemple consulter ou mettre à jour des données). Les techniques d'encryption et de certificats utilisés conjointement à celle des mots de passe ajoutent un très haut degré de sécurité dans le domaine de l'authentification des utilisateurs.

# 1.6 Les VLAN(Virual Local Area Network)

## 1.6.1 Présentation de VLAN

Un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel(logique) permet de regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources ,appartenance à un département, etc.),sans les contraintes physiques (câblage informatique inapproprié,etc.).

## 1.6.2 Types de VLAN

Il existe quatre types de VLAN :

**1. Les Vlan par port (Vlan de niveau 1)**

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Si on déplace physiquement une station il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si on déplace logiquement une station (on veut la changer de Vlan) il faut modifier l'affectation du port au Vlan.[10]

**2. Les Vlan par adresse MAC (Vlan de niveau 2)**

On affecte chaque adresse MAC à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables).Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

**3. Les Vlan par adresse de Niveau 3 (VLAN de niveau 3)**

On affecte une adresse de niveau 3 à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient (le commutateur doit donc accéder à ces informations).En fait, il s'agit à partir de l'association adresse niveau 3/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2.

**4. Les vlan par protocole de niveau 3**

Les VLAN se font de deux manières :

- **Attribution statique (niveau 1)**
  C'est la méthode la plus simple et aussi la moins souple, qui consiste à attribuer un port du SWITCH à un VLAN donné, en configurant statiquement le SWITCH.

- **Attribution dynamique (niveaux $>$ 1)**
  C'est la méthode qui fait appel à 802.1x et à un procédé d'authentification (serveur d'authentification RADIUS). Il faut disposer d'un switch capable d'envoyer à un serveur d'authentification l'adresse MAC de la station connectée à un port, en guise de "login/password". Si l'adresse MAC est connue (Authentification réussie), le serveur pourra envoyer au SWITCH le numéro du VLAN attaché à la station.
  Cette méthode est plus souple, puisqu'une station donnée pourra se connecter sur n'importe quel port, elle se retrouvera toujours sur le VLAN qui lui convient.

**Fonctionnement des ports**

Il existe trois modes d'accès au port :

**Mode d'accès** ;

**Mode trunk** (étiquetage de trame) ;

**Mode dynamique ou automatique** .[10]

### 1.6.3 Les avantages de VLAN

- support des transferts de données allant jusqu'à 1Gb=s ;
- peut couvrir un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large ;
- une station peut appartenir au plusieurs VLAN simultanément.
- Flexibilité de la segmentation du réseau (dynamique).
- Simplification de la gestion du réseau : l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement sans devoir manipuler les connexions physiques dans un local technique.
- Augmentation des performances du réseau : trafic réseau segmenté, limitation des broadcast.
- renforcement de la sécurité du réseau : les frontières (virtuelles) entre les VLAN ne peuvent être franchies que par le biais d'un routage.

## Conclusion

Dans ce chapitre,on a présenté les concepts de base sur les réseaux et la sécurité informatiques,notamment la notion basique de l'authentification,les mécanismes de protection et quelques protocoles de sécurité qui nous permet de bien analyser notre sujet.le chapitre suivant va être consacré à la présentation de l'organisme d'acceuil.

# 2

# Présentation de l'organisme d'acceuil

# Introduction

Effectuer un stage au sein de l'entreprise CEVITAL est une réussite sur le plan pratique et professionnel, vu que cette entreprise est considérée parmi les plus grandes entreprises de l'Algérie, dans son secteur. Le souci permanent des responsables de production est de fournir à leurs clients un produit de qualité irréprochable. Nous sommes conscients que les connaissances théoriques à elle seules ne suffisent pas pour faire face aux problèmes réels au sein des entreprises industrielles. Dans ce cadre Cevital nous a invités à effectuer un stage de perfectionnement car c'est une occasion exceptionnelle pour développer nos connaissances et c'est aussi un complément de formation au niveau de leur future vie professionnelle. Dans ce chapitre nous allons représenter l'état actuel de l'entreprise CEVITAL, trouver les insuffisances, puis créer des solutions qui résolvent les anomalies trouvées.

## 2.1 Présentation de l'organisme d'acceuil

CEVITAL c'est un ensemble industriel intégré, concentré en première partie dans le secteur de l'agro-alimentaire, raffinage d'huile et de sucre, produits dérivés, négoce de céréales, distribution de produits destinés à l'alimentation humaine et animale. L'ensemble industriel a connu une croissance importante et a consolidé sa position de Leader dans le domaine agro-alimentaire et entend poursuivre sa croissance et exploiter les synergies en poussant l'intégration des activités agro-alimentaires et en développant des activités dans le secteur à fort potentiel de croissance du verre plat.

- elle s'est taillée en 7 ans, une part de marché dominante sur le marché algérien des produits alimentaires de base.
- Son organisation et sa structure de coûts lui permettent d'envisager devenir un joueur compétitif sur le marché régional des produits alimentaires de base. L'envergure de ses activités et la capacité de gestion de ses dirigeants lui permettent d'envisager répliquer le succès industriel qu'elle a connu dans le domaine agro-alimentaire en développant des activités industrielles dans la production de panneaux préfabriqués et de verre plat

## 2.2 Organigramme de l'entreprise

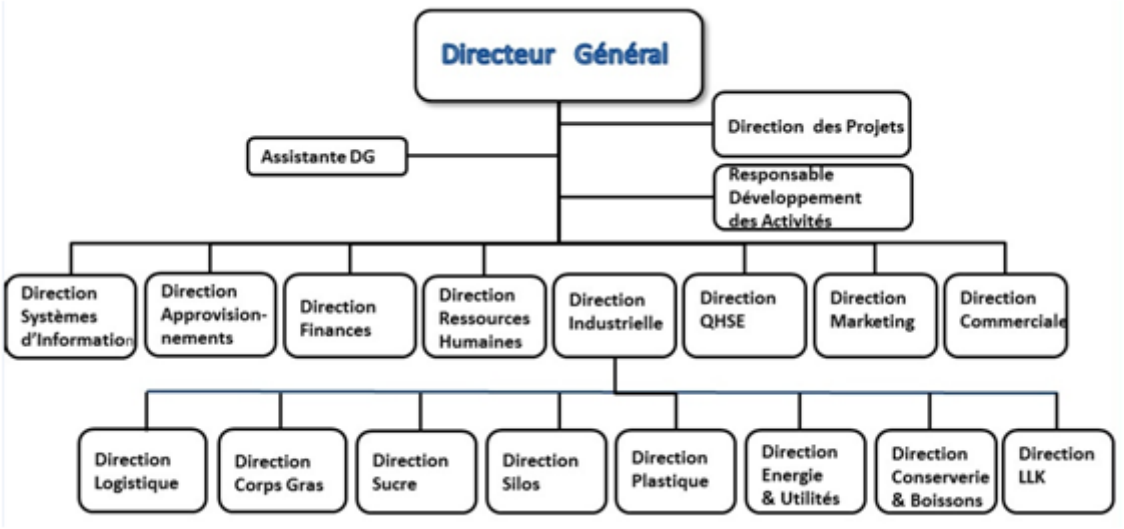


**Figure 2.1 – Plan de masse du complexe CEVITAL**

1. **La direction des Finances**

   Le rôle de cette direction est de préparer et mettre à jour les budgets, tenir la comptabilité et préparer les états comptables et financiers selon les normes et pratiquer le contrôle de gestion.

2. **La direction commerciale**

   Elle a en charge de commercialiser toutes les gammes des produits et le développement du Fichier clients de l'entreprise, au moyen d'actions de détection ou de promotion de projets à base de hautes technologies. En relation directe avec la clientèle, elle possède des qualités relationnelles pour susciter l'intérêt des prospects.

3. **La direction des Ressources Humaines**

   Cette direction a pour rôle de définir et proposer à la direction générale les principes de Gestion ressources humaines en support avec les objectifs du busi-

ness. Elle assure le recrutement et la gestion des carrières. Elle se charge de la formation du personnel et participe avec la direction générale à l'élaboration de la politique de communication afin de développer l'adhésion du personnel aux objectifs fixés par l'organisation.

4. **La direction Système d'informations :**
   - Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise.
   - Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mis à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité.
   - Elle définit, également, dans le cadre des plans pluriannuels les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

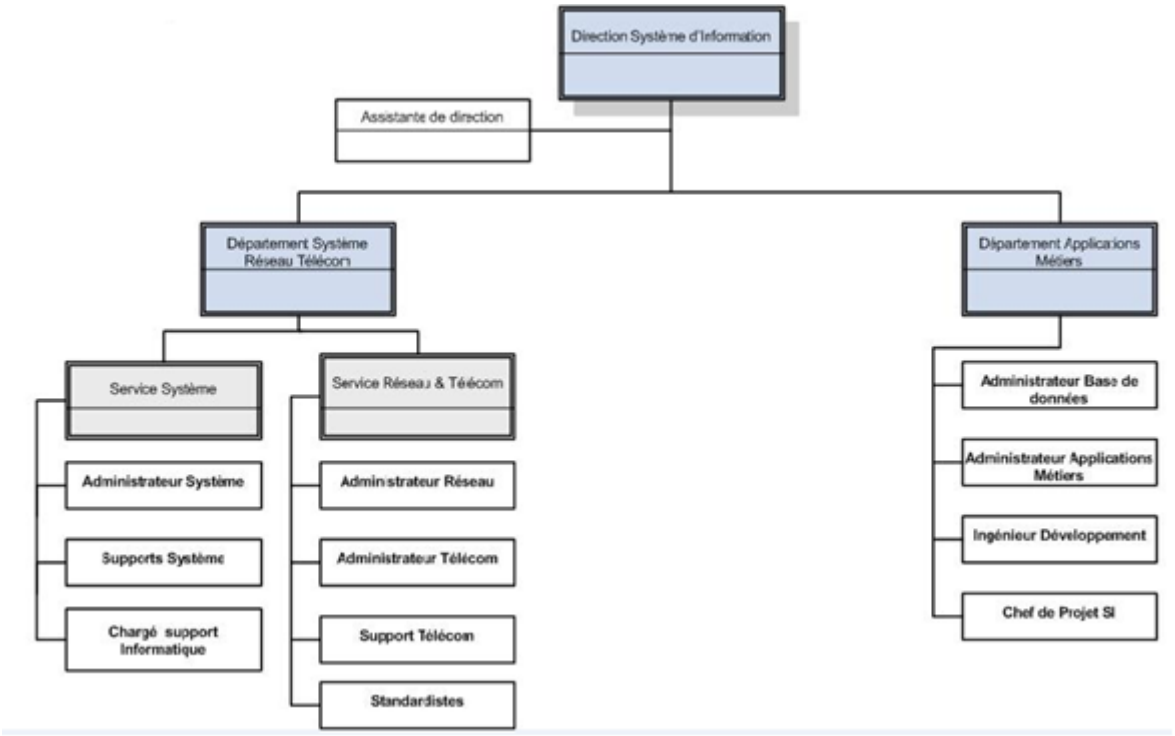


**Figure 2.2 – La direction Système d'informations**

## 2.3 Activités de CEVITAL

Lancé en Mai 1998, le complexe CEVITAL a débuté son activité par le conditionnement d'huile en Décembre 1998. En Février1999, les travaux de génie civil de la raffinerie ont débuté, elle est devenue fonctionnelle en Août 1999. L'ensemble des activités de CEVITAL est concentré sur la production et la commercialisation des huiles végétales, de margarine et de sucre, ainsi que la production de l'énergie électrique qu'elle est en cours d'études, elles se présentent comme suit :

- Raffinage des huiles (1800 tonnes/jour) ;
- Conditionnement d'huile (1400 tonnes/heure) ;
- Production de margarine (600tonnes/jour) ;
- Fabrication d'emballage (PET) : Poly-Ethylène-Téréphtalate (9600unités/heur) ;
- Raffinage du sucre (1600 tonnes/jour) et (3000 tonnes /jour) ;
- Stockage des céréales (120000 tonnes) ;
- Minoterie et savonnerie en cours d'étude ;
- Cogénération (production de l'énergie électrique avec une capacité de 64MW et de la vapeur).

Aujourd'hui, cevital spa offre des produits de qualité supérieure à des prix compétitifs, grâce à son savoir faire, ses unités de production ultramodernes, son contrôle stricte de qualité et son réseau de distribution performant.

## 2.4 Mission et objectifs

CEVITAL dispose d'un réseau commuté de taille importante composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements : 40 Switchs d'accès, 3 routeurs et un Firewall, pour la plupart de marque Cisco.

La gestion du réseau est à la charge de la direction informatique qui doit veiller à son bon fonctionnement, cependant l'augmentation continuelle de sa taille, devient de plus en plus, à la fois difficile à maintenir dans un état de marche tout en le préservant des aléas Externes qui peuvent nuire à sa sécurité. Cet état de fait est dû à la méthode de travail adoptée par la direction pour mener à bien cette mission et qui se base principalement sur un mode de gestion entièrement manuelle.

## 2.5 Architecture actuelle du réseau LAN de CEVITAL de Bejaia

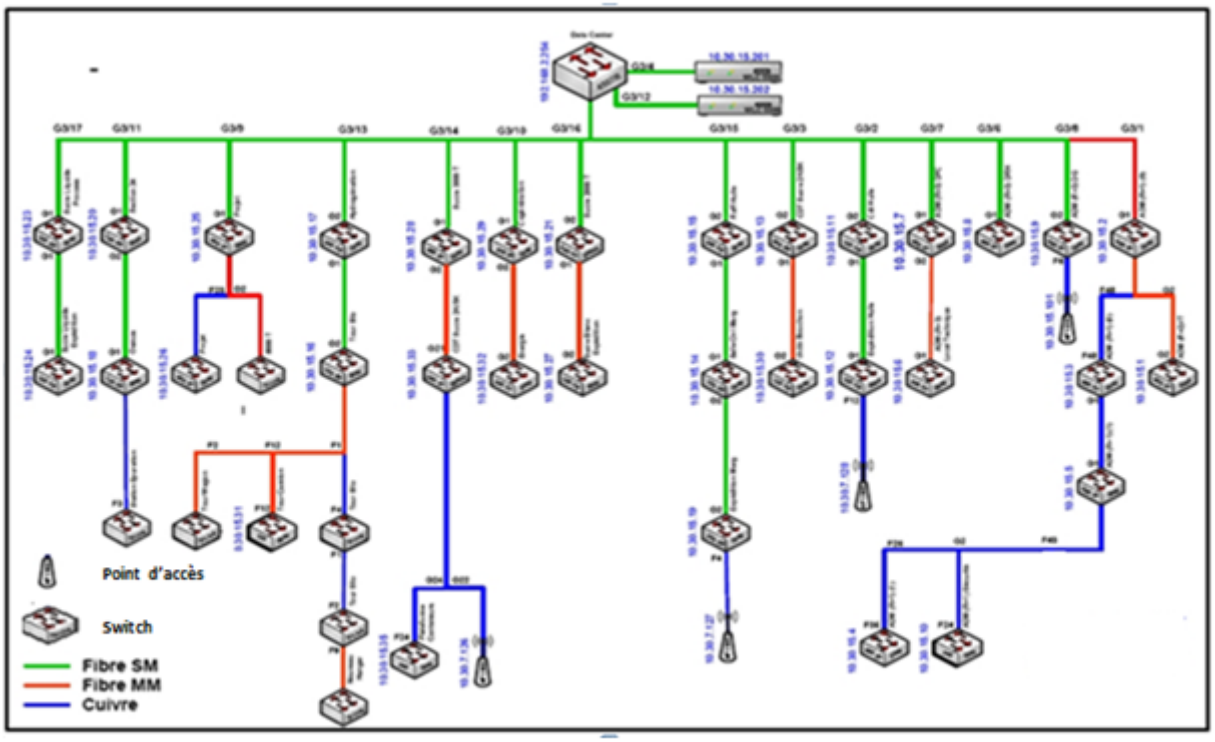


**FIGURE 2.3 – Architecture actuelle du réseau LAN de CEVITAL de Bejaia**

## 2.6 Problématique

CEVITAL dispose d'un réseau commuté de taille importante composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements : 40 Switch d'accès, 3 routeurs et un Firewall, pour la plupart de marque Cisco. La gestion du réseau est à la charge de la direction informatique qui devient veiller à son bon fonctionnement, cependant l'augmentation continuelle de sa taille, devient de plus en plus, à la fois difficile à maintenir dans un état de marche tout en le préservant des aléas externes qui peuvent nuire à sa sécurité. Cet état de fait est dû à la méthode de travail adoptée par la direction pour mener à bien cette mission et qui se base principalement sur un mode de gestion

entièrement manuelle. Le système est très vulnérable du fait qui ne dispose pas d'un système d'authentification interne adéquat, ce qu'il le rend accessible sans aucun contrôle.

## 2.7 Solutions proposée

L'objectif principal de notre étude est la mise en oeuvre d'une solution d'authentification permettant de sécuriser l'accessibilité aux services réseau de Cevital. Cette authentification des utilisateurs qu'elle soit interne ou externe au cercle de confiance est indispensable.

L'implémentation du service d'authentification RADIUS, le stockage des utilisateurs dans un annuaire Active Directory et la mise en place du standard 802.1x sur certains équipements de l'infrastructure répond aux besoins de l'entreprise Cevital.

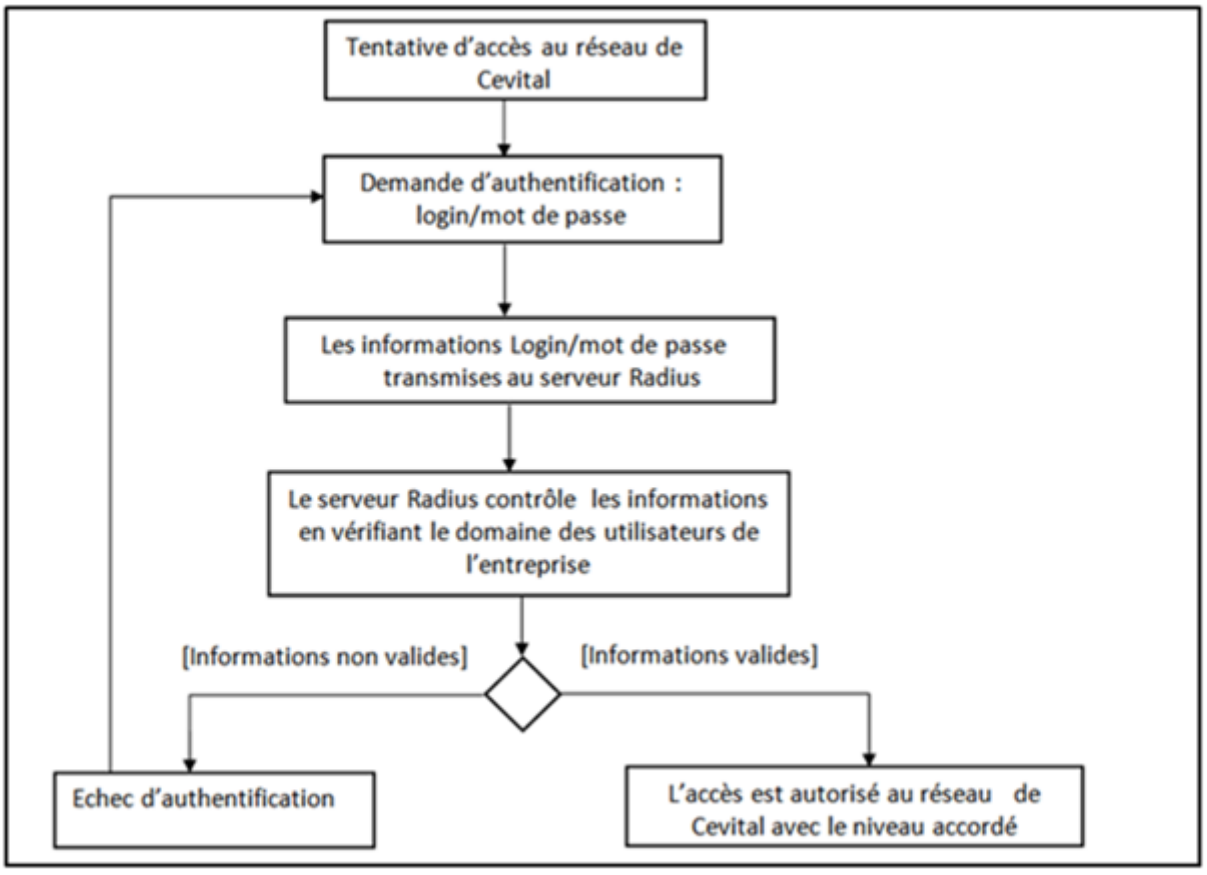


**Figure 2.4 – Schéma global de la solution proposée**

# Conclusion

Une bonne étude de l'existant et de l'état des lieux, permettra de mieux s'approfondir dans son projet et de bien étudier sa problématique, en prenant compte l'étude des solutions qui porteront vraiment un plus au cas présenté.

# 3

# Etude des solutions proposées

# Introduction

Lorsque l'on doit assurer le bon fonctionnement d'un réseau qui dépasse les dimensions du réseau familial, il devient nécessaire de s'assurer que le danger ne vient pas de l'intérieur. Avec la prolifération des ordinateurs personnels portables, le risque de voir une machine inconnue venir polluer le réseau de l'intérieur doit être pris au sérieux.

Ce chapitre a pour but d'apporter quelques ébauches de solutions à tous ces problèmes.Nous ferons appel aux VLANs pour le réseau câblé, à la norme 802.1x, en mettant en oeuvre une solution d'authentification autour de serveurs Radius.

## 3.1 Expression de la politique de sécurité

Le but de cette mise en place est de placer l'utilisateur non identifié, en gros un prestataire externe à l'entreprise, dans un sous-réseau différent (Vlan)pour qu'il ne puisse avoir qu'un accès restreint au réseau.

- Lorsque un utilisateur est identifié, c'est-à-dire qu'il est connecté avec un compte utilisateur du domaine ou sur un ordinateur du domaine, il est envoyé dans le VLAN Users (Production, DRH, Commercial).
- Si l'utilisateur, en plus d'être identifié, appartient au pôle informatique, alors il est envoyé dans le VLAN IT.
- Enfin, si l'utilisateur n'est pas identifié par le serveur radius ou que le switch n'arrive pas à communiquer avec le serveur alors il est envoyé dans le VLAN Guest. ( Les utilisateurs connectés sur le VLAN Guest n'auront qu'un simple accès à Internet et la possibilité d'imprimer sur les imprimantes disponibles du réseau).

## 3.2 Les équipements réseau

L'élément pivot de tout le dispositif est l'équipement réseau, c'est-à-dire le commutateur ou la borne sans fil. Dans la terminologie Radius, ces équipements sont appelés NAS (Network Access Server),ils sont aussi nommés clients Radius puisque ce sont eux qui soumettent des requêtes au serveur.

Avec 802.1X, ils sont appelés authenticators. Ils doivent impérativement supporter au moins les standards suivants :

- les protocoles IEEE(Institute of electrical and electronics engineers) 802.1x , et EAP(Extention authentication protocol)
- le protocole Radius(Remote Access Dial In User Service)

De plus, si l'utilisation des réseaux virtuels est souhaitée, les NAS devront être compatibles avec le protocole IEEE 802.1Q qui définit les critères d'utilisation des réseaux virtuels, appelés VLAN du démarrage, ou au moment de la connexion d'un utilisateur.

## 3.3 Le protocole RADIUS

### 3.3.1 Historique

Le protocole RADIUS a été créé par Livingston,il est développé en trois étapes présentées comme suit :

- Janvier 1997 : Première version de RADIUS décrite dans RFC 2058(authentication) et 2059 (accounting).
- Avril 1997 : Deuxième version de RADIUS décrite dans RFC 2138 (authentication) et 2139 (accounting).
- Juin 2000 : La dernière version de RADIUS décrite dans RFC 2865 (authentication) et 2866 (accounting).[11]

### 3.3.2 Présentation de protocole RADIUS

RADIUS avait tout d'abord pour objet de répondre aux problèmes d'authentification pour des accès distants, par liaison téléphonique, vers les réseaux des fournisseurs d'accès ou des entreprises. C'est de là qu'il tient son nom qui signifie Remote Access Dial In User Service. Au fil du temps, il a été enrichi et aujourd'hui il peut être utilisé pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil. Le protocole RADIUS est décrit dans la RFC 2865 de l'IETF (Internet Engineering Task Force).

RADIUS est un système client/serveur qui permet de sécuriser des réseaux contre des accès à distance non authorisés.il répond au modèle AAA résumant ses trois fonctions comme suit :

A = Authentication : authentifier l'identité du client ;
A = Authorization : accorder des droits au client ;
A = Accounting : enregistrer les données de comptabilité de l'usage du réseau par le client. [12]

### 3.3.3 Rôles de protocole RADIUS

- Authentifier les machines/utilisateurs pour l'accès au réseau local.
- Utilisable en filaire et sans-fil.
- Placer les machines dans des sous-réseaux virtuels.
- Plusieurs moyens d'authentification.
- Initialiser les algorithmes de chiffrement des communications (WPA).
- Les communications WiFi peuvent être sécurisées.
- Radius est un élément actif du réseau, pas seulement une base de donnée.
- Interfaçage avec des logiciels de portails captifs.
- Authentification distante par redirection de requêtes (proxy).
- Utilisable par d'autres types de serveurs (VPN).

### 3.3.4 Principes de protocole RADIUS

- RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.), et sur un client RADIUS, appelé NAS , faisant office d'intermédiaire entre l'utilisateur final et le serveur.
- L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré par la clé (secret) partagée afin de renforcer la sécurité et garantir l'intégrité de ces transactions.
- Le serveur RADIUS peut faire office de proxy en transmettant les requêtes du client à d'autres serveurs RADIUS.
- Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine.
- Protocole de prédilection des fournisseurs d'accès à internet : relativement standard, propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

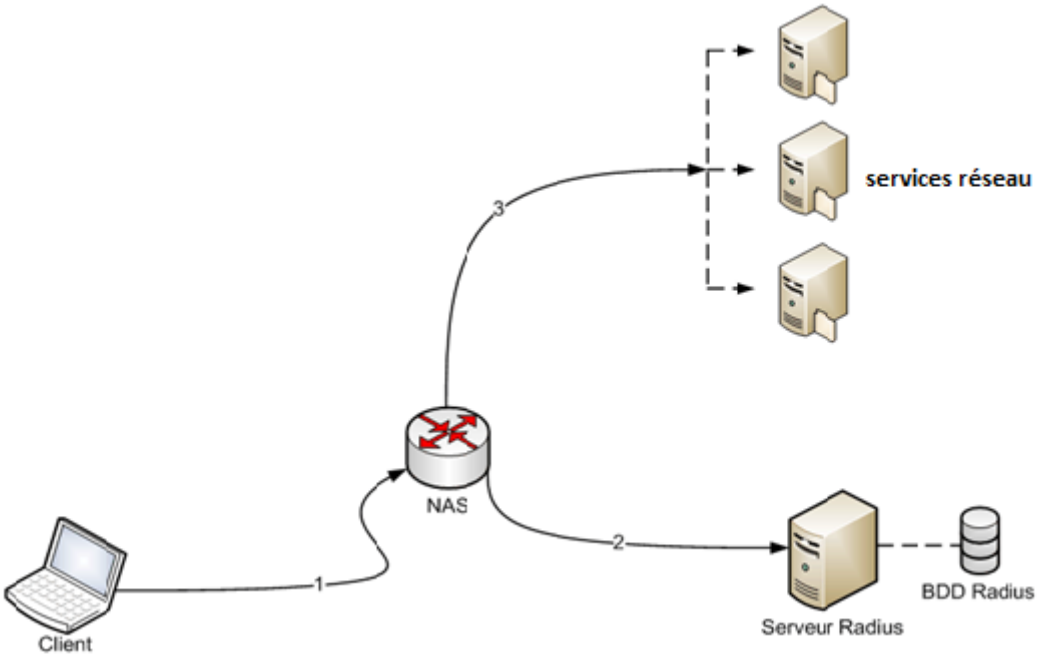


FIGURE 3.1 – principe de protocole RADIUS

### 3.3.5 Eléments d'authentification RADIUS

– **Authentification avec l'adresse Ethernet (adresse MAC)**

L'adresse MAC de la carte Ethernet du poste de travail identifie ce dernier. Cette adresse MAC n'est pas une preuve absolue d'identité puisqu'il est relativement facile de la modifier et d'usurper l'identité d'un autre poste de travail. Néanmoins, sur un réseau filaire, cette adresse peut être suffisante puisque, pour tromper le système d'authentification, il faudra tout de même pénétrer sur le site, connaître une adresse MAC valide et réussir à s'en servir. Même si on peut imaginer qu'une personne décidée peut y arriver, cette solution est suffisante si on considère qu'il s'agit là d'une première barrière. En revanche, si on souhaite une authentification très forte il faudra utiliser une autre méthode, à savoir 802.1X et EAP. Dans le cas du sans-fil, l'authentification par adresse MAC fonctionne également mais elle est fortement déconseillée comme unique moyen. En effet, même si on met en place un chiffrement fort des communications, l'adresse MAC circule toujours en clair. Or, le problème du sans-fil est que le périmètre du réseau est flou et incontrôlable. Par conséquent, n'importe qui, écoutant ce réseau, même sans accès physique, peut capter des adresses

MAC et s'en servir très facilement ensuite pour s'authentifier. Cet inconvénient est moindre en filaire car le périmètre est complètement déterminé et une présence physique dans les locaux est nécessaire. Ce type d'authentification est appelé Radius-MAC ou encore MAC-based.

– **Authentification par certificat électronique X509**

Ce type d'authentification consiste à faire présenter par le client un certificat électronique dont la validité pourra être vérifiée par le serveur.Il peut s'agir d'un certificat appartenant à un utilisateur. Dans ce cas on parlera d'authentification par utilisateur. Mais il peut également s'agir d'un certificat machine qui sera alors lié à la machine. L'usage des certificats implique l'existence d'une IGC (Infrastructure de gestion de clés, ou PKI en anglais, pour Public Key Infrastructure).

– **Authentification RADIUS par identifiant et mot de passe**

Ce type d'authentification correspond plutôt à une authentification par utilisateur et suppose qu'il existe quelque part une base de données qui puisse être interrogée par le serveur. Plusieurs protocoles peuvent être mis en oeuvre pour assurer une authentification par identifiant et mot de passe. Cependant, il convient d'éliminer ceux pour lesquels le mot de passe circule en clair sur le réseau ou bien est stocké en clair dans la base de données. Le protocole 802.1X nous permettra de mettre en oeuvre des solutions (EAP/PEAP ou EAP/TTLS) qui permettront de résoudre ces problèmes. Comme les utilisateurs sont déjà confrontés à la nécessité de posséder de multiples mots de passe pour de multiples applications, il sera intéressant de réutiliser une base existante comme un domaine Windows ou une base LDAP.

Dans notre cas, nous avons choisit l'authentification RADIUS 802.1x par identifiant et mot de passe

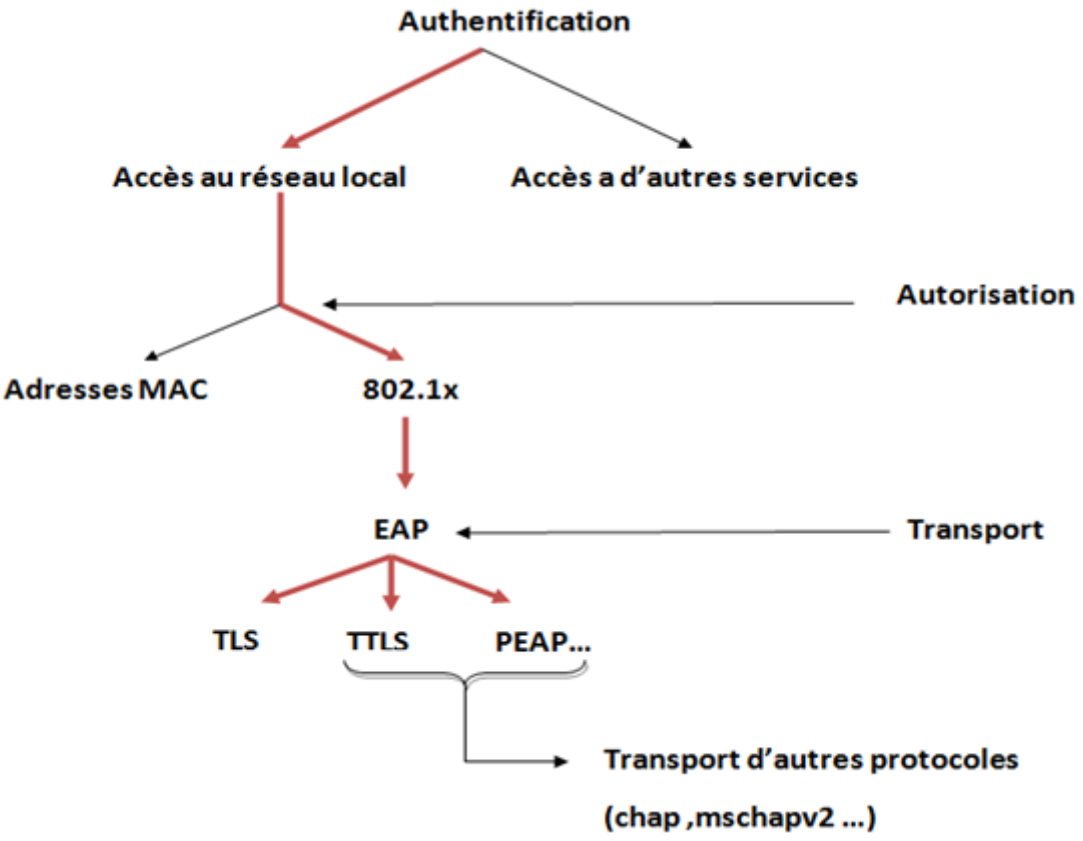


FIGURE 3.2 – L'authentification Radius

| Type d'authentification | Emetteur de l'identifiant | Protocole |
|---|---|---|
| Adresse MAC | L'équipement réseau | RADIUS |
| Login/Password<br>Certificat | Le poste utilisateur (supplicant) | RADIUS + 802.1x + EAP |

FIGURE 3.3 – L'identifiant

### 3.3.6 Le fonctionnement de protocole RADIUS

1. **L'authentification RADIUS**

   Le NAS reçoit une requête pour une connexion à distance, envoie une demande d'authentification au serveur radius. Si l'utilisateur est accepté, le serveur radius autorise et détermine les services que l'utilisateur peut accéder et ainsi que des paramètres de connections.

   Explications détaillées :

   – L'utilisateur entre le nom d'utilisateur et le mot de passe.

   – Le nom d'utilisateur et le mot de passe encrypté sont envoyés au travers du réseau (réseaux telecom,..) au serveur radius

   – L'utilisateur reçoit l'une des réponses suivantes :

   **ACCEPT :** l'identification de l'utilisateur a réussi.

   **REJECT :** l'identification a échoué.

   **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur.

Une autre réponse est possible : CHANGE PASSWORD où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe. Change-password est un attribut VSA (Vendor-Specific Attributes), c'est-à-dire qu'il est spécifique à un fournisseur.

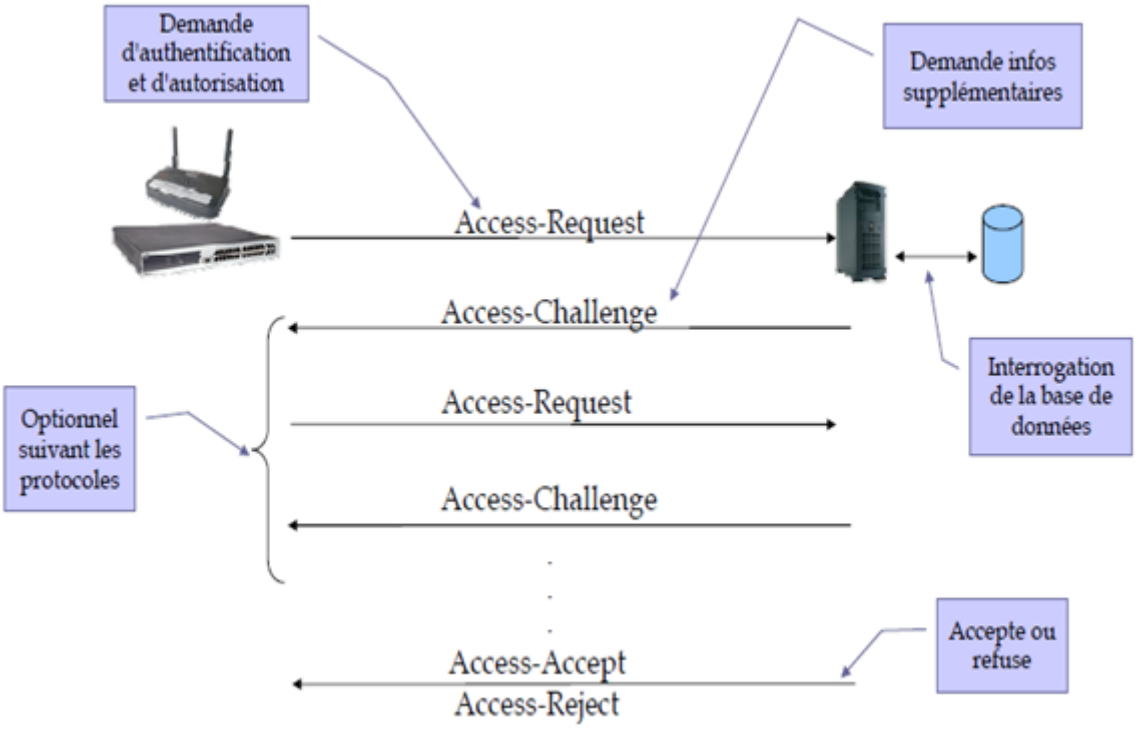


FIGURE 3.4 – fonctionnement de protocole RADIUS

**A. Les différents types de paquets RADIUS**

- **Access-Request :**la conversation commence toujours par un paquet Access-Request émis par le NAS(client RADIUS) vers le serveur RADIUS. Il contient au moins l'attribut User-Name et une liste d'autres attributs tels que Calling-Station-Id, Nas-Identifier, etc.

- **Access-Challenge :** après réception d'un paquet Access-Request, le serveur peut renvoyer un paquet Access-Challenge qui a pour but de demander d'autres informations et de provoquer l'émission d'un nouveau paquet Access-Request :par le NAS. Access-Challenge sera toujours utilisé avec EAP puisqu'il permettra au serveur de demander un certificat ou un mot de passe au poste de travail.
- **Access-Accept :** Ce paquet est renvoyé au NAS par le serveur Radius si l'authentification transmise par l'Access-Request a été correctement validée.

Ce paquet contient alors des attributs qui spécifient au NAS les autorisations accordées par le serveur.

– **Access-Reject :** nvoyé par le serveur Radius au NAS si l'authentification a échoué.

**B. Format générale des paquets RADIUS**

Radius utilise quatre types de paquets pour assurer les transactions d'authentification.Tous les paquets ont le format général indiqué par la figure suivante :

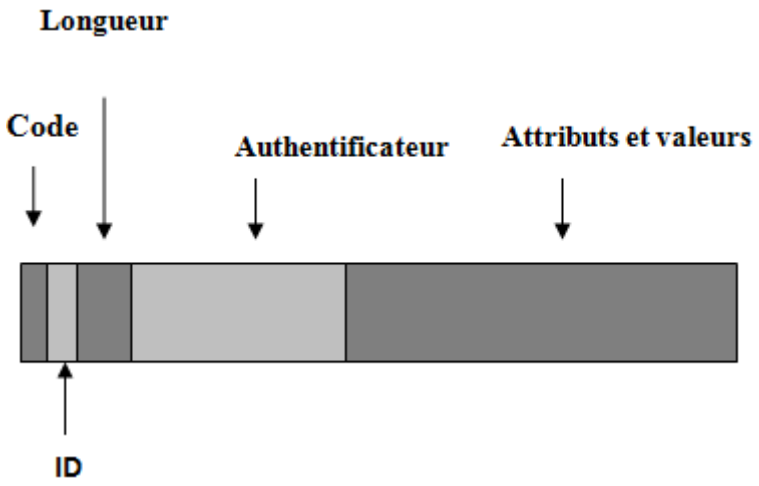


FIGURE 3.5 – Format des paquets RADIUS

– **Code :** Ce champ d'un seul octet contient une valeur qui identifie le type du paquet. La RFC 3575 (IANA considerations for Radius) définit 255 types de paquets. Par chance, quatre d'entre eux seront suffisants pour les problèmes qui nous préoccupent ici. Il s'agit de :
Access-Request (code=1) ;
Access-Accept (code=2) ;
Access-Reject (code=3) ;
Access-Challenge (code=11).

– **ID :** Ce champ, d'un seul octet, contient une valeur permettant au client Radius d'associer les requêtes et les réponses.

– Longueur : Champ de seize octets contenant la longueur totale du paquet.

- **L'authentificateur :** Ce champ de seize octets a pour but de vérifier l'intégrité des paquets. On distingue l'authentificateur de requête et l'authentificateur de réponse. Le premier est inclus dans les paquets de type Access-Request ou Accounting-Request envoyés par les NAS. Sa valeur est calculée de façon aléatoire. Et l'authentificateur de réponse est présent dans les paquets de réponse de type Access-Accept, Access-Challenge ou Access-Reject. Sa valeur est calculée par le serveur à partir d'une formule de hachage MD5 sur une chaîne de caractères composée de la concaténation des champs code, ID, longueur, authentificateur de requête et attributs.[12]

- **Attributs et valeur :** Ce champ du paquet est de longueur variable et contient la charge utile du protocole, c'est-à-dire les attributs et leur valeur qui seront envoyés soit par le NAS (client RADIUS) en requête, soit par le serveur en réponse.

  Suite à la phase d'authentification définie au-dessus, débute une phase d'autorisation où le serveur RADIUS retourne les autorisations de l'utilisateur.

2. **Autorisation RADIUS**

   Dés que la phase d'authentification est passée, celle d'autorisation commence. Des données supplémentaires peuvent être transmises à l'utilisateur :
   - Les services autorisés, Telnet, connections PPP, etc.
   - Les paramètres de connexion, host, adresse IP, temps de connexion, etc.
3. **Accounting RADIUS** La comptabilité permet de suivre les services que l'utilisateur accède et les ressources réseaux utilisés.

### 3.3.7 RADIUS et Les protocoles de mots de passe

RADIUS connaît nativement deux protocoles de mot de passe qu'on a déjà défini dans le premier chapitre :

- PAP (échange en clair du nom et du mot de passe),
- CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du 'challenge').

La similarité de deux protocoles MS-CHAP et MS-CHAPv2 avec CHAP permet de les transporter en RADIUS de la même façon, à l'initiative du serveur et sous réserve bien entendu de possibilité de transport de bout en bout du supplicant au

client Radius, du client au serveur Radius et enfin du serveur RADIUS à la base de données d'identification.

### 3.3.8 Le protocole RADIUS et la couche de transport UDP

Le protocole RADIUS établit une couche applicative au-dessus de la couche de transport UDP. Les ports utilisés seront :

- 1812 pour recevoir les requêtes d'authentification et d'autorisation ;
- 1813 pour recevoir les requêtes de comptabilité[12].

## 3.4 Le Protocole 802.1x

### 3.4.1 Présentation

Le protocole 802.1X est un protocole d'authentification au niveau Ethernet mis au point par l'IEEE (Institute of electrical and electronics engineers), a comme objectif de réaliser une authentification de l'accès au réseau au moment de la connexion physique à ce dernier. Cette authentification intervient avant tout mécanisme d'auto-configuration (ex. DHCP, ...). Dans la plupart des cas, le service autorisé en cas de succès est le service Ethernet.

L'objectif de ce standard est d'autoriser l'accès physique à un réseau local après authentification depuis un réseau filaire ou sans fil, indépendamment du support de transmission utilisé, et en s'appuyant sur des mécanismes d'authentification existants.

Le 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles :

- **Le système à authentifier (supplicantou client) :** c'est un poste de travail (terminal informatique) demandant un accès au réseau.
- **L'authenticator** (commutateur, borne wifi,...ect) : c'est l'unité qui contrôle et fournit la connexion au réseau. Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé. Lorsque le client n'est pas authentifié, le port est dans l'état non autorisé et seulement le trafic nécessité par l'authentification est permis entre le terminal et l'authentificateur. Ce dernier transmet la requête d'authentification au serveur d'authentification en utilisant le pro-

tocole EAP. Les autres paquets sont bloqués lorsque le port se trouve dans l'état non autorisé.

– **Le serveur d'authentification :** il réalise la procédure d'authentification avec l'authentificateur et valide la demande d'accès. Durant cette phase, l'authentificateur n'interprète pas le dialogue entre le serveur et le terminal. Il s'agit d'un simple relais passif. Si la requête d'accès est validée par le serveur, le port est commuté dans l'état autorisé et le client est autorisé à avoir un accès complet au réseau.


FIGURE 3.6 – Acteurs principaux de 802.1x

### 3.4.2 Principe Général de 802.1x

– Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le point d'accès.
– Une fois authentifié, le point d'accès laisse passer le trafic lié au client.

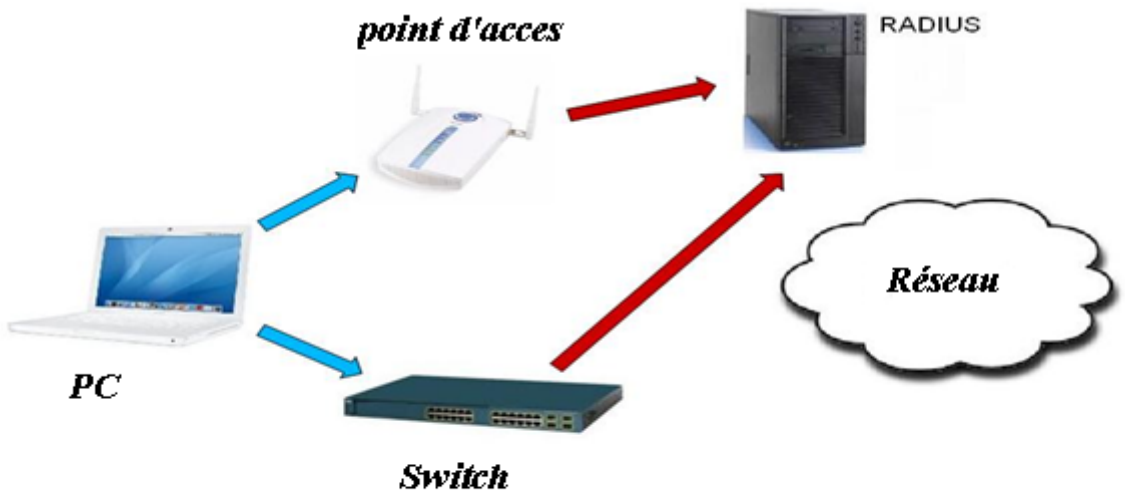


FIGURE 3.7 – Accès avant authentification

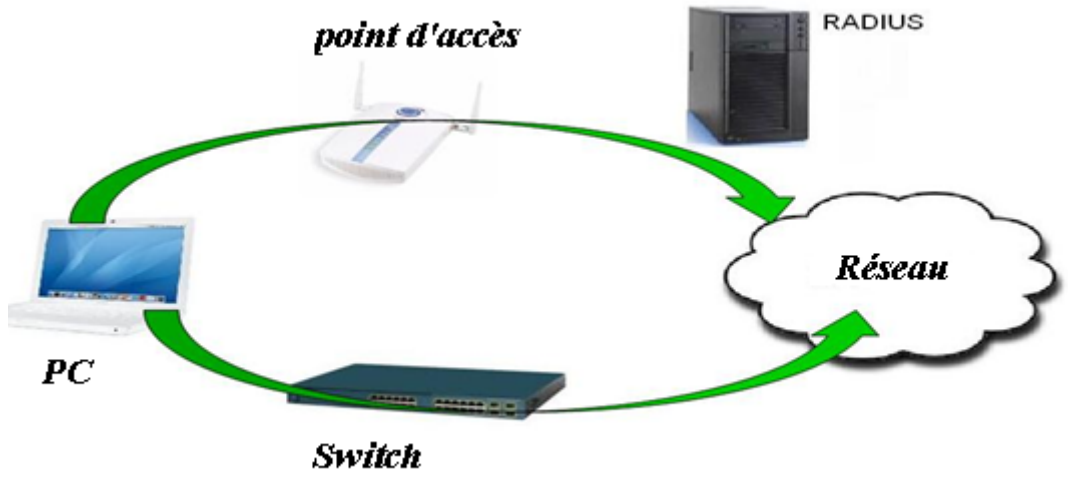


FIGURE 3.8 – Accès après authentification

Le 802.1x s'appuie sur :

- **le protocole EAP (Extensible Authentication Protocol** :pour les communications client/serveur, dont le rôle est de transporter les informations d'identification des utilisateurs.
- **serveur d'identification Radius**(ou Tacacs si c'est du full Cisco) :Ce dernier servira à authentifier les utilisateurs qui se connectent au réseau et à leur permettre ou non l'accès à certaines ressources de l'entreprise.

Avec l'IEEE 802.1X il est possible de contrôler l'accès à chacun des ports d'un équipement réseaux (switch ou bornes Wifi par exemple).

### 3.4.3 Mécanisme Général

Le supplicant souhaite accéder aux ressources du réseau. Mais pour cela il va devoir s'authentifier. Le système authentificateur gère cet accès via le PAE. Il se comporte comme un relais, comme un proxy entre l'entité qui souhaite être sur le réseau et le serveur d'authentification. Le supplicant va dialoguer avec le serveur via le relais, grâce au protocole EAP. Si l'authentification réussit, le serveur donne au demandeur l'accès aux ressources via le système authentificateur et son PAE.
La structure du 802.1x s'appuie donc sur 4 couches :

- couche média : le Token Ring, l'Ethernet...
- couche protocole : l'EAP, protocole d'identification
- couche méthode d'authentification : elle s'appuie sur les mots de passe, les certificats...
- couche infrastructures qui comportent le matériel d'authentification comme le serveur Radius.[13]

### 3.4.4 Authentification basée sur le contrôle des ports

En 802.1X, dans la mesure où c'est le supplicant qui envoie les éléments d'authentification, il y a bien une communication. Or, comment peut-il y avoir une communication, et donc un trafic réseau, puisque le port du commutateur n'est pas ouvert et qu'il ne le sera que lorsque le poste aura été authentifié ? C'est justement là que tient tout le protocole 802.1X. Les ports du commutateur seront configurés d'une façon particulière. Avant d'être complètement ouverts, ils ne laisseront passer qu'un seul type de protocole : EAP. D'ailleurs, l'autre nom de 802.1X est " Port-Based Network Access Control " qui, traduit littéralement, signifie " Accès au réseau basé sur le contrôle de port ". Tout se passe comme si chaque port était coupé en deux :

- port contrôlé : au départ, il est maintenue fermée par le commutateur.
- port non contrôlé : Par cette voie, le commutateur n'accepte que le protocole EAP.

Comme l'indique la figure suivante :

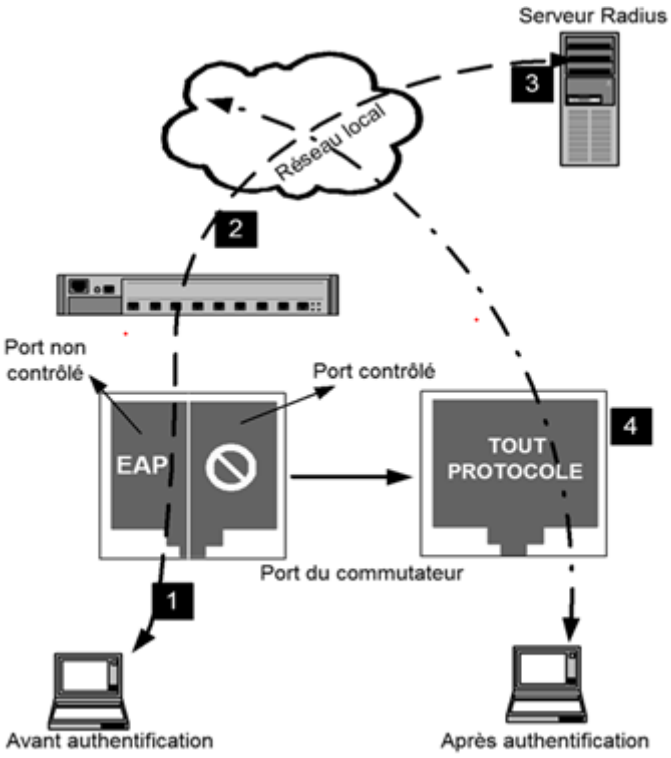


FIGURE 3.9 – Principe des ports contrôlés et non contrôlés

1. le supplicant envoie ses informations vers le commutateur dans des paquets EAP.
2. le commutateur reçoit les informations par le port non contrôlé et les retransmet encapsulés dans des paquets Radius vers le serveur.
3. Après interrogation de sa base et, éventuellement après plusieurs échanges avec le commutateur, le serveur lui renvoie l'ordre d'ouvrir complètement le port et sur un VLAN donné.
4. le commutateur ouvre le port sur le VLAN commandé par le serveur ; le poste peut alors utiliser pleinement le réseau.

Les communications entre le poste de travail et le commutateur ne sont pas des communications IP, mais Ethernet de bas niveau. Le commutateur sert alors d'intermédiaire entre les deux parties et encapsule les paquets EAP venant du supplicant dans les paquets du protocole Radius. Et c'est avec ce protocole qu'il communique avec le serveur, cette fois en utilisant la couche UDP.[12]

### 3.4.5 Méthode d'authentification 802.1x

Le protocole 802.1X définit l'utilisation d'EAP (RFC 2284), mécanisme décrivant la méthode utilisée pour réaliser l'authentification.

**A.Présentation du protocole EAP**

Le protocole EAP (Extensible Authentication Protocol) est une norme IETF (Internet Engineering Task Force), qui définit une infrastructure permettant aux clients d'accès réseau et aux serveurs d'authentification d'héberger des modules pour les méthodes et technologies d'authentification actuelles et futures.

Microsoft Windows utilise EAP pour authentifier l'accès réseau pour les connexions PPP (Point-to-Point Protocol) (accès distant et réseau privé virtuel) et pour l'accès réseau basé sur IEEE 802.1X aux commutateurs Ethernet et points d'accès sans fil.[14]

EAP n'est pas un protocole d'authentification mais un protocole de transport de protocoles d'authentification (TLS, PEAP, TTLS...). Il définit des mécanismes d'échanges entre équipements, mais pas les principes mêmes de l'authentification. Les paquets du protocole d'authentification sont encapsulés dans des paquets EAP L'équipement réseau connaît le protocole EAP et c'est tout (il ne sait pas ce que transporte EAP) et redirige les paquets EAP vers un serveur d'authentification grâce au protocole Radius. [12]

Le domaine d'application de ce protocole correspond à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que : connexion réseau sans fil entre un poste utilisateur et une borne d'accès, connexion filaire entre un poste utilisateur et un commutateur[15].

**On distingue deux types de trafic EAP :**

- entre le système à authentifier et le point d'accès (support : 802.11a, b, g ou 802.3) :**EAP over LAN (EAPOL)**
- entre le point d'accès et le serveur d'authentification (de type RADIUS) : **EAP over Radius**

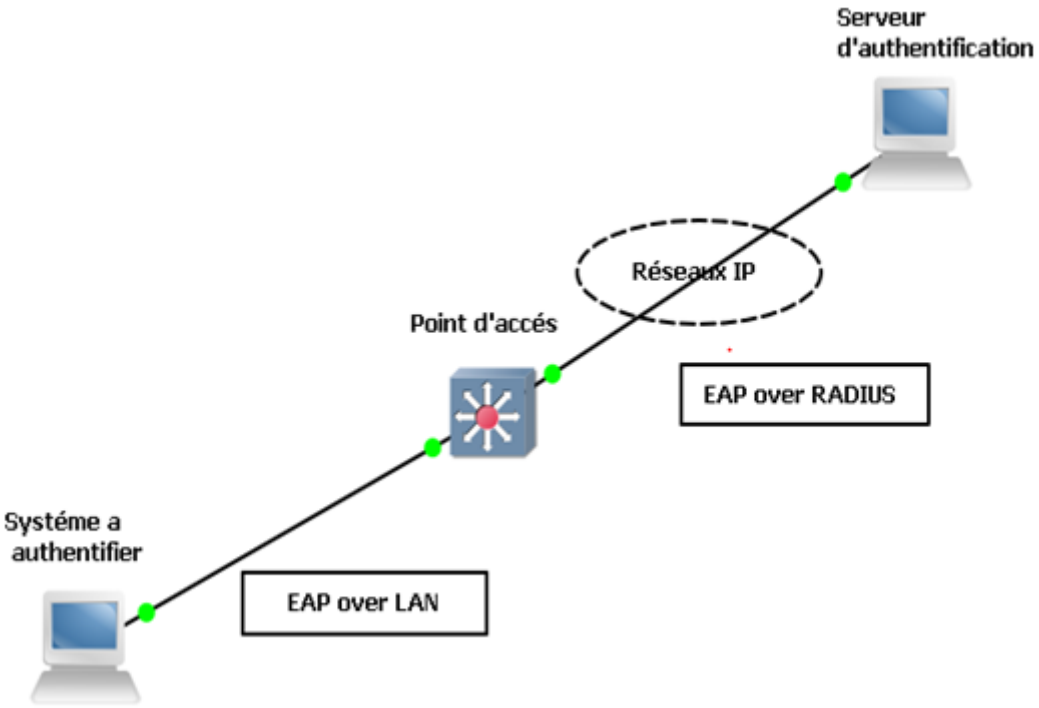


FIGURE 3.10 – Types EAP

### B. Trame EAP

Un message EAP peut être de quatre types/code : Request, Response, Success ou Failure. Une trame EAP se compose de 5 champs de longueurs différentes détaillés ci-dessous.

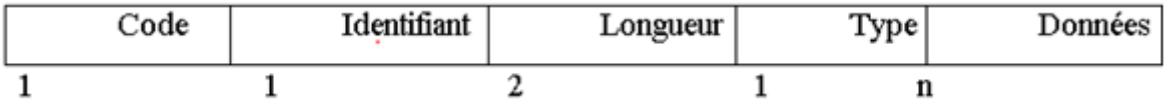


FIGURE 3.11 – Trame EAP

**Code :** 1 octet (de 1 à 6 pour Request, Response, Success, Failure, Initiate, Finish) ;
**Identifiant :** 1 octet (pour l'association des requêtes et des reponses) ;
**Longueur :** 2 octets ; **Type :** 1 octet (uniquement présent dans les échanges Request/Response, identifie le type de requête : identifiant, challenge de type donnée, etc.) ; **Données :** variable, encapsulation des méthodes EAP (vide pour Success et Failure).[16]

Les quatre types de messages EAP les plus fréquents sont les suivants :

- Identity : identité de l'utilisateur souhaitant accéder au réseau
- Notification : chaine de caractère envoyé au client (supplicant)
- Nak : type proposé uniquement lors des réponses indiquant un refus de la méthode d'authentification et en propose une autre.
- MD5-Challenge : utiliser lors du "challenge".

Les trames EAP sont encapsulées dans des trames EAP over LAN (EAPOL) pour pouvoir être transmises sur les réseaux locaux (Ethernet, Token Ring...).

### C. Les couches EAP

EAP est un protocole qui place trois couches au-dessus la couche liaison, IEEE 802. C'est là qu'intervient le code logiciel du supplicant. Lorsque l'authentification sera terminée, ces couches EAP resteront en place car elles seront utiles pour gérer, par exemple, les ré-authentifications. Quatre types de paquets sont utilisés pour le protocole EAP :

Request , Response , Success et Failure.

Ces paquets traversent trois couches comme l'indique la figure ci dessous.

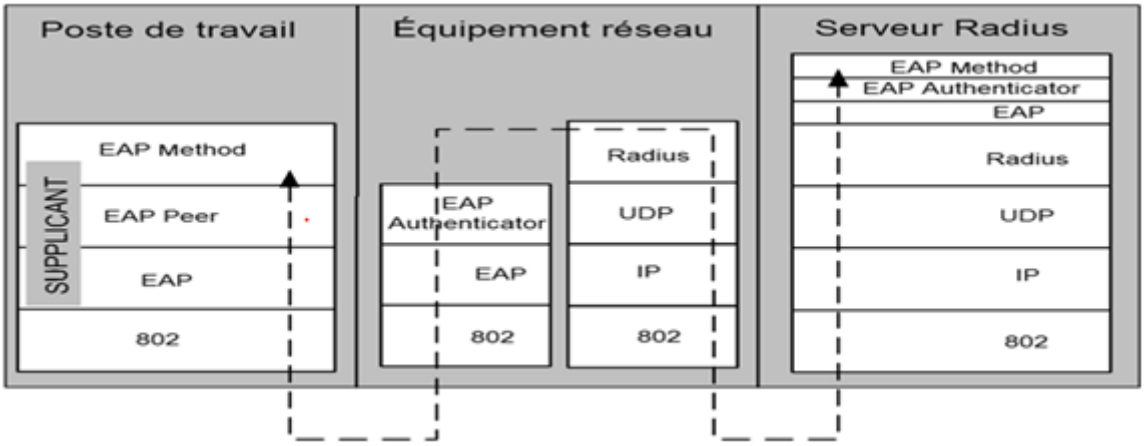


FIGURE 3.12 – Les couches EAP

**La couche EAP** Elle reçoit et envoie les paquets vers la couche basse (802) et transmet les paquets de type Request, Success et Failure à la couche EAP Peer. Les paquets Response sont transmis à la couche EAP Authenticator.

**Les couches EAP Peer et EAP Authenticator** La couche EAP Peer est implémentée sur le poste de travail, tandis que la couche EAP Authenticator est

implémentée sur le NAS et sur le serveur Radius. Ces couches ont pour rôle d'interpréter le type de paquet Request ou Response et de les diriger vers la couche EAP Method correspondant au protocole d'authentification utilisé (par exemple, TLS, PEAP).

**La couche EAP Method** C'est dans cette couche que se tient le code logiciel du protocole d'authentification utilisé. Le NAS n'a pas besoin de cette couche puisqu'il agit de façon transparente (sauf si le serveur Radius est embarqué dans le NAS). Le rôle du NAS est d'extraire le paquet EAP qui lui arrive du supplicant et de le faire passer dans la couche Radius (et vice versa). Pour cela, il doit encapsuler, c'est-à-dire écrire, le paquet EAP dans un attribut particulier de Radius qui a été ajouté au modèle d'origine pour cette fonction. Il s'agit de l'attribut EAP-Message (numéro 79). Un autre attribut, Message-Authenticator (numéro 80), a été ajouté. Cependant, Cet attribut sera présent dans tous les paquets échangés entre le NAS et le serveur mais n'influe pas sur la compréhension globale du protocole. Du côté du serveur Radius, c'est un module spécifique qui décapsulera la valeur de l'attribut EAP-Message et qui l'interprétera en suivant le modèle de couches d'EAP vu plus haut.

### D. Les méthodes associées à EAP

Une méthode d'authentification EAP utilise différents éléments pour identifier un client :

- login / mot de passe ;
- certificat électronique ;
- biométrie ; (SIM). ;

Certaines méthodes combinent plusieurs critères (certificats et login/mot de passe etc.) Les méthodes d'authentification les plus communes sur EAP sont :

**EAP-TLS** (Transport Layer Security) : a été créé par Microsoft et acceptée par l'IETF comme RFC 2716. Cette méthode se base sur les certificats numériques. Le serveur et le client s'authentifie mutuellement tout en cryptant les données échangées dans cette phase d'authentification. L'utilisation de clés publiques et privées des deux côtés va permettre de créer un tunnel sécurisé entre les deux parties, ce qui garantit notamment l'intégrité des données. Avec ce principe, le client ne fournit pas de mot de passe, le certificat permettant l'authentification.

**EAP-TTLS** (Tunneled Transport Layer Security) : est un protocole propriétaire développé par Microsoft, Cisco et RSA Security. Ce protocole assure une authenti-

fication mixte par certificat et mot de passe, le tout dans un tunnel sécurisé. Cette méthode combine l'avantage de l'authentification du client via le couple login/mot de passe ainsi que la sécurité des données via l'encapsulation cryptée des données et l'authentification du serveur par un certificat.

**PEAP :** est un protocole propriétaire développé par Microsoft, Cisco et RSA Security.ici seul le serveur d'authentification dispose d'un certificat numérique. Il le transmet au client qui va pouvoir l'authentifier. Un tunnel sécurisé TLS est alors établit entre les deux parties. Le client va s'authentifier via une méthode EAP quelconque mais bénéficiera de l'encapsulation sécurisée des données dans le tunnel TLS.

**EAP-MD5 Challenge :** l'utilisateur va être authentifié via son login et son mot de passe mais ce dernier ne sera pas transmis en clair sur le réseau. Grâce au mécanisme de challenge / réponse, le serveur envoie un challenge au client, celui renvoie son mot de passe associé au challenge, le serveur compare le résultat avec le mot de passe qu'il détient dans sa base plus le challenge envoyé. Si le résultat est identique alors l'accès est autorisé, sinon il est refusé.

**LEAP (Lightweight EAP) :** est une implémentation propriétaire d'EAP conçu par Cisco Systems assurant une authentification simple par mot de passe via une encapsulation sécurisée, ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

**EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) :** est une proposition de Cisco Systems pour fixer les faiblesses de LEAP en garantissant une flexibilité d'authentification via une encapsulation sécurisée.[15]

### E. Echange des messages EAP

Le schéma ci-dessous explique le mécanisme classique d'authentification EAP. Il représente une demande d'authentification d'un client au commutateur jouant le rôle de l'authentificateur. Ce dernier va demander l'accès au serveur d'authentification qui acceptera ou non l'authentification du client.

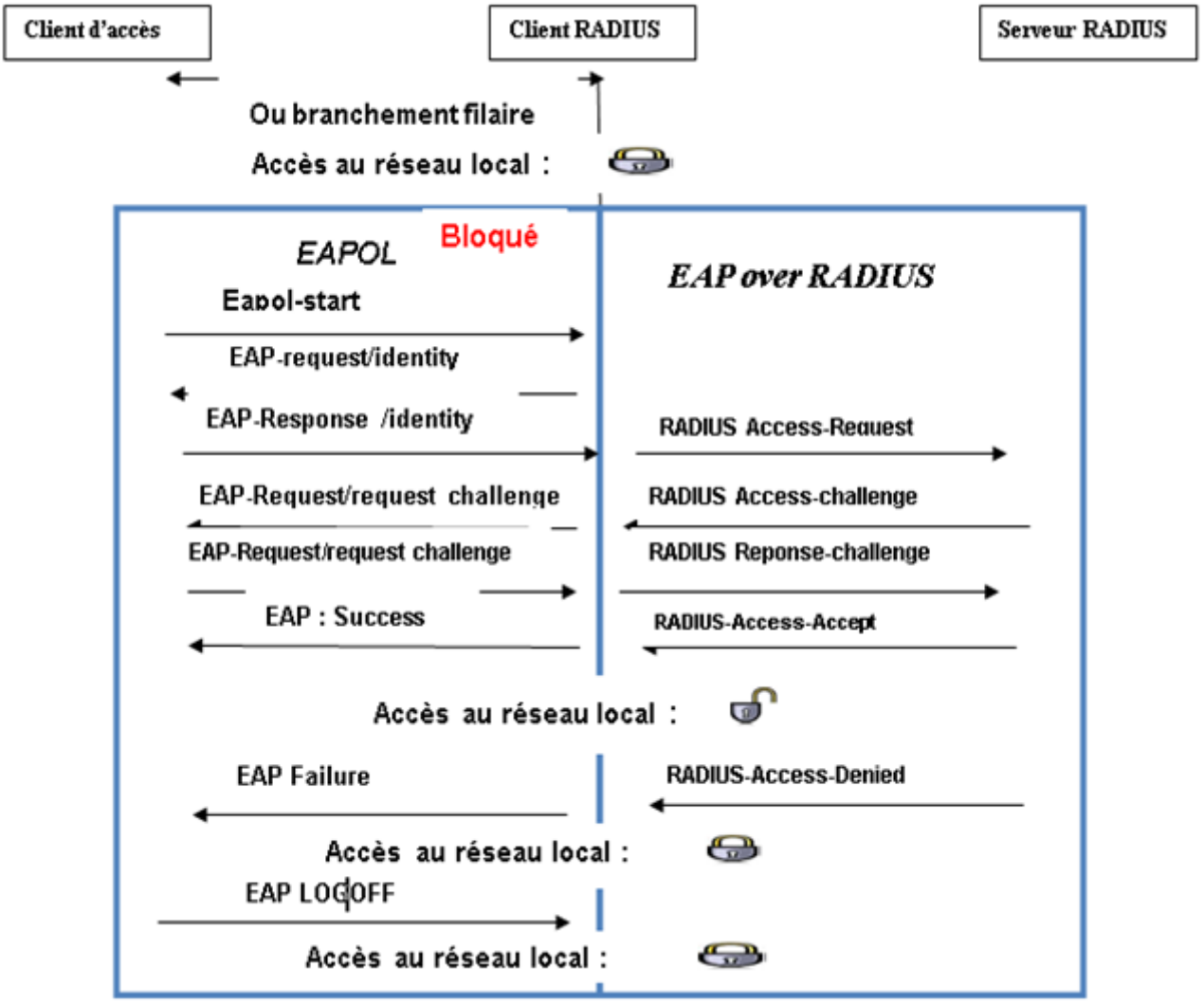


FIGURE 3.13 – Echange des messages EAP

### F. Etapes de protocole EAP

Le protocole EAP peut être découpé en quatre étapes :

- Identité externe.
- Négociation de protocole.
- Protocole transporté.
- Gestion des clés de chiffrement.

**Étape "Identité externe" :**cette étape intervient entre le poste de travail, ou plus précisément le supplicant, et le NAS

1. Le supplicant et le NAS négocient l'usage d'EAP.

2. Le NAS envoie un paquet EAP de type EAP-Request/Identity, c'est-à-dire qu'il demande au supplicant son identité. On l'appellera identité externe
3. Le supplicant répond par un EAP-Response/Identity, c'est-à-dire l'identité qui lui est demandée. Cette identité est fournie par le supplicant qui a été configuré par le propriétaire de la machine.
4. Le NAS fabrique un paquet Access-Request dans lequel il écrit un en-tête (code + identifiant + longueur + authentificateur) puis un champ attributs et valeurs. À l'intérieur de celui-ci, il écrit l'attribut EAP-Message dans lequel il encapsule le paquet EAP venant du supplicant. Il écrira également un attribut User-Name dans lequel il copiera l'identité (celle envoyée dans l'EAP-Response/identity). Le serveur Radius utilisera le contenu de User-Name comme point d'entrée dans sa base de données (AD).
5. Le NAS envoie le paquet Access-Request au serveur. Le NAS écrit d'autres attributs dans l'Access-Request, parmi lesquels Calling-Station-Id qui permettra au serveur Radius de disposer de l'adresse MAC du poste de travail en plus de l'authentification envoyée par le supplicant.

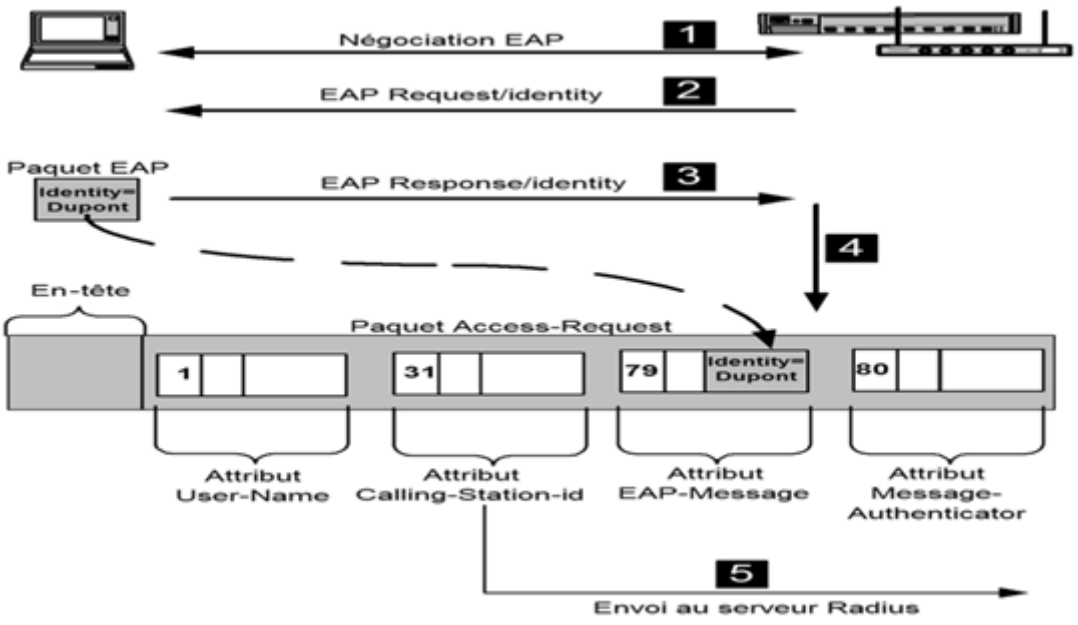


FIGURE 3.14 – Étape " identité externe " d'EAP

**Étape " Négociation de protocole "** Cette étape correspond à la réception du paquet Access-Request par le serveur et à sa réponse vers le supplicant afin de proposer une méthode d'authentification.

1. Le serveur reçoit le paquet Access-Request.
2. Il construit un paquet Access-Challenge dans lequel il écrit un attribut EAP-Message formé d'un paquet EAP-Request qui contient une proposition de protocole d'authentification. Par exemple, il propose PEAP.
3. Le NAS décapsule le paquet EAP contenu dans EAP-Message et le transfère sur la couche EAP vers le supplicant. Celui-ci répond par un paquet EAP-Response. S'il connaît le protocole proposé et qu'il est configuré, il l'acceptera. Dans le cas contraire, il proposera un protocole pour lequel il est configuré, par exemple TLS.
4. La réponse du supplicant est encapsulée, comme dans la première phase, dans un nouveau paquet Access-Request. Si le serveur accepte ce protocole alors on passe à la troisième phase, c'est-à-dire l'exécution du protocole d'authentification. Dans le cas contraire, il envoie un Access-Reject au NAS.

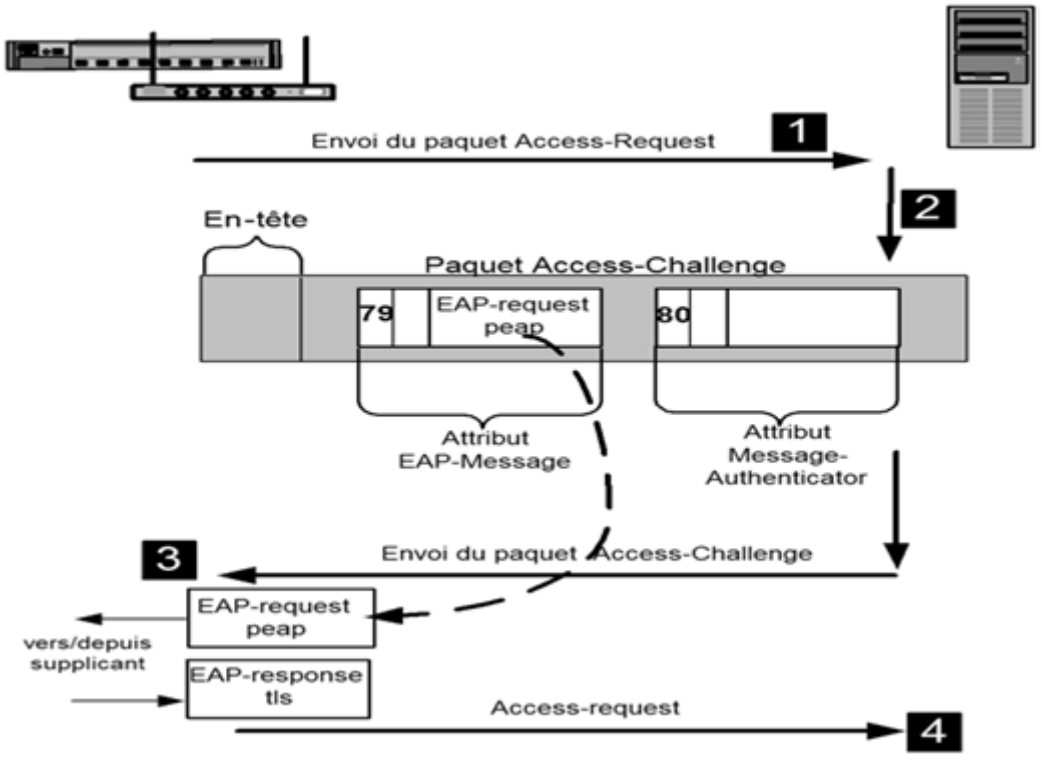


FIGURE 3.15 – Étape " Négociation de protocole " d'EAP

**Étape " Protocole transporté "**

Cette étape correspond à l'exécution du protocole d'authentification transporté. Le principe est le même que pour les deux premières étapes, c'est-à-dire un échange de paquets Radius Access Request/Access-Challenge encapsulant des paquets EAPRequest ou EAP-Response. La quantité et le contenu de ces échanges dépend du protocole ( " Le protocole EAP/TLS ", " Le protocole PEAP " et " Le protocole EAP/TTLS ").

**Étape " Gestion des clés de chiffrement "**

Cette étape n'a de sens que dans le cas du Wi-Fi. Elle permet la gestion dynamique des clés de chiffrement.

## 3.5 Objectifs de l'authentification 802.1x

L'objectif principal de cette authentification est la traçabilité des transactions. Le contrôle permanent de l'intégrité et de l'accès (usage, identité du destinataire, émetteur, propriétaire) à un contenu ou à un service constitue le fondement de la

traçabilité des transactions et permet :

- La protection du patrimoine informatique de l'entreprise : réduire les dégâts qui résultent d'attaques, de la perte de temps, de la perte d'informations ou de l'espionnage...
- La protection de la vie privée. Les données personnelles véhiculées dans les systèmes d'information sont des données sensibles à protéger.
- La nécessité désormais d'identifier les utilisateurs d'un réseau.
- Les besoins de sécurité en matière d'accès au réseau (attribution de VLAN).
- Les besoins de traçabilité des utilisateurs du SI : le contexte réglementaire et les bonnes pratiques impliquent que l'administration du SI soit traçable. On parlera d'accounting avec RADIUS.
- La mobilité de certains utilisateurs (mobilité interne et externe). Quel que soit l'accès au SI, les conditions doivent être les mêmes.
- La possibilité d'avoir un réseau invité où les personnes extérieures pourront se connecter avec des droits restreints.
- La localisation géographique des utilisateurs grâce à l'attribution des VLAN.

# Conclusion

L'étude d'une solution a pour objectif, de permettre une bonne réalisation. Dans ce chapitre on a bien détaillé le protocole RADIUS qui convient à la norme 802.1X et supporte les protocoles EAP. Le chapitre qui suit va être consacré à la mise oeuvre d'un service RADIUS pour l'authentification 802.1X.

# 4

# Mise en oeuvre et réalisation

# Introduction

Notre projet s'inscrit dans le domaine de la sécurité informatique,il vise à apporter une solution au problème de l'authentification dans le réseau de l'entreprise Cevital de Bejaia.

Ce chapitre est consacré à la mise en oeuvre des solutions proposées pour la réalisation d'un système d'authentification permettant d'authentifier des utilisateurs avant tout accès au réseau de l'entreprise, ce système est le serveur RADIUS qui s'appuie sur l'authentification 802.1x et utilise le protocole EAP.

## 4.1 les composantes nécessaires :

pour implémenter ce systéme d'authentification,trois composantes sont necessaires

- Un Windows Server 2008 exécutant NPS(Network Policy Server) ;
- Un client sous Windows XP SP3 ;
- Un commutateur prenant en charge le protocole 802.1X et la gestion des VLAN ;

## 4.2 Les outils utilisés

Pour la réalisation de notre projet, on a utilisé les outils suivants :

### 4.2.1 Virtualisation

La virtualisation représente l'ensemble des techniques matérielles et logicielles qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation , séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.parmi les avantages de la virtualiation :

- La possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine
- portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre
- Accélération des déploiements de systèmes et d'applications en entreprise

– Administration simplifiée de l'ensemble des serveurs[17] Tous ces avantages nous ont motivés à utiliser un environnement virtuel qui est la VMware

Dans notre cas, on a utilisé comme machine virtuelle le windows server 2008 R2 qui inclut le serveur d'authentification RADIUS et windows XP comme machine cliente.

### 4.2.2 Windows Server 2008 R2

Le windows server 2008 est un système d'exploitation de Microsoft qui Reprend les fonctionnalités et les caractéristiques de la version actuelle de Windows Server 2008, Windows Server 2008 R2 permet de créer des solutions plus simples à planifier, à déployer et à gérer qu'avec les versions précédentes de Windows Server. S'appuyant sur le haut degré de sécurité, de fiabilité et de performance de Windows Server 2008, Windows Server 2008 R2 étend la connectivité et le contrôle aux ressources locales et distantes. [18]

La grande nouveauté de Windows Server 2008 en ce qui concerne la protection réseau est son composant NPS, acronyme de Network Policy Server. Il s'agit du nouveau serveur RADIUS de Microsoft destiné à remplacer IAS (Internet Authentification Service). Rappelons qu'un serveur RADIUS a pour mission de centraliser l'authentification et l'autorisation en s'appuyant généralement sur Active Directory. Entièrement reconçu ; le service NPS se présente comme la clé de voute de la technologie NAP(Network access protocol). Quelque soit la méthode d'enfoncement que vous serez amenés à mettre en place, la configuration du service NPS sera une étape déterminante dans la procédure.

1. **Active Directory**
   a. **Définition** Active Directory est la plus grande évolution qu'aient connue les environnements de Microsoft depuis les premières versions serveurs. Il s'agit d'une base d'annuaire qui va regrouper tous les objets présents sur le réseau. Active Directory est l'outil de travail principal dans la gestion d'un domaine Windows. Cette base d'annuaire va permettre une administration simplifiée, offrant une forte tolérance aux pannes puisqu'il s'agit d'une base d'annuaire distribuée.

**b. Installation de l'Active Directory sous windows server 2008** L'installation et la configuration de l'Active Directory nécessite plusieurs étapes à suivre :

**i. Ajout de rôle "Active Directory Domain Services" (service s de domaine Active Directory)** : pour ajouter ce rôle,un clic droit sur **Roles** puis **Add roles** ensuite on coche la case de rôle **"Active Directory Domain Services"** comme suit : newpage

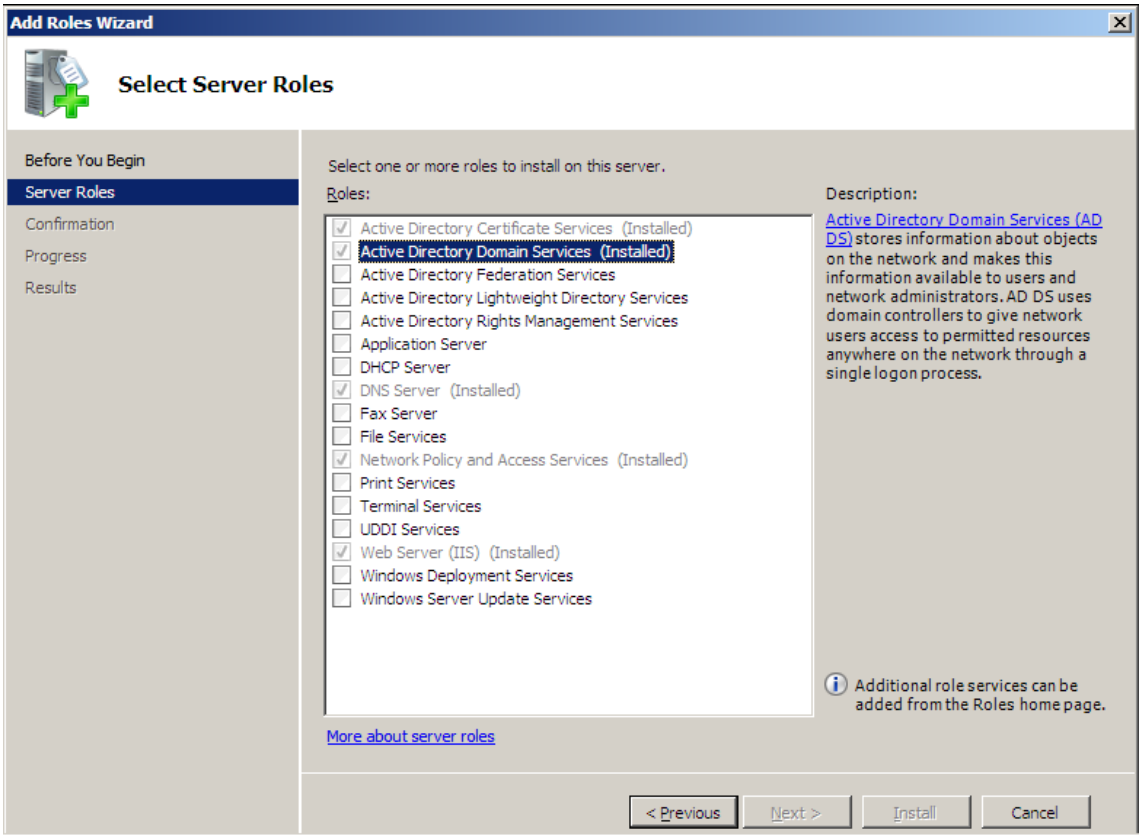


FIGURE 4.1 – Ajout de services de domaine Active Directory

### ii. Installation

– Pour faire de votre Windows Server 2008 R2 un contrôleur de domaine, il suffit de lancer la commande **dcpromo**,pour ce faire ;on clique sur **Démarrer**, **executer** et on tape la commande,l'assistant Installation de Active Directory démarre .


**Figure 4.2 – Installation de Active Directory**

– On choisit l'installation en mode avancé

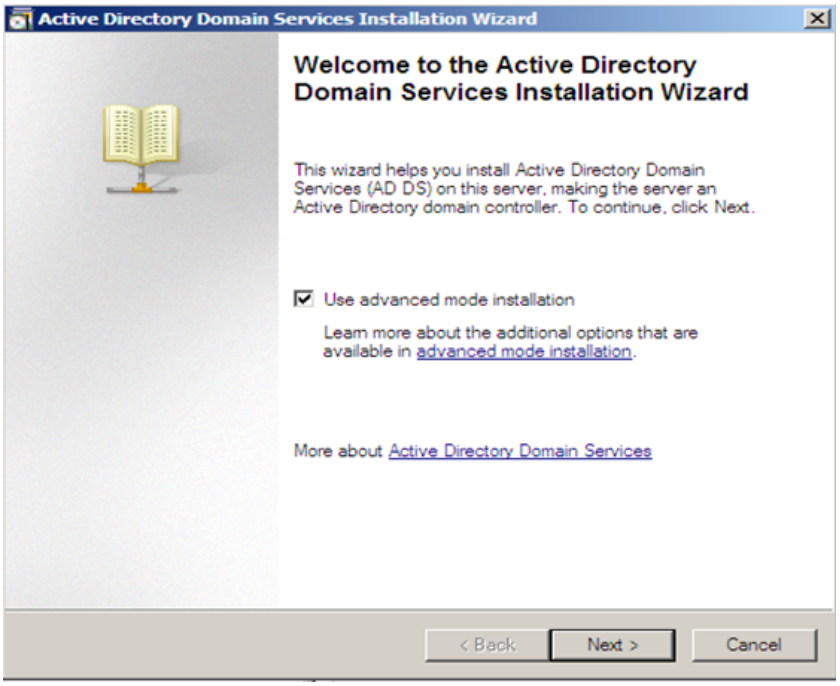


**Figure 4.3 – Installation de Active Directory en mode avancé**

– On sélectionne "créer un domaine dans une nouvelle forêt" et on clique sur "next" pour saisir le nom de notre domaine :**cevital.local**

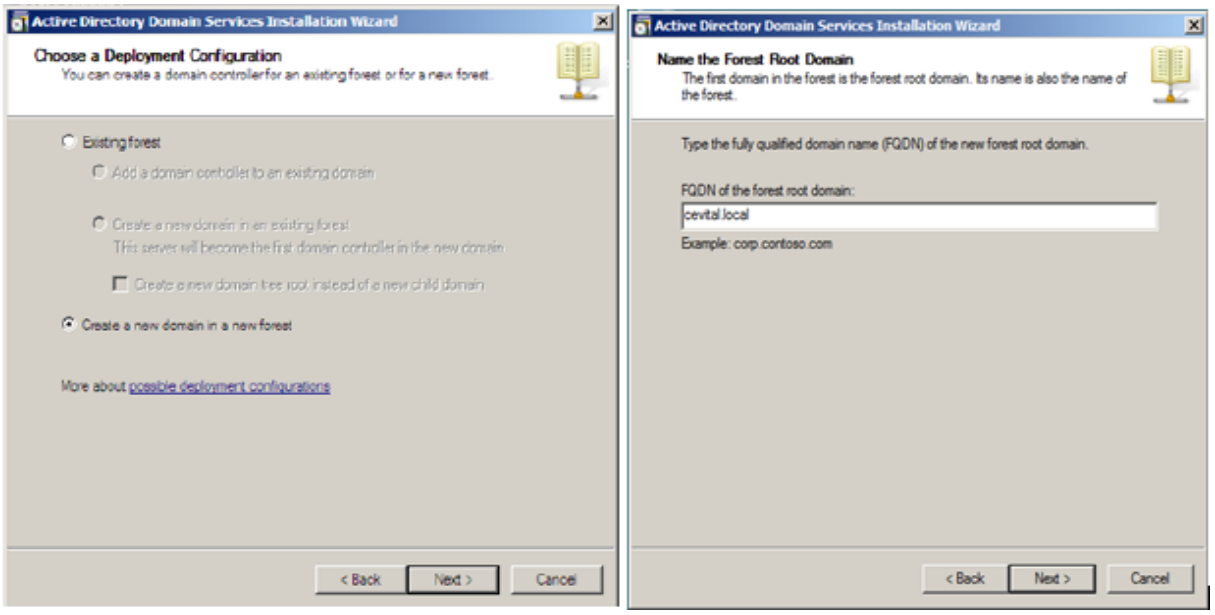


**Figure 4.4 – Création de domaine "cevital.local"**

– l'assistant suivant montre le nom NetBIOS de domaine ; pour poursuivre l'installation on choisit le niveau fonctionnel de la forêt, dans notre cas on a choisi le niveau fonctionnel "windows server 2003" qui a plus de fonctionnalités par rapport aux autres serveurs .

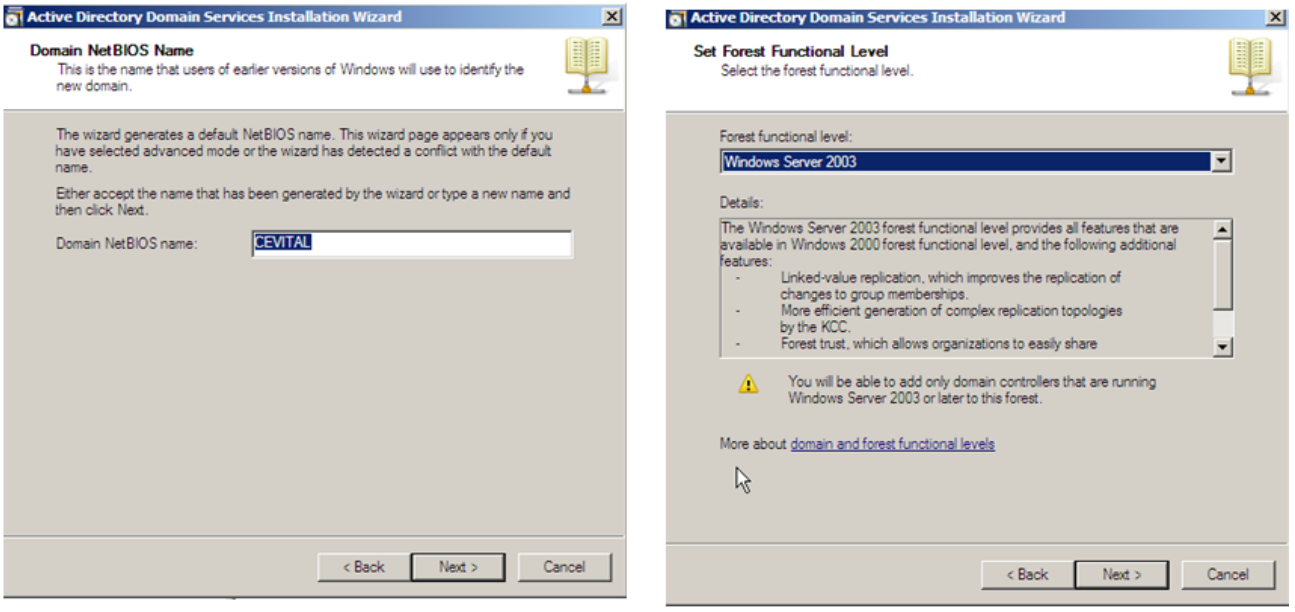


**FIGURE 4.5 – Nom NetBIOS de domaine et le niveau fonctionnel de la forêt**

– En suite on spécifie les dossiers qui contiendront la base de données du contrôleur de domaine Active directory, les fichiers journaux et SYSVOL.

Et pour éviter les restauration non souhaitées de Active Directory,il est demandé de saisir un mot de passe de restauration.

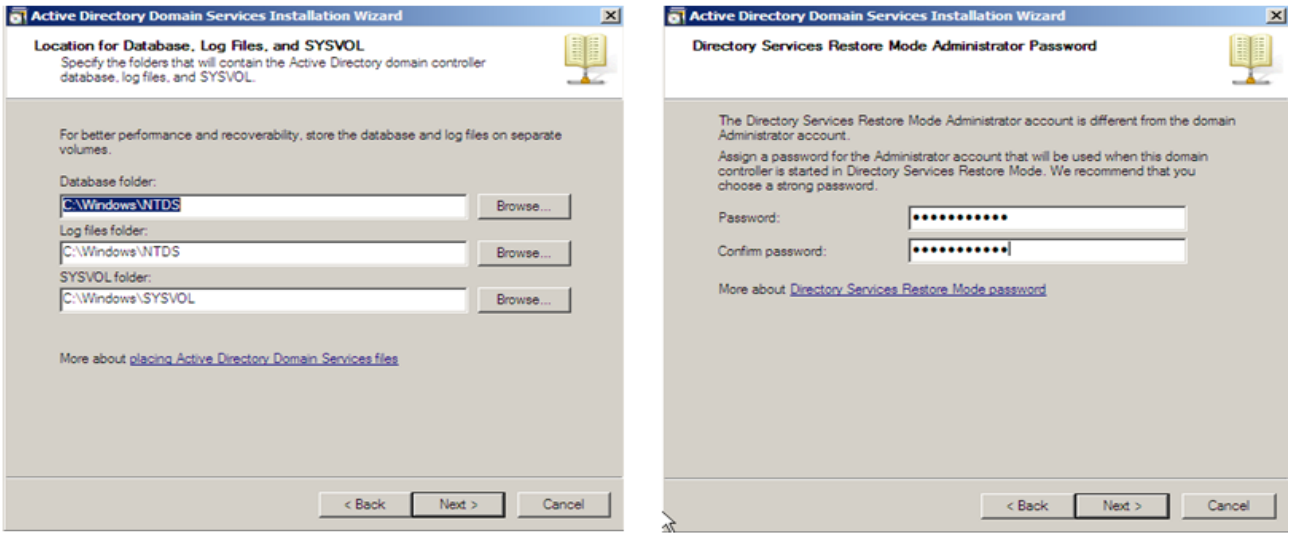


**FIGURE 4.6 – l'emplacement des fichiers Active Directory et Introduction de mot de passe.**

– L'installation de service de domaine d'active directory commence après un récapitulatif de sélections

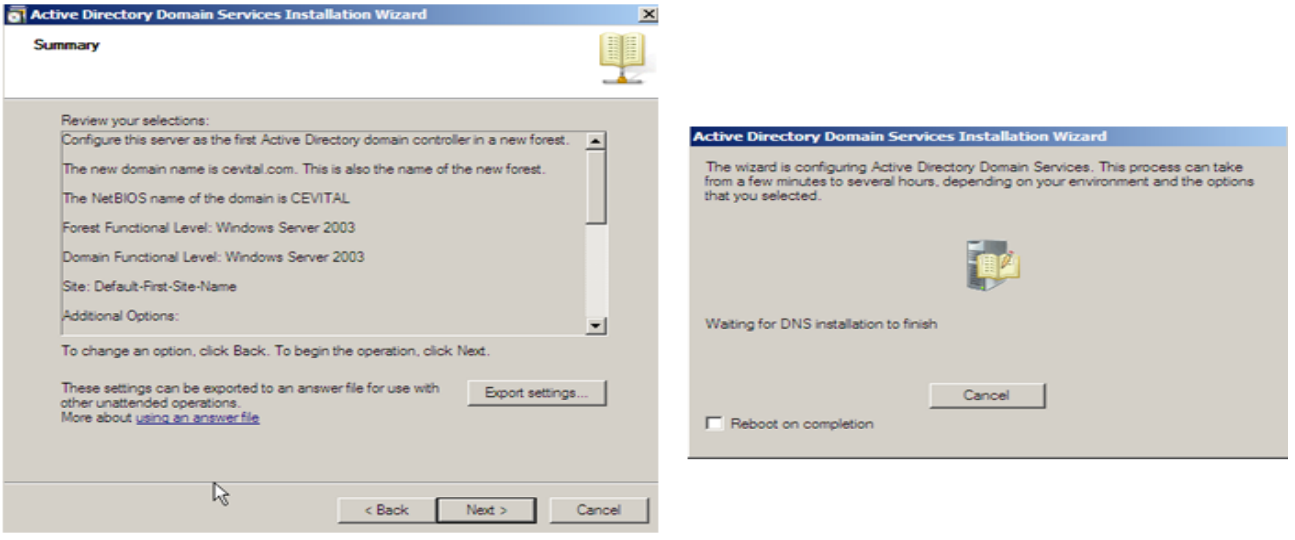


**FIGURE 4.7 – l'installation de services de domaine Active directory**

– L'installation de domaine Active Directory se termine en cliquant sur "Finish"

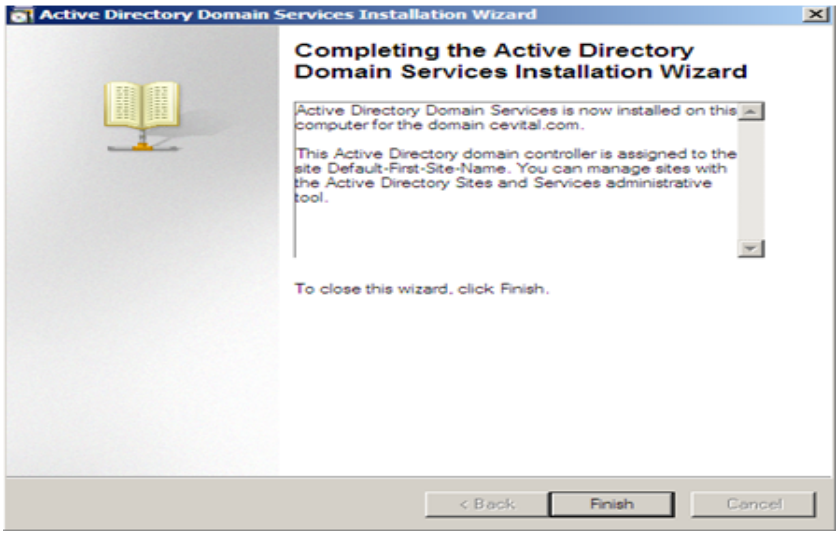


**Figure 4.8 – Fin d'installation de domaine Active Directory**

### 4.2.3 GNS3(Graphical Network Simulator)

GNS3(Graphical Network Simulator) est un simulateur d'équipements Cisco. Cet outil permet donc de charger de véritables images IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur pour avoir un routeur Cisco virtuel. Afin de permettre ces simulations, GNS3 est composé des outils suivants :

- **Dynamips :** Emulateur d'IOS Cisco.
- **Dynagen :** Interface permettant l'interconnexion de plusieurs machines émulées(virtuelles) ;
- **Qemu :** Emulateur de système ;
- **Virtualbox :** Logiciel permettant la création de machines virtuelles[19].

## 4.3 Présentation des VLANs utilisés

Les VLAN permettent de créer des réseaux logiques au sein de commutateurs et routeurs physiquement raccordés au même réseau. Ils permettent de regrouper les utilisateurs par fonction dans l'entreprise (commerciaux, techniciens, assistants, ...), par niveau de droits (administrateurs, utilisateurs, ...) ou autre. Il s'agit d'une conception pleinement logique, sans tenir compte de la localisation géographique de l'utilisateur dans l'Entreprise. Les Vlans représenté dans notre projet sont les suivants :

- VLAN Production ;

- VLAN DRH ;
- VLAN Commercial ;
- VLAN IT ;
- VLAN MGT ;
- VLAN Guest.

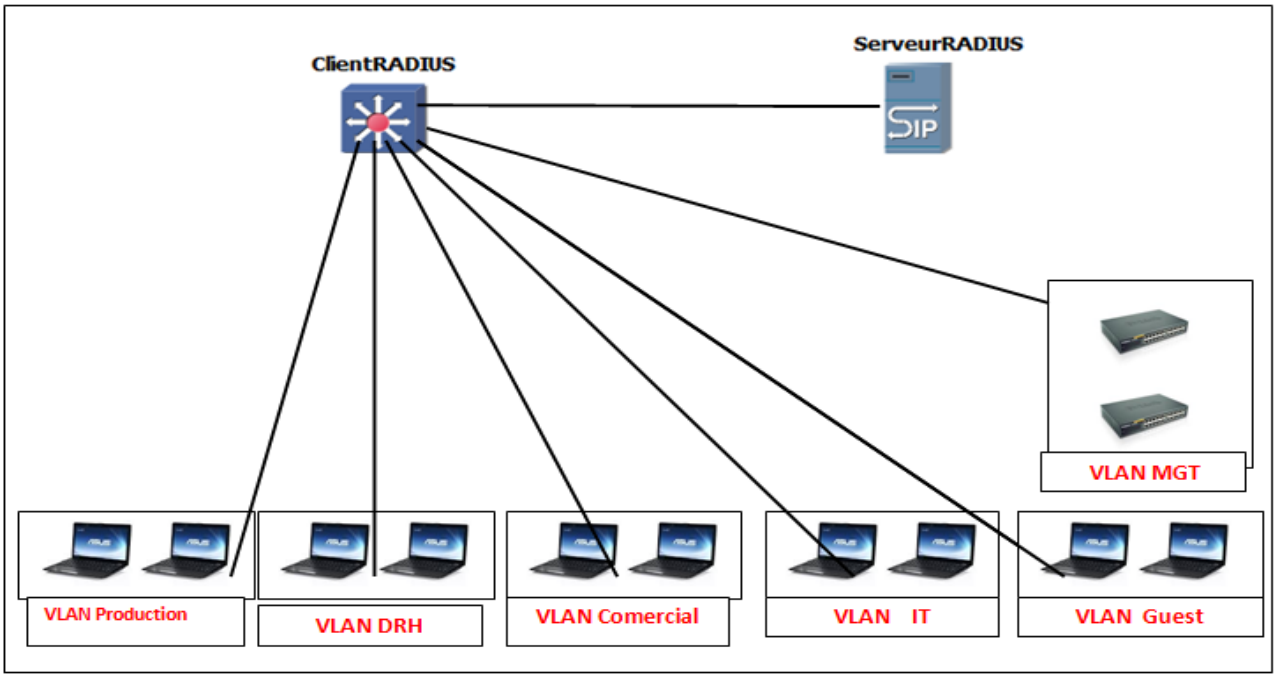


**FIGURE 4.9 – présentation des différents VLANs**

- **Nomination et adressage des VLANs**

  Les noms et identificateurs des VLANs à implémenter ainsi leur adresssage serons représentés comme suit :

| Nom du VLAN | VLAN-ID | Description | Adresse VLAN |
|---|---|---|---|
| Production | 10 | Production | 10.10.10.0/24 |
| DRH | 11 | Direction Ressources Humaine | 10.10.11.0/24 |
| Commercial | 12 | Vlan de direction Commerciale | 10.10.12.0/24 |
| IT | 13 | Informatique Technologie | 10.10.13.0/24 |
| MGT | 25 | Vlan management (pour les équipements réseau) | 10.10.25.0/24 |
| Guest | 30 | Vlan pour les invités | 10.10.30.0/24 |

**FIGURE 4.10 – Nomination et adressage des VLANs**

## 4.4 Présentation de l'architecture réseau

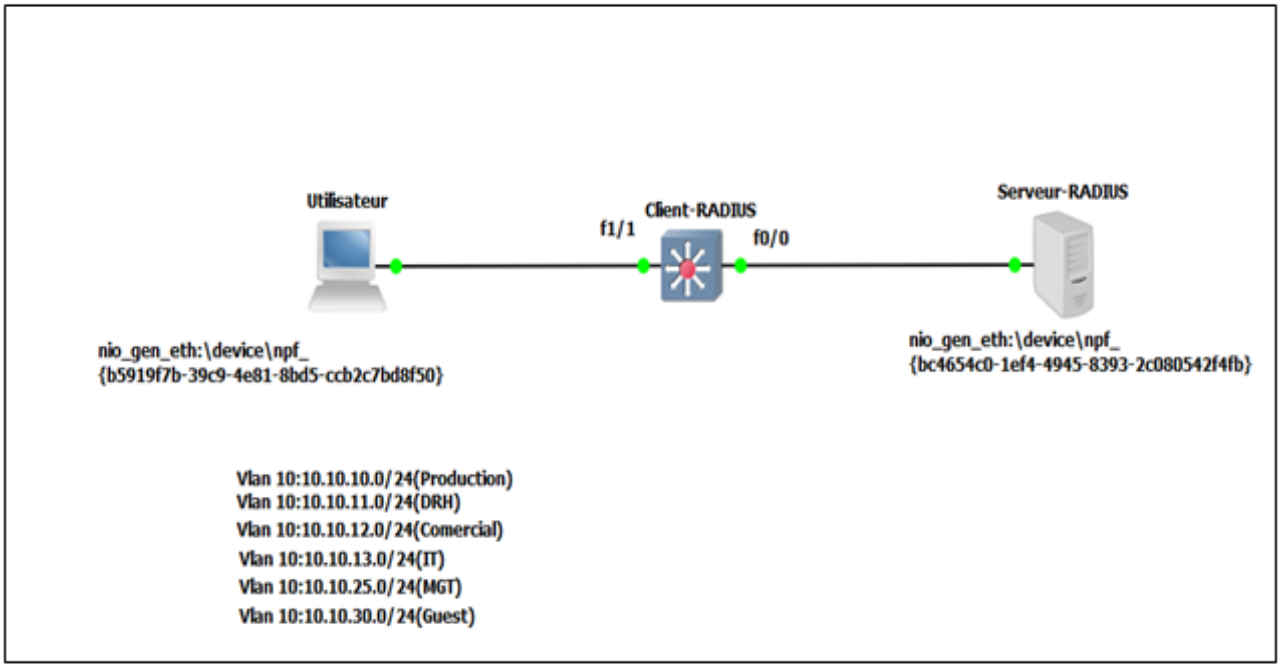


**Figure 4.11 – Présentation de l'architecture réseau**

## 4.5 Configuration de la partie réseau :

Le commutateur ou le point d'accès sans-fil devra être configuré de manière à gérer des VLAN. Le premier sera réservé aux utilisateurs en quarantaine , et les autres seront réservé aux utilisateurs ayant été déclaré conforme par le serveur NPS . Dernier point de la configuration matérielle : activer le protocole 802.1x afin de rediriger l'authentification sur le serveur NPS.

Pour bien configurer le commutateur,Les étapes suivantes sont nécessaires :

### 4.5.1 Création des vlans

```
Client-RADIUS#vlan database
Client-RADIUS(vlan)#vlan 10 name Production
VLAN 10 added:
    Name: Production
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#vlan 11 name DRH
VLAN 11 added:
    Name: DRH
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#vlan 12 name Commercial
VLAN 12 added:
    Name: Commercial
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#vlan 13 name IT
VLAN 13 added:
    Name: IT
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#vlan 25 name MGT
VLAN 25 added:
    Name: MGT
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#vlan 30 name Gest
VLAN 30 added:
    Name: Gest
Client-RADIUS(vlan)#apply
APPLY completed.
Client-RADIUS(vlan)#exit
APPLY completed.
Exiting....
Client-RADIUS#
```

**Figure 4.12 – Création des différents vlans**

– Voir les diffétrents Vlan créés :

```
Client-RADIUS#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa2/0, Fa2/1, Fa2/2, Fa2/3
                                                Fa2/4, Fa2/5, Fa2/6, Fa2/7
                                                Fa2/8, Fa2/9, Fa2/10, Fa2/11
                                                Fa2/12, Fa2/13, Fa2/14, Fa2/15
10   Production                       active
11   DRH                              active
12   Commercial                       active
13   IT                               active
25   MGT                              active
30   Gest                             active
```

**Figure 4.13 – Vérification des différents vlans**

### 4.5.2 Configuration des interfaces des Vlan(Attribution d'adresses et Activation)

```
Client-RADIUS#
Client-RADIUS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#interface vlan 10
Client-RADIUS(config-if)#ip address 10.10.10.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#interface vlan 11
Client-RADIUS(config-if)#ip address 10.10.11.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#interface vlan 12
Client-RADIUS(config-if)#ip address 10.10.12.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#interface vlan 13
Client-RADIUS(config-if)#ip address 10.10.13.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#interface vlan 25
Client-RADIUS(config-if)#ip address 10.10.25.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#interface vlan 30
Client-RADIUS(config-if)#ip address 10.10.30.1 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
Client-RADIUS(config)#exit
Client-RADIUS#
*Mar  1 00:06:50.091: %SYS-5-CONFIG_I: Configured from console by console
Client-RADIUS#wr
Building configuration...
[OK]
Client-RADIUS#
```

**Figure 4.14 – Configuration des interfaces des Vlans**

### 4.5.3 Configuration de l'interface fa0/0

```
Client-RADIUS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#interface fa0/0
Client-RADIUS(config-if)#ip address 10.10.19.254 255.255.255.0
Client-RADIUS(config-if)#no shutdown
Client-RADIUS(config-if)#exit
```

**Figure 4.15 – Attribution d'une adresse à l'interface fa0/0**

### 4.5.4 Création des sous interface logiques (Encapsulation des vlan)

```
Client-RADIUS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#interface fa0/0.10
Client-RADIUS(config-subif)#encapsulation dot1q 10

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#interface fa0/0.11
Client-RADIUS(config-subif)#encapsulation dot1q 11
Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#interface fa0/0.12
Client-RADIUS(config-subif)#encapsulation dot1q 12
Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#interface fa0/0.13
Client-RADIUS(config-subif)#encapsulation dot1q 13
Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#interface fa0/0.25
Client-RADIUS(config-subif)#encapsulation dot1q 25
Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#interface fa0/0.30
Client-RADIUS(config-subif)#encapsulation dot1q 30
Client-RADIUS(config-subif)#no shutdown
Client-RADIUS(config-subif)#exit
Client-RADIUS(config)#exit
Client-RADIUS#
```

**Figure 4.16 – Encapsulation des vlan**

### 4.5.5 Activation du routage

il est nécessaire pour l'utilisation du routage,que la fonction soit activée avant de commencer la configuration. les tables de routage sont accessible via la commande :**show ip route**


FIGURE 4.17 – Activation du routage

## Test de routage inter Vlans

pour la vérification de routage inter-vlan ,on prend un seul exemple du vlan IT au vlan DRH,pour cela on lance une requette ping du vlan IT(10.10.13.12) vers le vlan DRH(10.10.11.13),le résultat est le suivant :

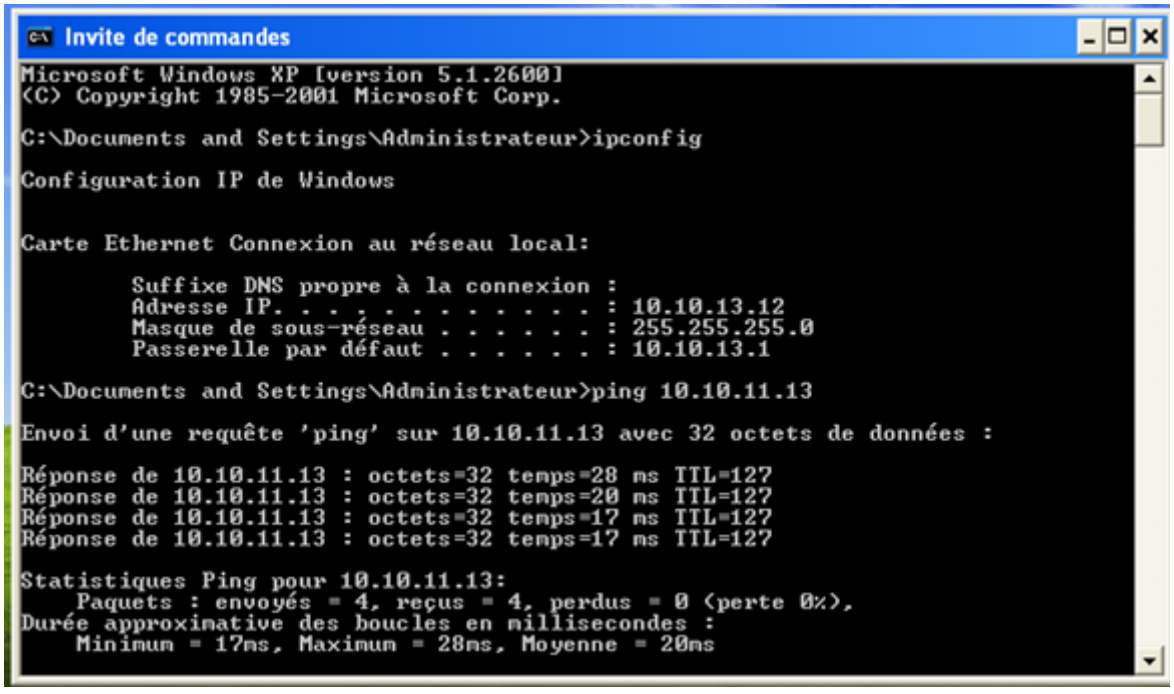


FIGURE 4.18 – Test de routage

### 4.5.6 Configuration du commutateur en tant que serveur DHCP

– **Le problème du DHCP**

Un problème rencontré durant l'implémentation de la solution aura été la gestion de l'adressage dynamique des machines situées sur les VLANs (via le DHCP). En effet comment faire pour que le serveur DHCP puisse alimenter tous les VLANs ? plusieurs solutions sont possibles : tagguer le serveur DHCP de façon à ce qu'il soit dans tous les Vlans ou faire du DHCP-Relay. Cette solution consiste à router les requêtes DHCP des clients vers le serveur et les réponses du serveur vers les clients et ce, même si le serveur ne se trouve pas dans le domaine de diffusion (dans le même VLAN).Cependant, dans le cadre de notre projet, le serveur DHCP est également le commutateur(Client-RADIUS) de ce fait, l'ensemble des machines est donc alimenté par le serveur DHCP.

– **Activation du DHCP**

Avant de commencer la configuration du commutateur pour qu'il serve de serveur DHCP,il est necessaire d'en activer le service.


FIGURE 4.19 – Activation du DHCP

– **Création des pools d'adresses**

Afin d'achever la configuration de commutateur pour le fonctionnement de celui-ci en tant que serveur DHCP,il faut maintenant configurer les pools d'adresses.

```
Client-RADIUS(config)#ip dhcp pool Production
Client-RADIUS(dhcp-config)#network 10.10.10.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.10.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
Client-RADIUS(config)#ip dhcp pool DRH
Client-RADIUS(dhcp-config)#network 10.10.11.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.11.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
Client-RADIUS(config)#ip dhcp pool Comercial
Client-RADIUS(dhcp-config)#network 10.10.12.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.12.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
Client-RADIUS(config)#ip dhcp pool IT
Client-RADIUS(dhcp-config)#network 10.10.13.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.13.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
```

FIGURE 4.20 – Création des pools d'adresses

- **network** :définition du réseau desservit par le dhcp ;
- **default-router** :adresse de routeur/passerelle envoyée aux clients ;
- **dns-server** :adresse du serveur DNS envoyée aux clients ;
- **domain-name** :nom de domaine au quel appartient les clients ;
- **lease** :durée du bail ip d'un client ;

```
Client-RADIUS(config)#ip dhcp pool MGT
Client-RADIUS(dhcp-config)#network 10.10.25.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.25.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
Client-RADIUS(config)#ip dhcp pool Guest
Client-RADIUS(dhcp-config)#network 10.10.30.0 255.255.255.0
Client-RADIUS(dhcp-config)#default-router 10.10.30.1
Client-RADIUS(dhcp-config)#domain-name cevital.local
Client-RADIUS(dhcp-config)#dns-server 10.10.19.1
Client-RADIUS(dhcp-config)#lease infinite
Client-RADIUS(dhcp-config)#exit
Client-RADIUS(config)#
```

FIGURE 4.21 – Création des pools d'adresses

– **Exclusion des pools d'adresses**

Une fois les pools définis,il reste à exclure les adressees ip des interfaces

```
Client-RADIUS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.10
Client-RADIUS(config)#ip dhcp excluded-address 10.10.11.1 10.10.11.10
Client-RADIUS(config)#ip dhcp excluded-address 10.10.12.1 10.10.12.10
Client-RADIUS(config)#ip dhcp excluded-address 10.10.13.1 10.10.13.10
Client-RADIUS(config)#ip dhcp excluded-address 10.10.25.1 10.10.25.10
Client-RADIUS(config)#ip dhcp excluded-address 10.10.30.1 10.10.30.10
```

FIGURE 4.22 – Exclusion des pools d'adresses

– **Phase de tests**

les différentes phases de configuration de DHCP étant terminée il faut désormais procéder à quelques tests ; pour se fair on va prendre l'exemple des Machines appartenant au vlan 10/13.

On peut fair le test de DHCP de deux manières :

1. on clique sur "démarrer","panneau de configuration","connexions réseau", "Support","Détails" puis "Réparer".

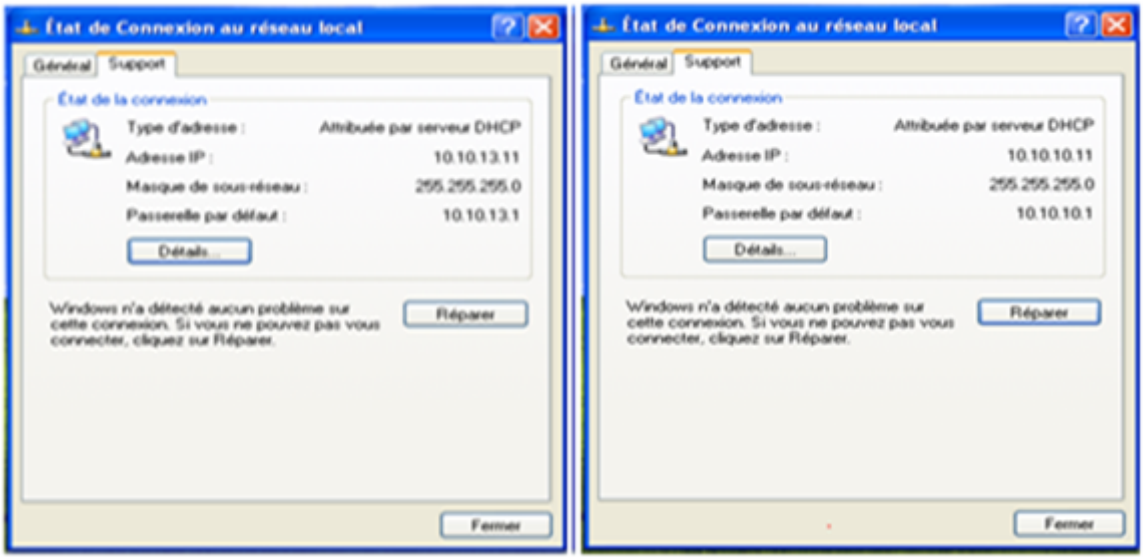


FIGURE 4.23 – Attribution automatique d'adresse IP

2. on clique sur "démarrer","Invite de commandes" puis on tape la commande "**ipconfig/release**" puis "**ipconfig/renew**"
   ipconfig/release :libère les connexions.
   ipconfig/renew :rétablit les connexions.

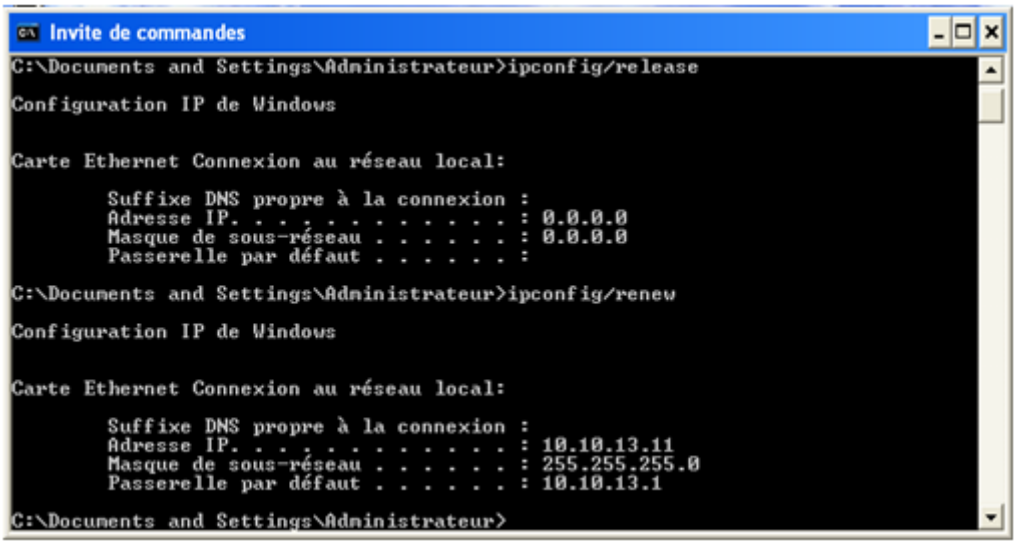


FIGURE 4.24 – Attribution automatique d'adresse IP

### 4.5.7 Configuration de l'authentification

1. **Authentification RADIUS 802.1x**
   - Activer le modèle AAA en utilisant la commande : "**aaa new model**"

```
Client-RADIUS#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#aaa new-model
Client-RADIUS(config)#
```

**FIGURE 4.25 – Activer le modèle AAA**

   - Créer une liste d'authentification "default" qui indique que l'authentification des utilisateurs se fera en 802.1x grâce au protocole RADIUS

```
Client-RADIUS(config)#aaa authentication dot1x default group radius
Client-RADIUS(config)#
```

**FIGURE 4.26 – L'authentification**

   - L'autorisation d'accès au réseau par le serveur RADIUS.

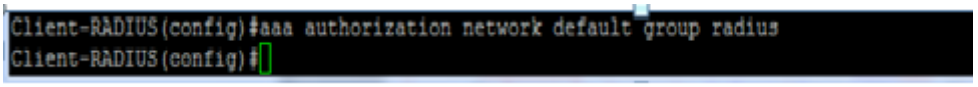


**FIGURE 4.27 – L'autorisation**

– Configurer les parametres du seveur RADIUS ainsi que la clé de cryptage partger entre le client radius(switch) et le serveur RADIUS.

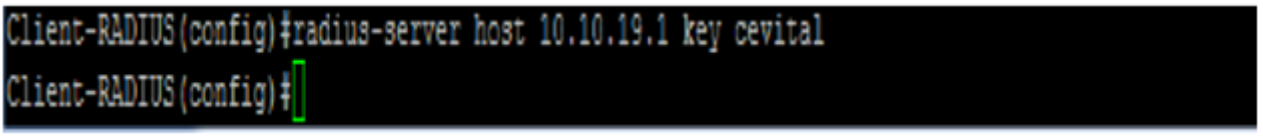


**FIGURE 4.28 – configuration de l'adresse IP de serveur RADIUS**

– Après,on active le protocole 802.1x sur le switch(Client-RADIUS)

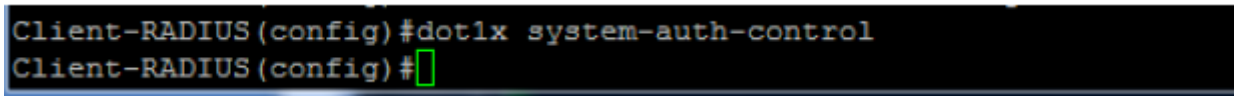


**FIGURE 4.29 – activation de protocole 802.1x au niveau de Client-RADIUS**

– Ensuite, on active le 802.1X sur le port relié à l'utilisateur :

```
Client-RADIUS(config)#interface fa1/1
Client-RADIUS(config-if)#switchport mode access
Client-RADIUS(config-if)#dot1x port-control auto
Client-RADIUS(config-if)#dot1x timeout quiet-period 20
Client-RADIUS(config)#dot1x timeout tx-period 30
Client-RADIUS(config)#exit
Client-RADIUS#
```

**FIGURE 4.30 – activation de protocole 802.1x sur le port de l'utilisateur**

**dot1x port-control auto :**Activer l'authentification 802.1x pour le port(dans notre cas fa1/1).

**dot1x timeout tx-period :** Le tepms d'attente(en secode)de client radius pour la réception d'une réponse(EAP) par le client d'accés.

**dot1x timeout quiet-period :** le temps d'attente de client radius(en seconde)pour renvoyer une requette d'identité au client en cas d'échec.

```
Client-RADIUS#debug aaa authentication
AAA Authentication debugging is on
Client-RADIUS#debug aaa authorization
AAA Authorization debugging is on
Client-RADIUS#debug aaa accounting
AAA Accounting debugging is on
Client-RADIUS#wr
Building configuration...
[OK]
Client-RADIUS#
```

**FIGURE 4.31 – Debug AAA**

Ces debugs montrent Les actions qui sont prises au cours de dialogue d'authentification .

2. **Authentification RADIUS**(Sécuriser l'accés a l'équipement)

   Lorsqu'un utilisateur souhaite se connecter à son équipement réseau, Switch ou Routeur Cisco en telnet ou ssh il doit spécifier un login et un mot de passe pour être autoriser à " rentrer ". En règle générale ce couple login/mot de passe est stocké en local sur l'équipement. Le compte utilisateur est créé à l'aide de la commande suivante :

   ClientRADIUS(config)username nom secret password.

On utilise le mot clef secret au lieu de password, pour chiffrer le mot de passe en MD5 (cypher 5) et non avec l'algorithme de chiffrement de Cisco (cypher 7) qui est beaucoup plus faible et facilement crackable. Cette méthode à l'avantage d'être simple et rapide à mettre en place. Mais lorsque plusieurs personnes susceptibles de se connectent aux équipements réseaux, devoir créer un compte pour chacun serait très contraignant. Sinon on peut mettre en place un login et un mot de passe unique pour tout le monde, mais c'est au niveau de la sécurité que ça craint. Pour remédier à cela, nous avons utiliser un **serveur RADIUS** qui sera chargé de valider l'authentification des utilisateurs qui souhaitent se connecter aux équipements réseaux. Nous avons utiliser un serveur sous Windows Server 2008 R2 avec le rôle NPS installé, comme serveur d'authentification radius.

Pour que le Switch/Routeur demande au serveur Radius d'authentifier les utilisateurs il faut spécifier quelques informations. Voilà les différentes étapes : On active dans un premier temps le model AAA de façon générale sur le Switch/Routeur par la commande **aaa new-model** les configurations ci-dessus

```
Client-RADIUS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Client-RADIUS(config)#aaa new-model
Client-RADIUS(config)#aaa authentication login default group radius local
Client-RADIUS(config)#aaa authentication enable default group radius enable
Client-RADIUS(config)#aaa authorization console
Client-RADIUS(config)#aaa authorization exec default group radius local
Client-RADIUS(config)#ip radius source-interface fa0/0
Client-RADIUS(config)#radius-server host 10.10.19.1 key cisco
Client-RADIUS(config)#line console 0
Client-RADIUS(config-line)#login authentication default
Client-RADIUS(config-line)#authorization exec default
Client-RADIUS(config-line)#line vty 0 15
Client-RADIUS(config-line)#login authentication default
Client-RADIUS(config-line)#authorization exec default
Client-RADIUS(config-line)#
```

**Figure 4.32 – Authentification RADIUS**

sont expliquées dans le tableau suivant :

| Commande | Explication |
|---|---|
| **-aaa authentication login default group radius local**<br>**-aaa authentication enable default group radius enable** | Nous avons ici crée une liste d'authentification appelé default ; Cette liste d'authentification va se servir des serveurs Radius pour pouvoir authentifier les utilisateurs. |
| **-aaa authorization console**<br>**-aaa authorization exec default group radius local** | indiquent les privilèges d'accès des utilisateurs à la console d'équipement par le serveur RADIUS. |
| **-radius-server host 10.10.19.1 key Cisco** | Spécifier l'adresse IP de serveur d'authentification RADIUS et la clé partagée entre le serveur et le client-RADIUS. |
| **-line console 0**<br>**-login authentication default authorization exec default** | Sécuriser l'accès en console à l'équipement par un nom d'utilisateur suivant les privilèges d'accès. |
| **-Line vty 0 15**<br>**-Login authentication default**<br>**-Authorization exec default** | Sécuriser l'accès à distance à l'équipement en utilisant un nom et mot de passe d'utilisateur suivant les privilèges d'accès. |

FIGURE 4.33 – **Authentification RADIUS**

## 4.6 Configuration de serveur :

### 4.6.1 Attribution d'une adresse Ip statique au serveur

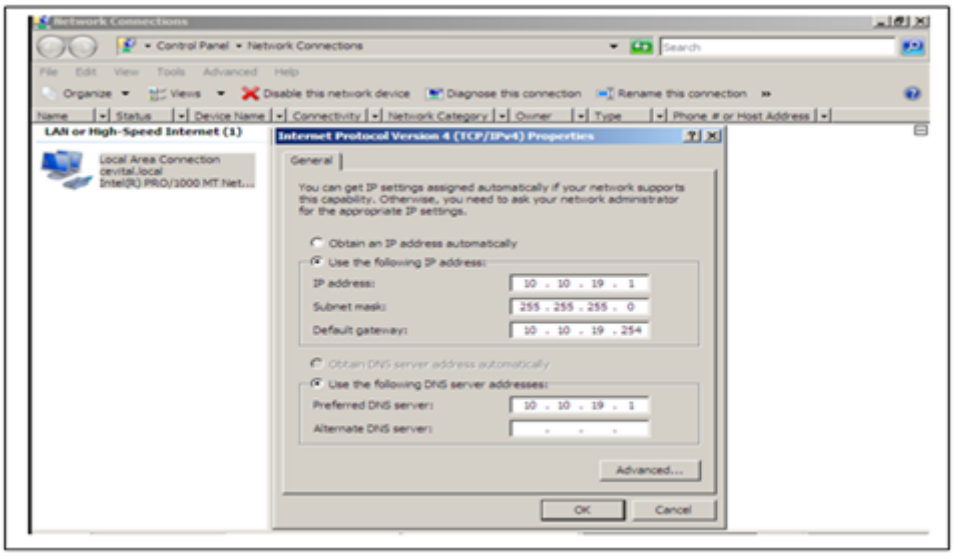


**Figure 4.34 – Attribution d'une adresse statique au serveur**

### 4.6.2 Création des groupes et des utilisateurs dans l'Active Directory

– Pour créer un groupe,un clique droit sur notre domaine "cevital.local", "new" puis "group"

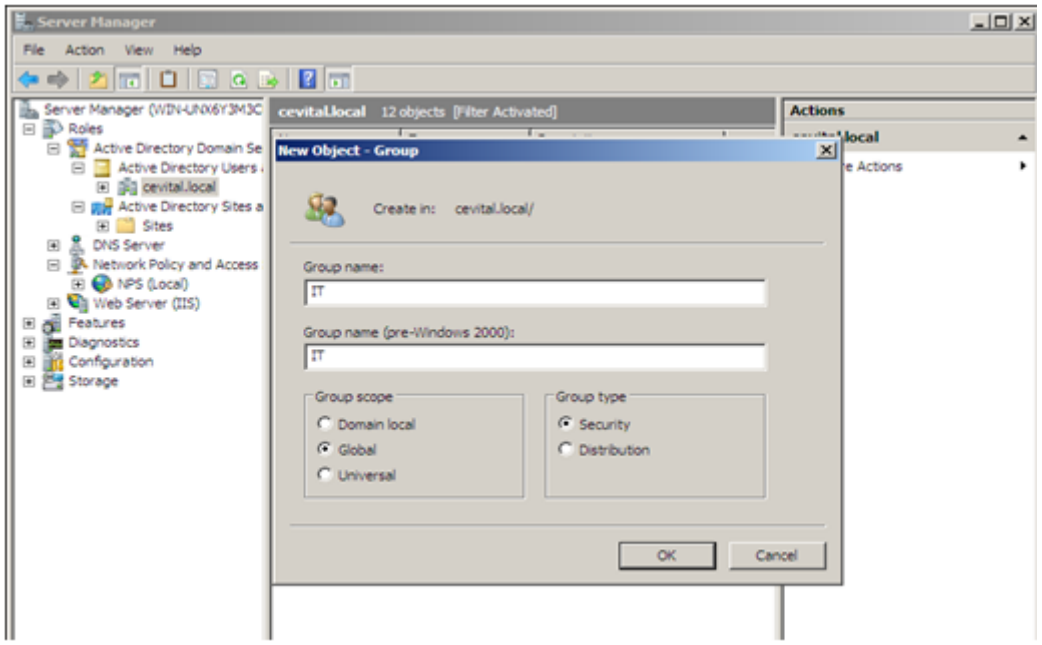


**Figure 4.35 – Création de groupe IT**

– Pour créer un utilisateur, un clique droit Sur le domaine "cevital.local" , "New user" (nouveau utilisateur)

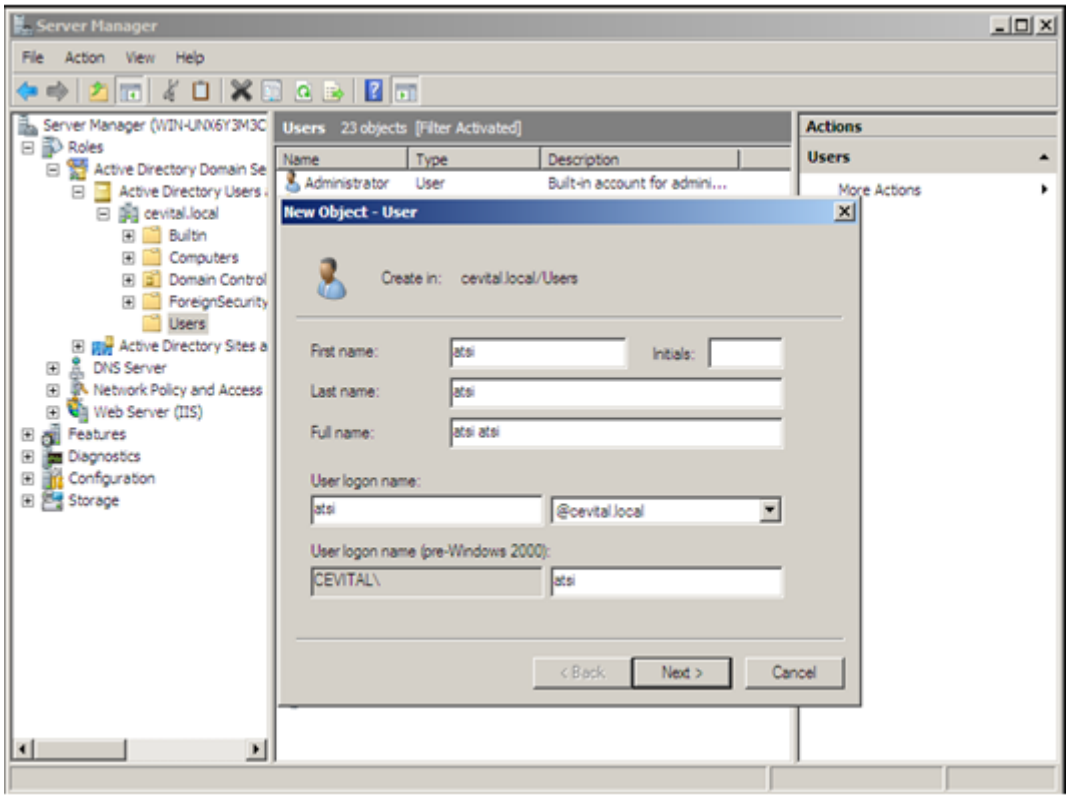


**Figure 4.36 – Création d'un utilisateur**

– "Après avoir cliqué sur "Next",on doit introduire le mot de passe ,ainsi cocher les deux cases "User cannot change password"(l'utilisateur ne peut pas changer le mot de passe) et "Password never expires" (le mot de passe n'expire jamais).

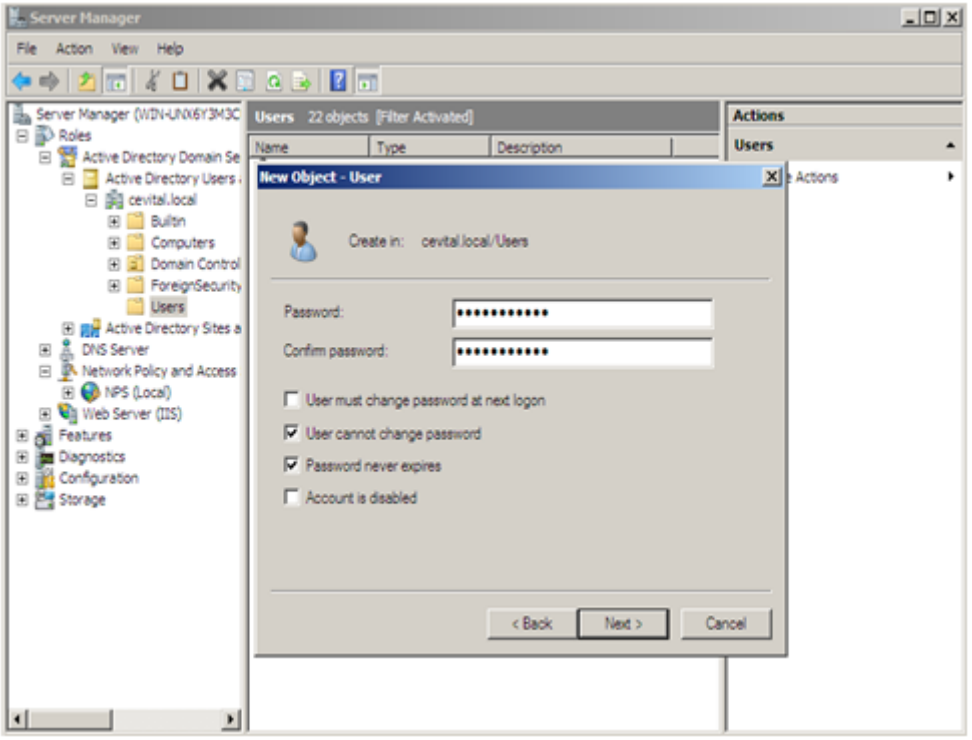


**Figure 4.37 – introduction de mot de passe de utilisateur**

Puis on fait un click droit sur l'utilisateur "atsi", dans propriétés on va dans l'onglet **Dial-in** Puis dans **Network Access Permission on** coche **Control access through NPS Network policy**.

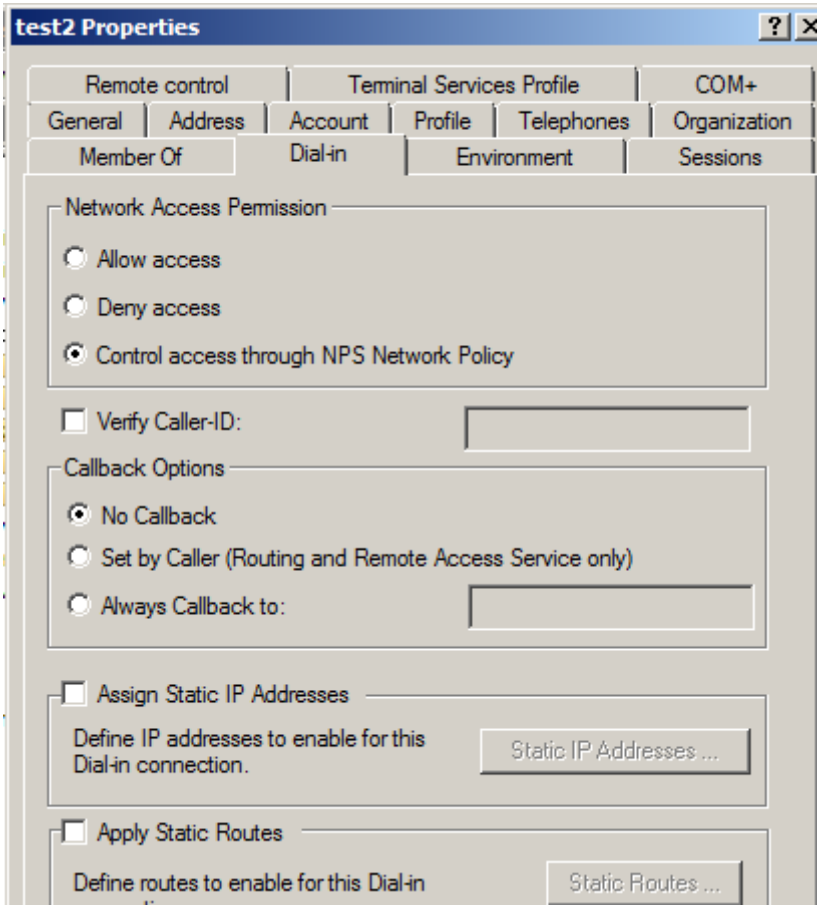


FIGURE 4.38 – Permission d'accés au réseau

On suit les mémes étapes pour la création des autres groupes et utilisateurs.

– par la suite,on va associer les utilisateurs aux groupes.
  la figure suivante montre l'ajoute de l'utilisateur "atsi" au groupe "IT" ,pour se fair un clique droit sur "atsi", "add to goup" et on spécifie le groupe :

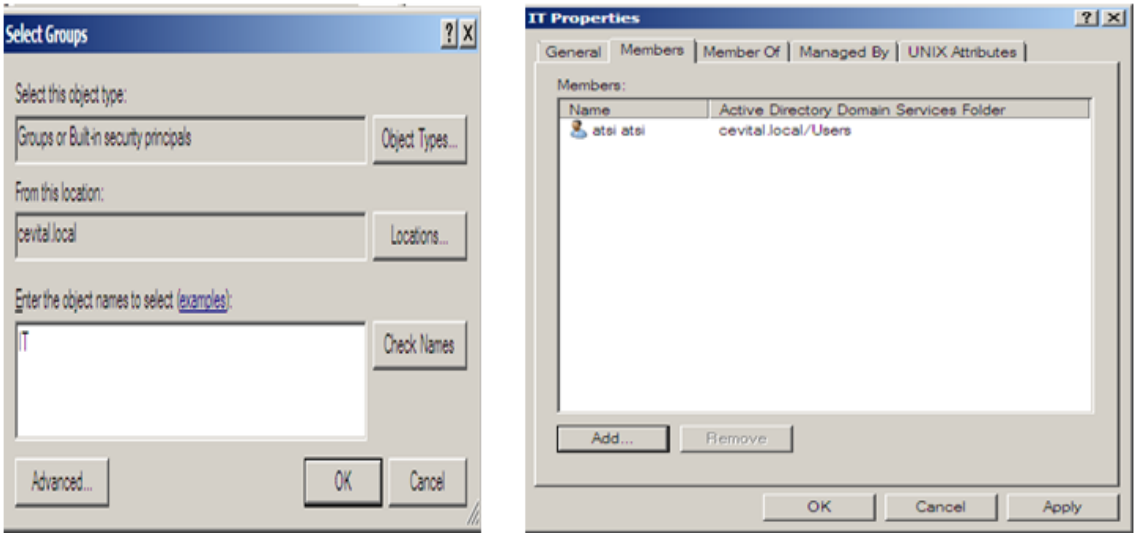


**Figure 4.39 – Associer l'utilisateur atsi au groupe IT**

### 4.6.3 Installation de service "Network Policy and Access Services"( Services de Stratégie et d'accés réseau)

Le serveur NPS permet de créer et de mettre en oeuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification et l'autorisation des demandes de connexion. pour l'installation, on procède comme suit :

Dans la console server manager-> Roles->add roles-> Network Policy and Access Services->Next->côcher (Network Policy Server) "NPS" -> install.

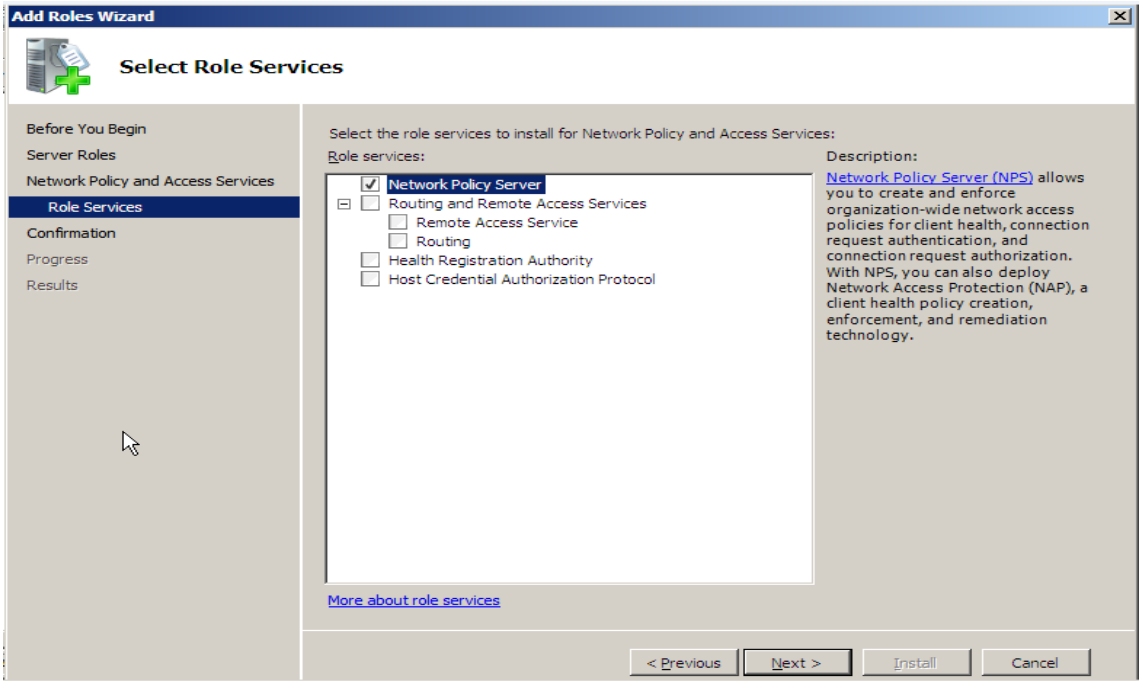


**FIGURE 4.40 – Selection de service "Network Policy Server"**

À la fin de l'installation,la console "NPS" est ajoutée :

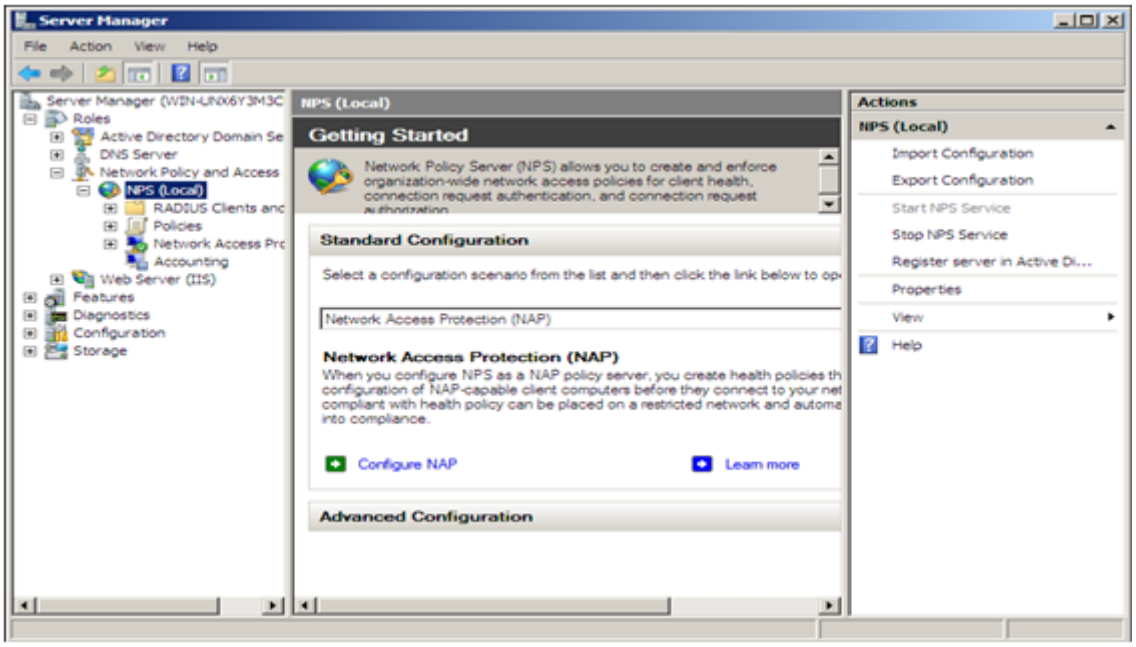


**Figure 4.41 – Console d'administration NPS**

### 4.6.4 configuration de "NPS" en tant que serveur RADIUS

Lorsque on configure le serveur NPS (Network Policy) comme un serveur RADIUS , NPS effectue l'authentification, autorisation et la gestion des demandes de connexion pour le domaine. pour la configuration de ce serveur les étapes suivantes sont necessaires :

- **Inscrire le serveur NPS dans le domaine :** Lorsque le serveur NPS est membre d'un domaine des services de domaine Active Directory (AD DS), NPS procède à l'authentification en comparant les informations d'identification de l'utilisateur qu'il reçoit des serveurs d'accès réseau à celles qui sont stockées pour le compte d'utilisateur dans les services de domaine Active Directory (AD DS). Il procède également à l'autorisation des demandes de connexion en utilisant la stratégie réseau et en vérifiant les propriétés de numérotation du compte d'utilisateur dans les services de domaine Active Directory (AD DS).
  Pour que NPS soit autorisé à accéder aux informations d'identification et aux propriétés d'accès distant des comptes d'utilisateurs dans les services de domaine Active Directory (AD DS), le serveur exécutant NPS doit être inscrit dans ces derniers. pour se fair Cliquez avec le bouton droit sur NPS (local), puis cliquez sur Inscrire un serveur dans Active Directory.
  Lorsque la boîte de dialogue "Inscrire un serveur dans Active Directory" s'ouvre, cliquez sur OK.

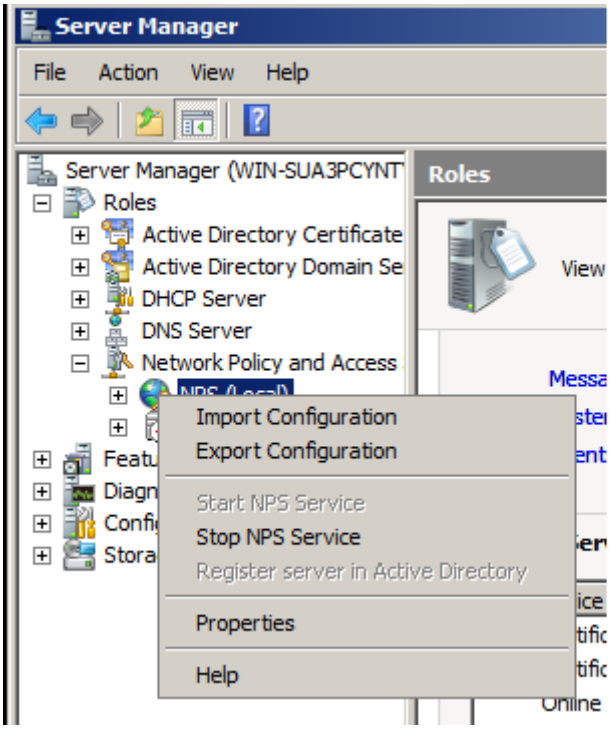


**FIGURE 4.42 – Inscrire le serveur NPS dans le domaine**

une fois le serveur inscrit dans le domaine,une interface qui indique que le serveur NPS est authorisé à lire les propriétés des utilisateurs de domaine Apparaît .

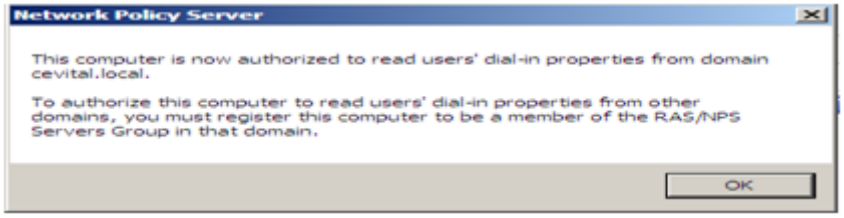


**FIGURE 4.43 – Inscription du serveur NPS dans le domaine**

– **Configuration de "NPS" en tant que client RADIUS** : les clients RADIUS sont des serveurs d'accès réseau, tels que les points d'accès sans fil, serveurs de réseau privé virtuel (VPN),commutateurs et serveurs d'accès distant. pour la configuration du client radius, allez à NPS->RADIUS Clients and Servers-> RADIUS Clients->new :

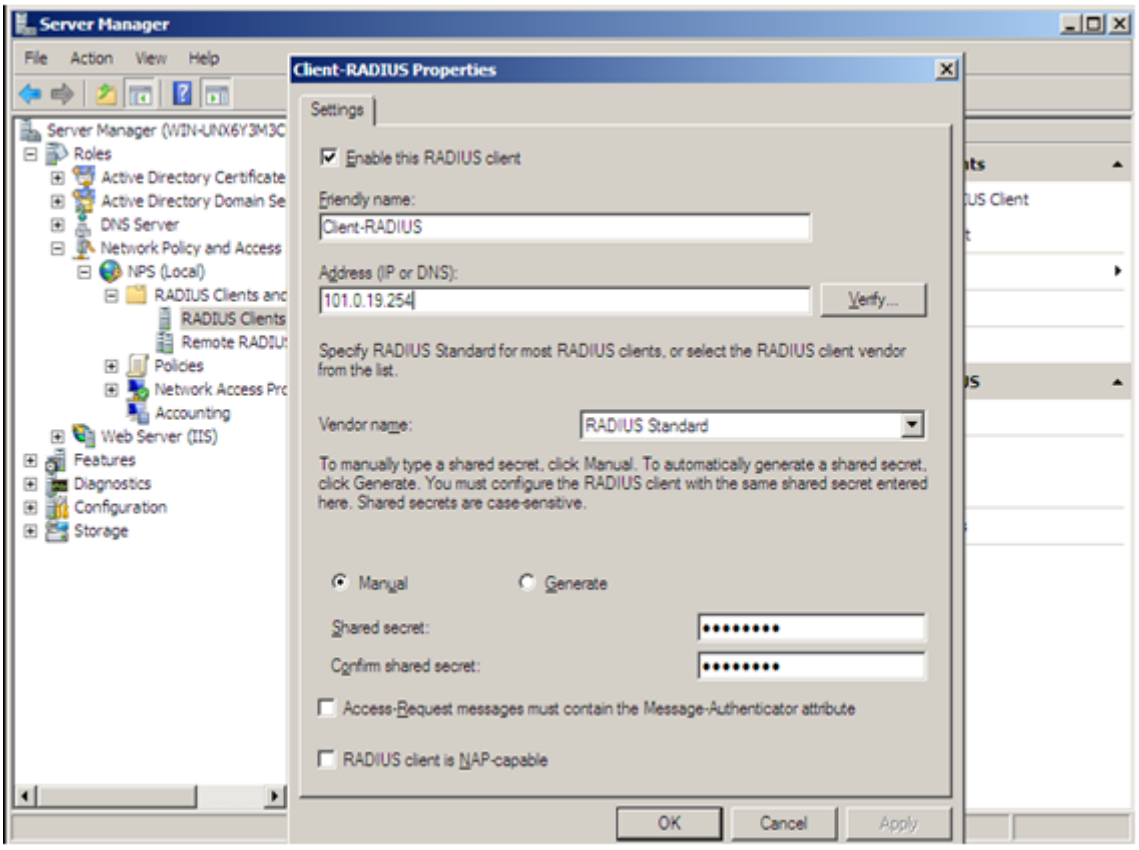


**FIGURE 4.44 – création de client RADIUS**

Comme indique La figure ci-dessus, le nom convivial de client RADIUS est "Client-RADIUS", l'adresse IP :"10.10.19.254" est l'adresse attribuée au switch "Client-RADIUS". Le secret partagé ' est la clé de chiffrement partagée entre le client RADIUS et le serveur RADIUS,le même que celui qu'on a configuré au niveau de switch(radius-server host 10.10.19.1 Key cisco).

– **Planifier les stratégies de réseau :**

les stratégies de réseau sont utilisés par NPS pour déterminer si les demandes de connexion reçus des clients RADIUS sont autorisés. NPS utilise également les propriétés de numérotation du compte d'utilisateur pour procéder à une détermination de l'autorisation. Dans la mesure où les stratégies de réseau sont traités dans l'ordre dans lequel ils apparaissent dans le composant logiciel enfichable NPS, envisagez de placer vos stratégies plus restrictifs tout d'abord dans la liste des stratégies. Pour chaque demande de connexion, NPS tente de faire correspondre les conditions de la stratégie avec les propriétés de demande de connexion. NPS examine chaque stratégie de réseau dans l'ordre jusqu'à ce qu'il trouve une correspondance. S'il ne trouve pas de correspondance, la

demande de connexion est rejetée. dans ce qui suit ;on va créer deux stratégies réseau.une stratégie pour authentifier l'acces à l'équippement et l'autre pour l'authentification 802.1x.

les étapes de configuration des stratégies réseau sont les suivantes :

1. **Première stratégie :authentification 802.1x**

   D'abord, on choisit le serveur RADIUS pour les connexions 802.1x câblés ou sans fils

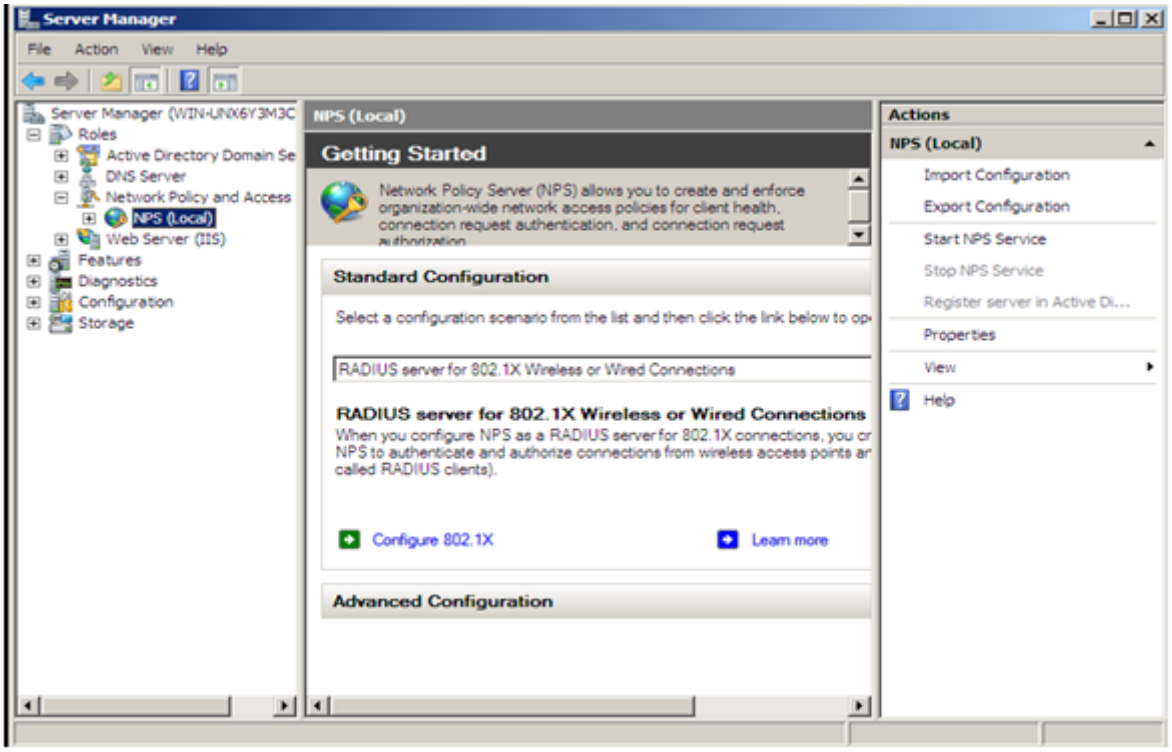


**Figure 4.45 – NPS pour les connexions 802.1x câblés et sans fil**

Après,on sélectionne le type de connexion 802.1x câblée .

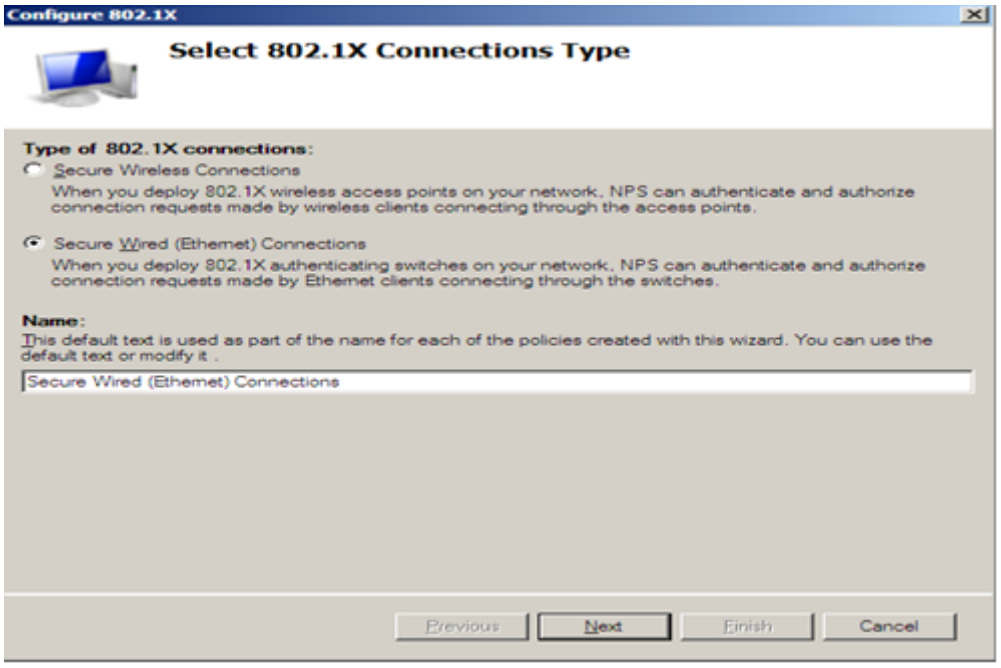


**Figure 4.46 – type de connexion 802.1X**

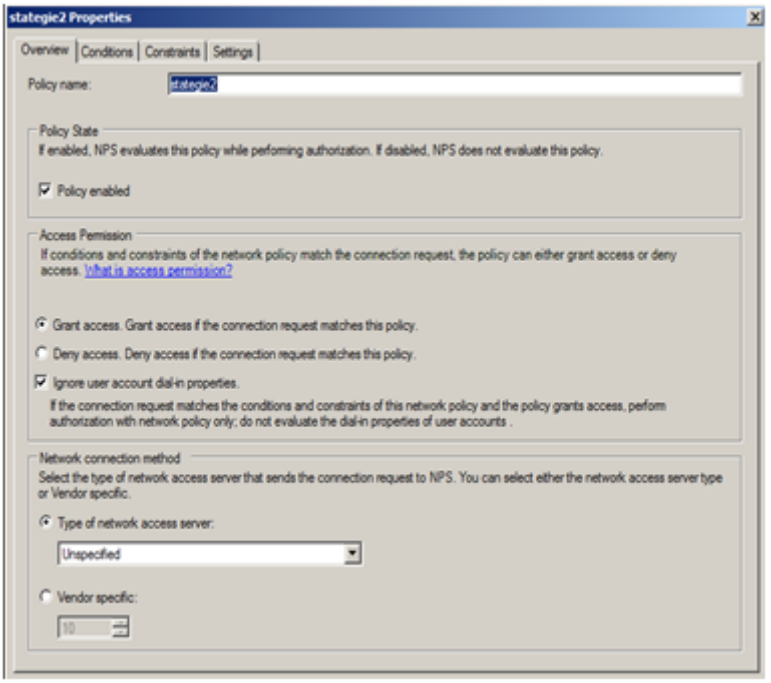


**Figure 4.47 – Vue d'ensemble de la stratégie**

Ensuite, on ajoute notre client RADIUS "Client-RADIUS"

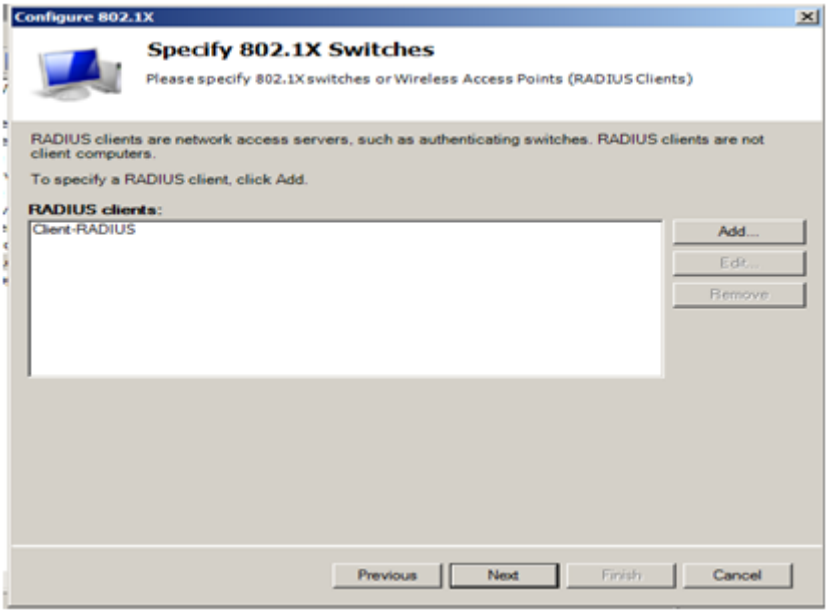


FIGURE 4.48 – Ajout de client RADIUS

Après avoir ajouté le client RADIUS, on doit spécifier le groupe d'utilisateurs "IT" pour cette stratégie

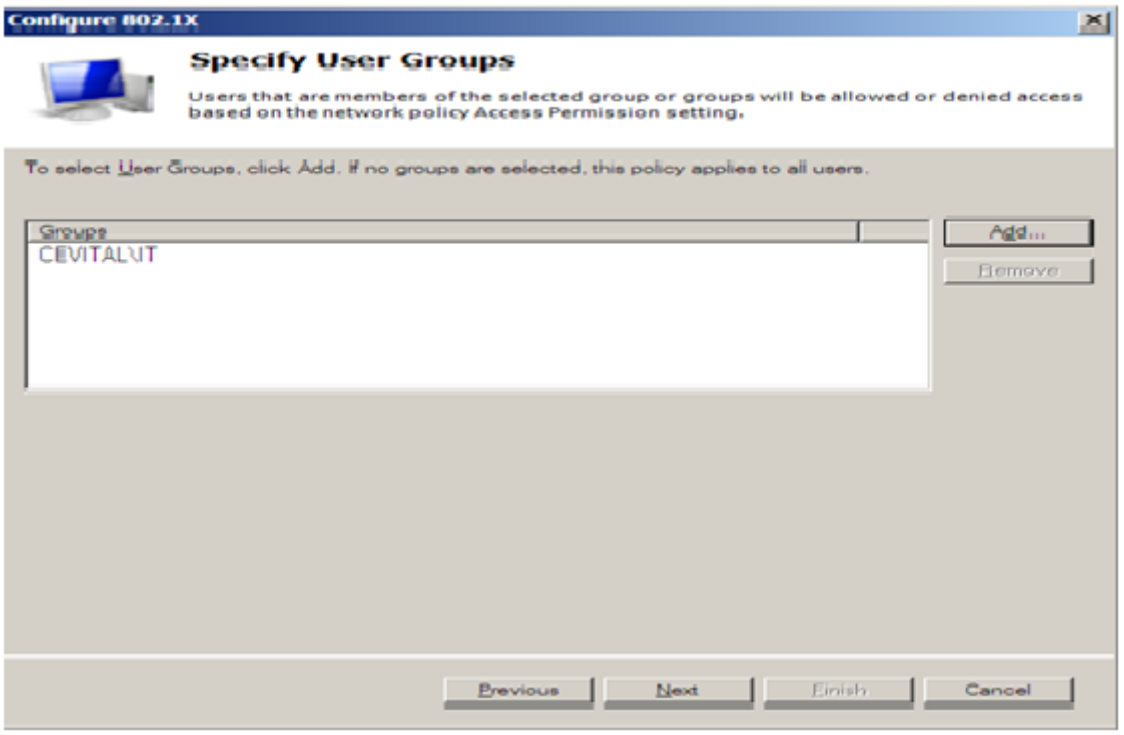


FIGURE 4.49 – Spécification de groupe d'utilisateurs pour la connexion 802 .1x câblée

Après la création de la stratégie NPS 802.1x pour les connexions câblées, on configure les conditions tel que :

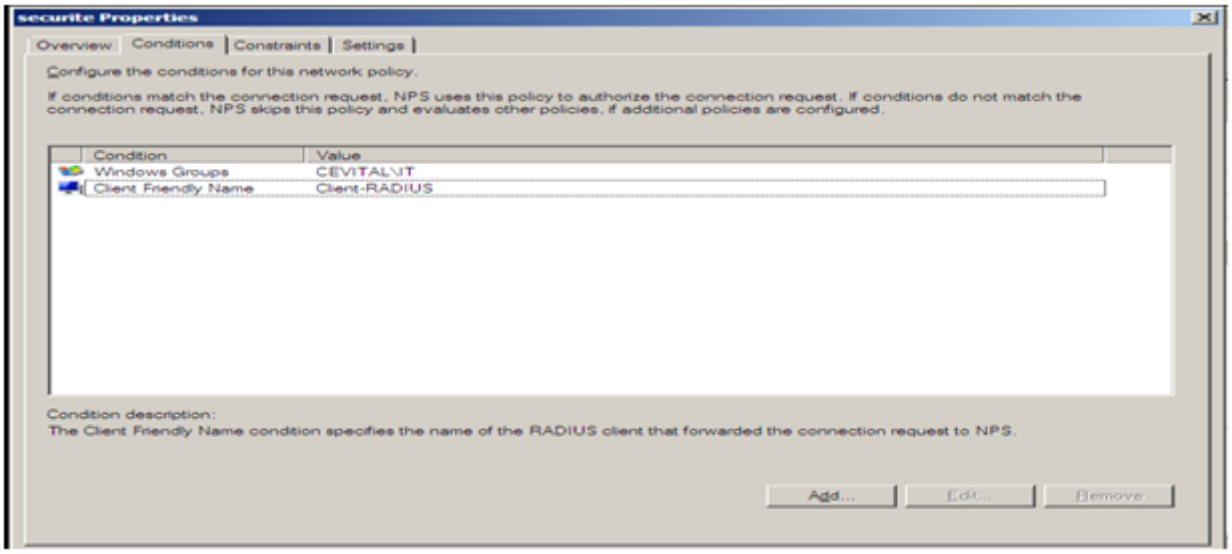


FIGURE 4.50 – Conditions de stratégie réseau

Dans l'onglet "contraints" (contraintes), on a choisi les méthodes d'authentification .

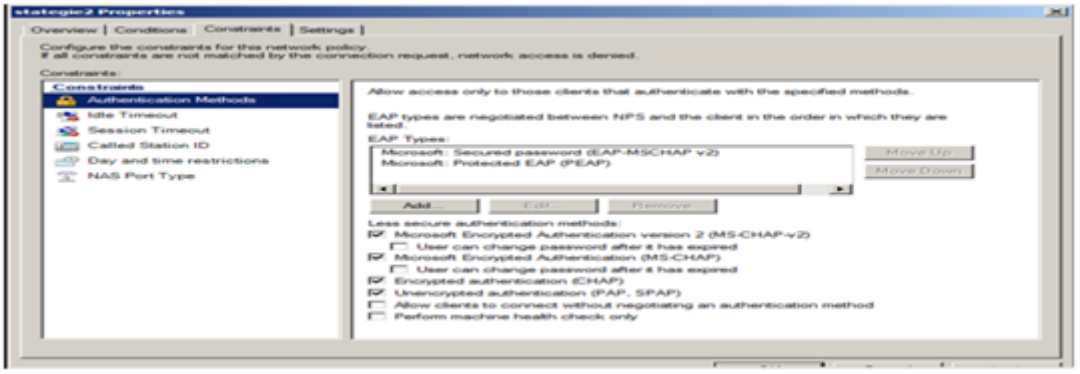


FIGURE 4.51 – Choix de méthodes d'authentification

Dans l'onglet " Settings ", " RADIUS Attributes ", "vendor specific",on ajoute l'attribut spécifique au fournisseur" Cisco-AV-Pair " .

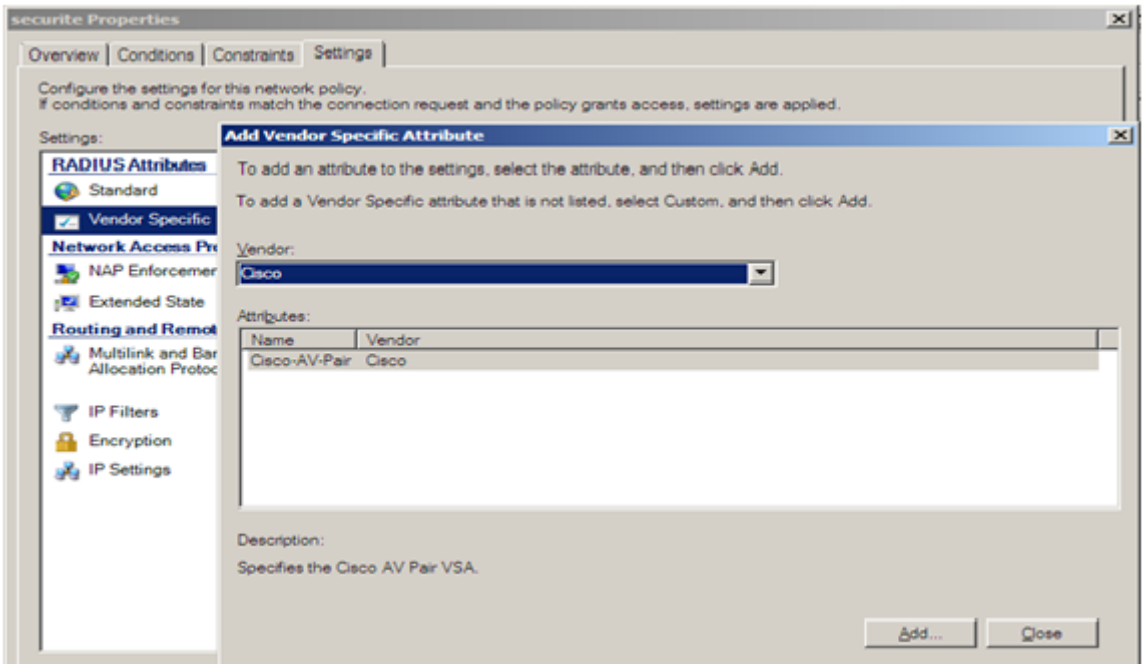


FIGURE 4.52 – Ajout d'un attribut spécifique au fournisseur

Après l'ajout de l'attribut spécifique au fournisseur, on précise le niveau d'accès de l'utilisateur comme indique la figure suivante :

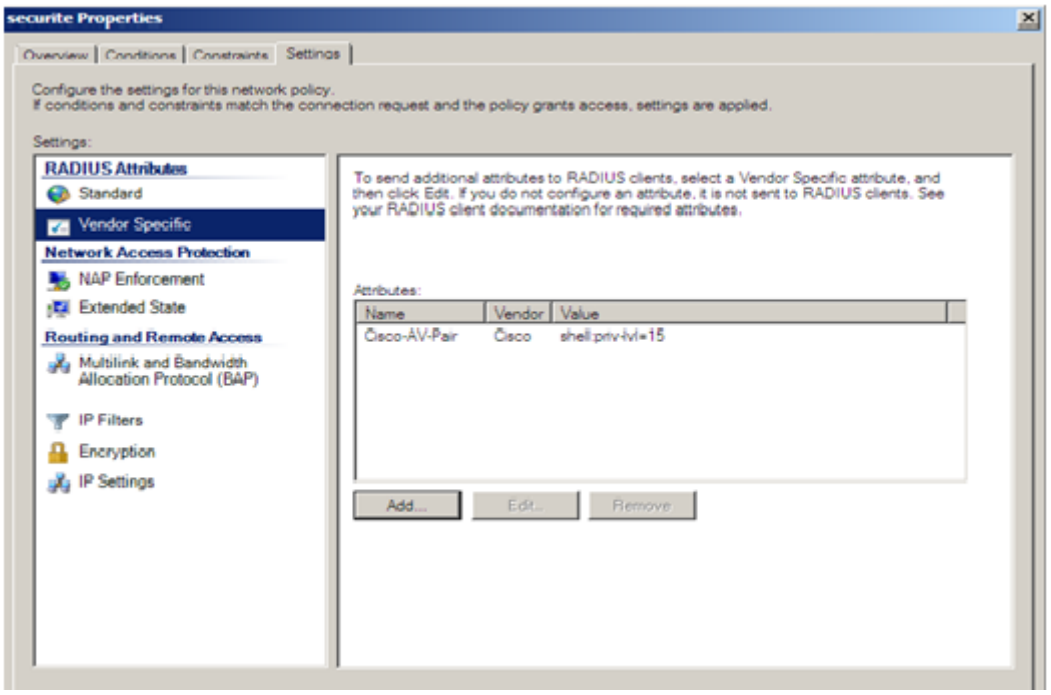


FIGURE 4.53 – Ajout d'attributs spécifique au fournisseur

Dans le même onglet " Setting " ->" RADIUS Attributes " ->" Standard ", on ajoute les attributs : Tunnel-Medium-Type, Tunnel-Preference, Tunnel-PVT-Group-ID (indique l'identifiant de vlan a attribuer à l'utilisateur aprés authentification),et l'attribut " tunnel-Type ".

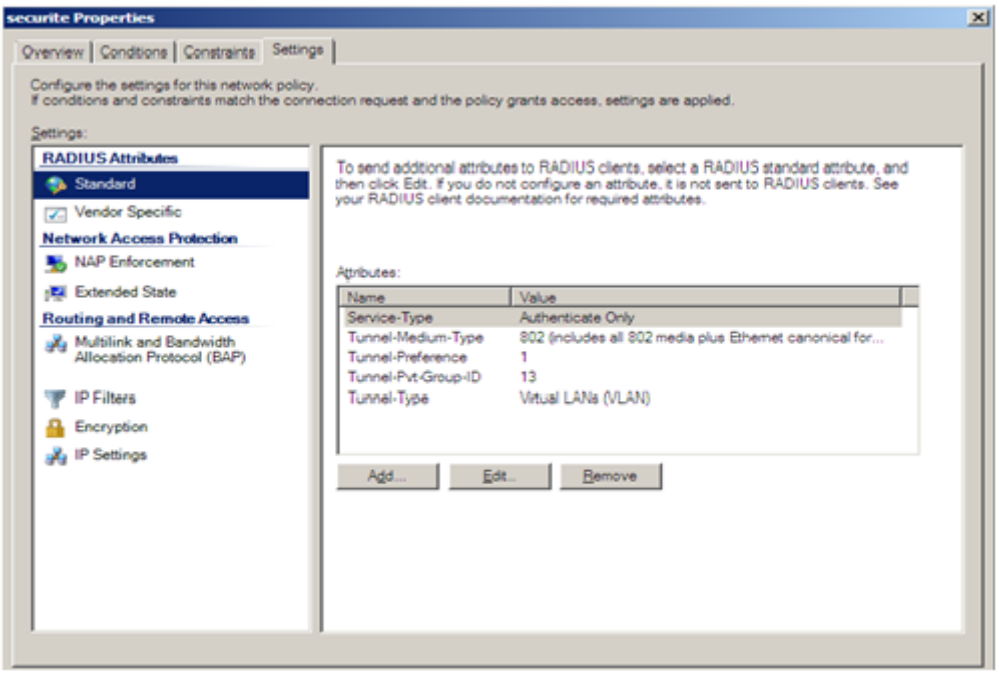


FIGURE 4.54 – Ajout d'attributs

2. **Deuxième stratégie :authentification RADIUS**

   pour créer cette stratégie,on fait un clic droit sur Network policies,"nouvelle stratégie",on indique le nom de la stratégie (stratégie1) et pour les conditions on ajoute les mêmes conditions que la stratégie Précédente (le groupe au quel doit appartenir l'utilisateur et le nom convivial de serveur d'accès).pour les méthodes d'authentification c'est aussi les mêmes que la stratégie Précédente.

   la configuration des paramètres :

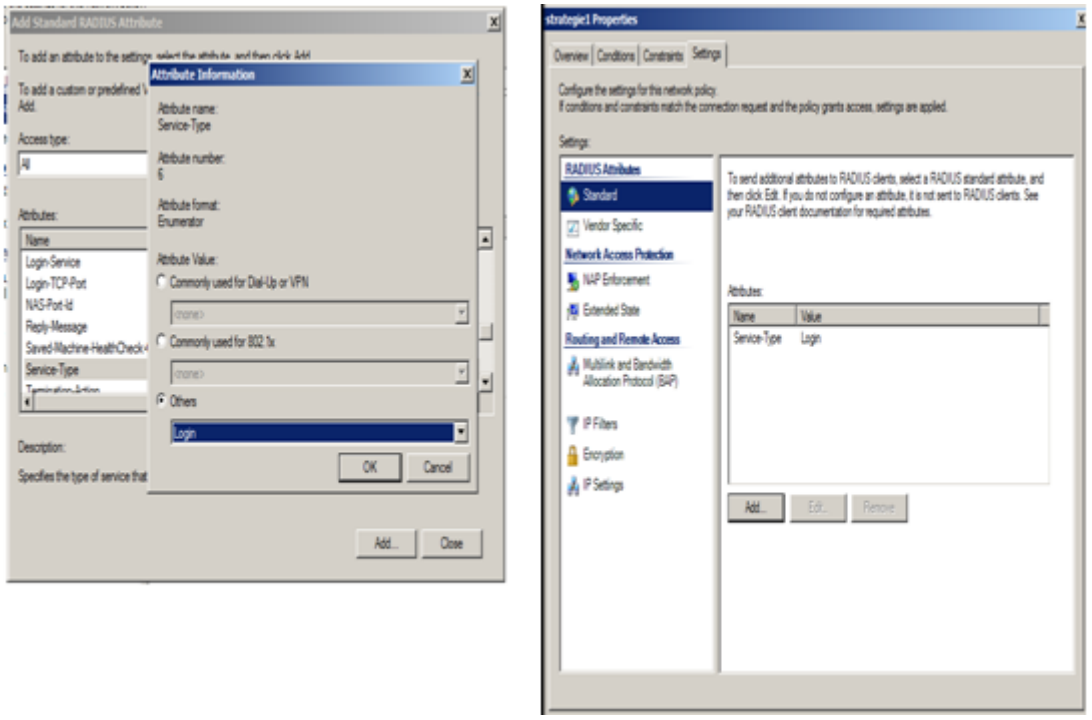


FIGURE 4.55 – Ajout d'un attribut spécifique au fournisseur

La configuration de notre serveur RADIUS sous Windows server 2008 est achevée, alors on passe à la configuration de la machine de l'utilisateur (client XP).

## 4.7 Configuration de client d'accès (Windows XP)

Pour la configuration de la machine de l'utilisateur (Cliente) "XP ", on a suivie les étapes suivantes :

– **Etape1 :**

activer le service de configuration automatique de réseau câblé, qui est désactivé par défaut. Pour cela on doit taper " services.msc " dans le champ de recherche présent dans la barre des tâches, On clique sur le service " configuration automatique du réseau câblé " ,"automatique" puis "démarrer".

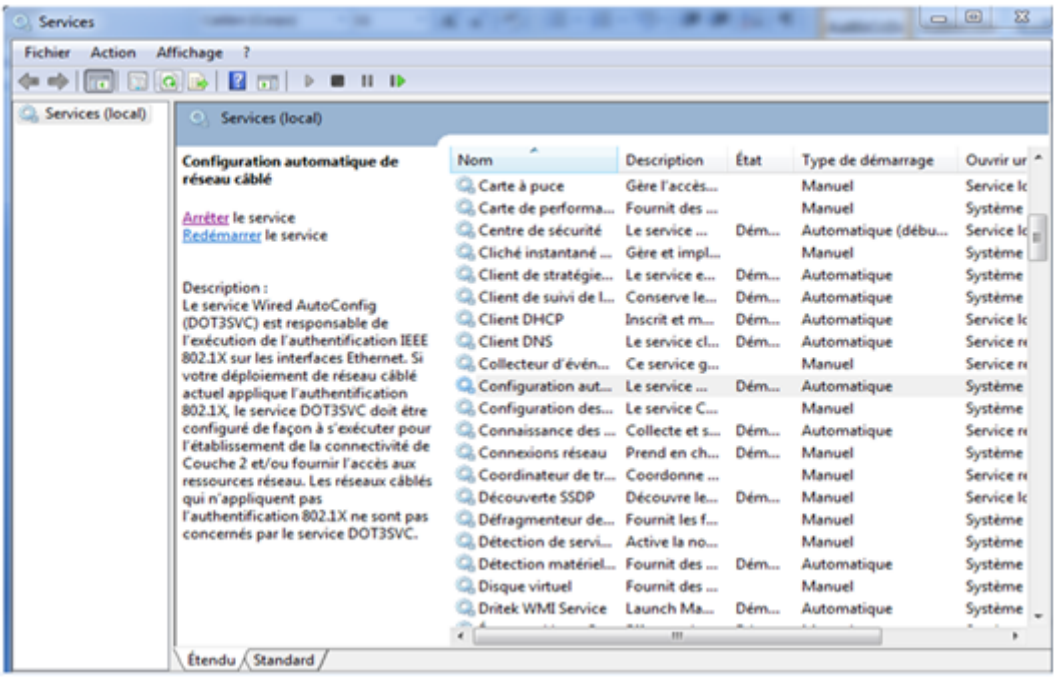


FIGURE 4.56 – Démarrage de service " Configuration automatique de réseau câblé"

- **Etape 2 :** Pour ouvrir Connexions réseau, cliquez sur le bouton Démarrer , sur Panneau de configuration, sur Réseau et Internet, sur Centre réseau et partage, puis sur Gérer les connexions réseau. Cliquez avec le bouton droit sur la connexion pour laquelle vous souhaitez activer l'authentification 802.1X, puis cliquez sur Propriétés. on clique sur l'onglet " Authentification " -> " Activer l'authentification IEEE 802.1X" puis on sélectionne "EAP protégé (PEAP) " comme Type EAP
- **Etape 3 :** Cliquer sur Propriétés du Type EAP. Décocher "Valider le certificat du serveur" puis Sélectionner "EAP-MSCHAP v2" comme méthode d'authentification et cliquer sur "Configurer" pour décocher "Utiliser automatiquement mon nom d'ouverture de session et mon mot de passe Windows".

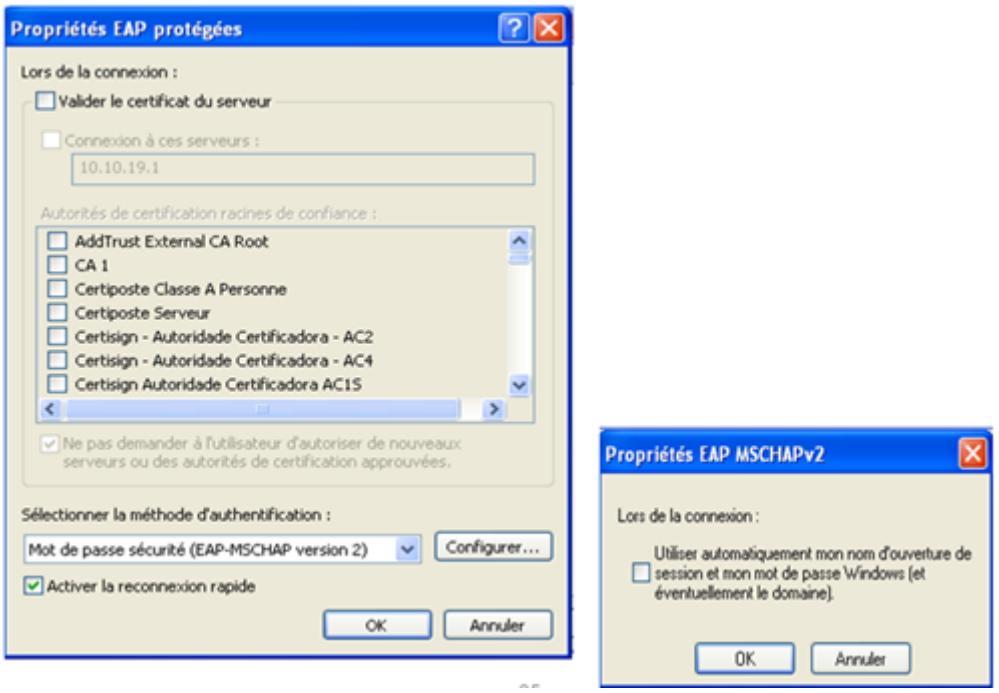


FIGURE 4.57 – Sélection de méthode d'authentification " EAP-MSCHAP v2 "

– **Etape 4 : L'ajout de la machine au domaine**
"démarrer",un clic droit sur"poste de travail","propriétés","Nom de l'ordinateur","Modifier",indiquer le nom de domaine(cevital.local) puis OK.

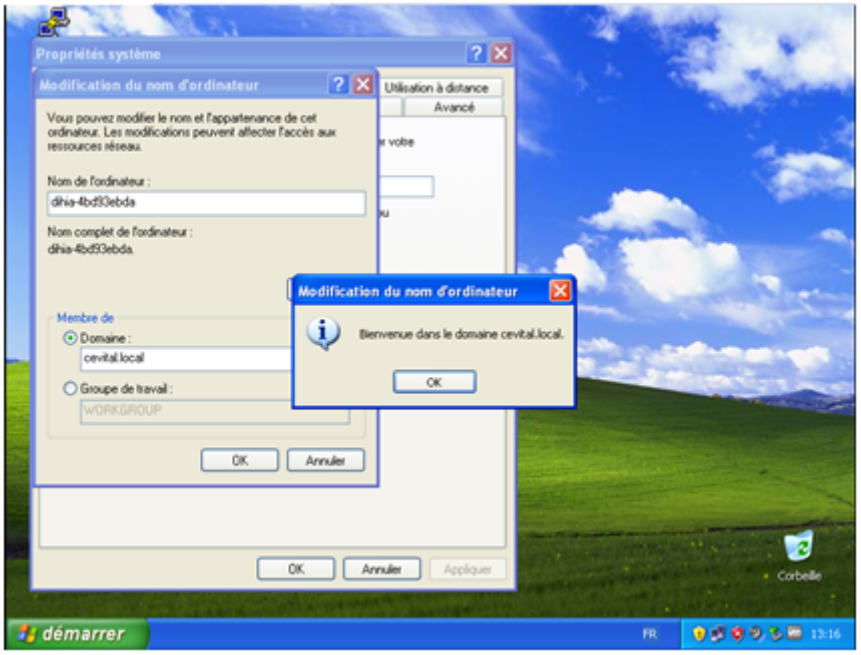


FIGURE 4.58 – l'ajout de la machine au domaine

## 4.8 Tests

### 4.8.1 Authentification RADIUS 802.1x

– Effectuer les tests sur le serveur d'accès :
Comme on la indiqué précédemment, la stratégie NPS nommée **stratégie2** qu'on a créer pour l'authentification 802.1x, n'authentifie et n'autorise que les utilisateurs appartenant aux vlan IT d'accéder au réseau.

– **Vérifiant alors les utilisateurs qui sont membres de vlan IT de notre domaine :**
"Server Manager","Roles","Active Directory User and Computers","cevital.local", IT,Members.

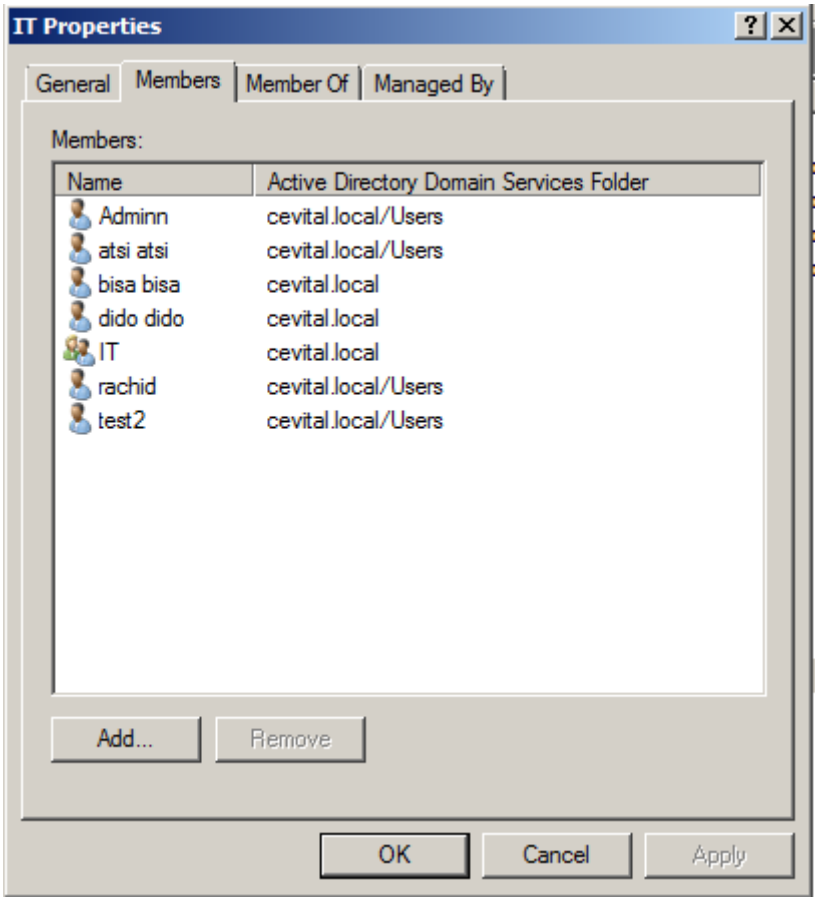


FIGURE 4.59 – Membres de vlan IT

– **Tests d'authentification 802.1x des utilisateurs appartenant au vlan IT**

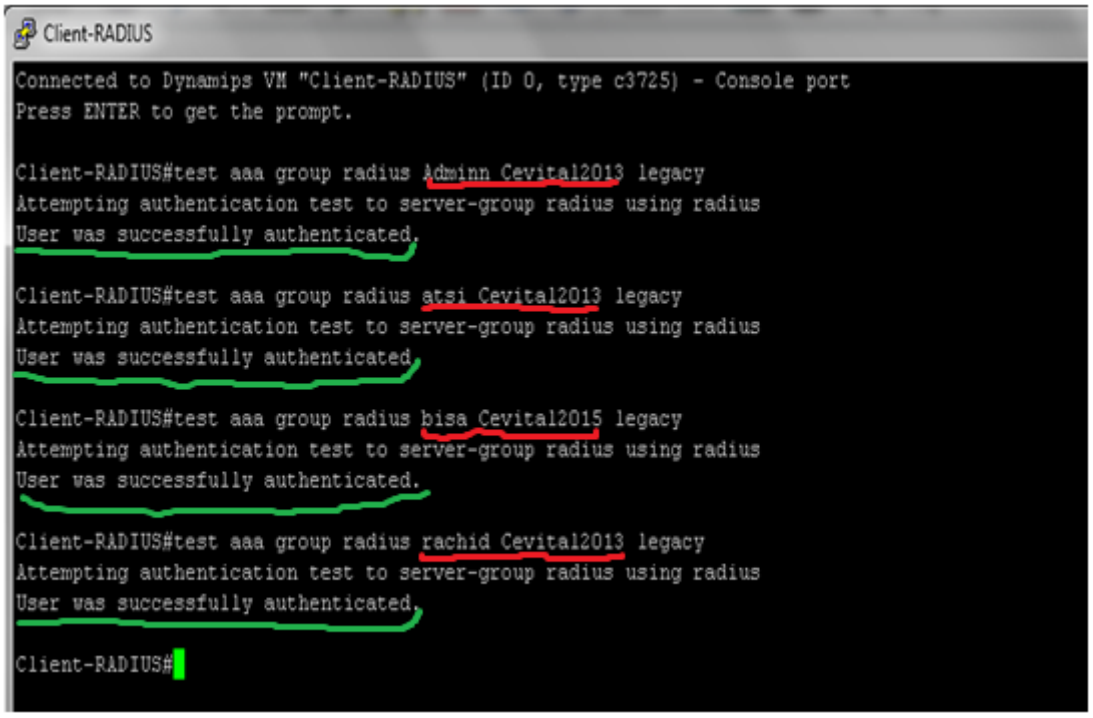


FIGURE 4.60 – Test d'authentification 802.1x

– **Exemple d'authentification 802.1x d'un utilisateur n'appartenant pas au vlan IT**

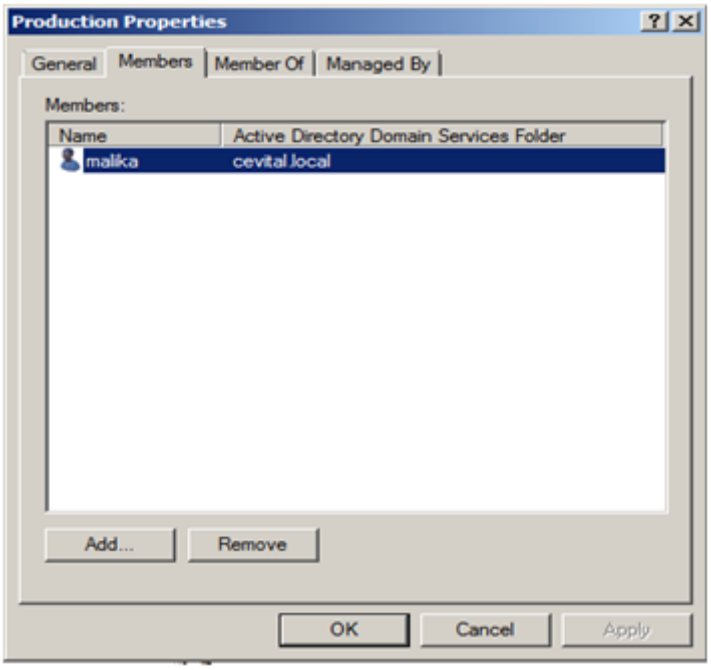


FIGURE 4.61 – Utilisateur n'appartenant pas au vlan IT

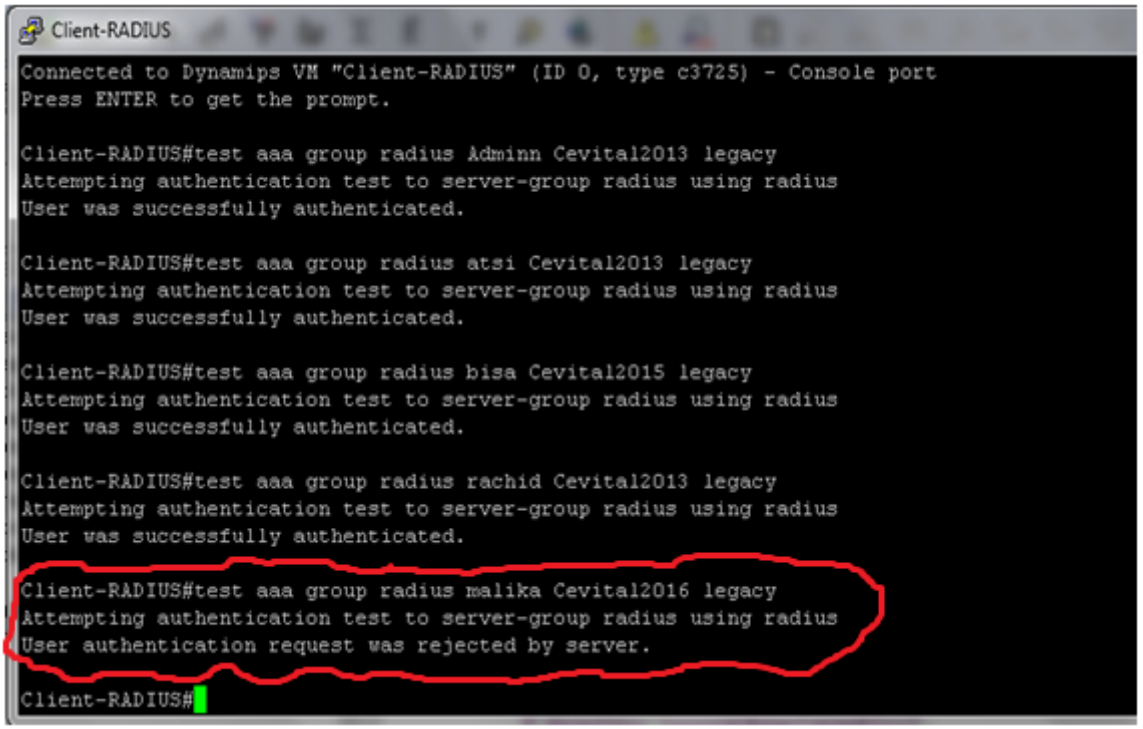


FIGURE 4.62 – Test d'authentification 802.1x

– **Vérification du Fonctionnement du protocole avec Wireshark**

**Wireshark** : c'est un outil de capture et d'analyse de paquets réseau Open Source et multi-protocole. Destiné aux administrateurs réseau et aux développeurs, Wireshark (anciennement appelé Ethereal) est une référence en matière d'analyse des transactions réseau. Cet outil puissant supporte plusieurs centaines de protocoles et dispose de fonctions de filtrage avancées pour la capture et l'interprétation des données[21].

pour ouvrir Wireshark,un clic droit sur les bulles vertes des interface sous GNS3,

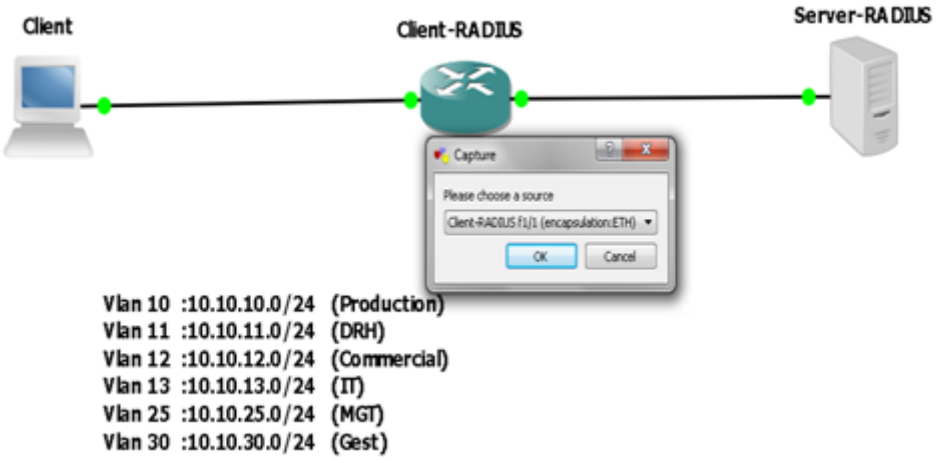


FIGURE 4.63 – Wireshark sous GNS3

faites OK, puis un clic droit sur la bulle,"Start wirechark" .

**Analyse des transaction réseau de l'authentification de l'utilisateur "Adminn"**

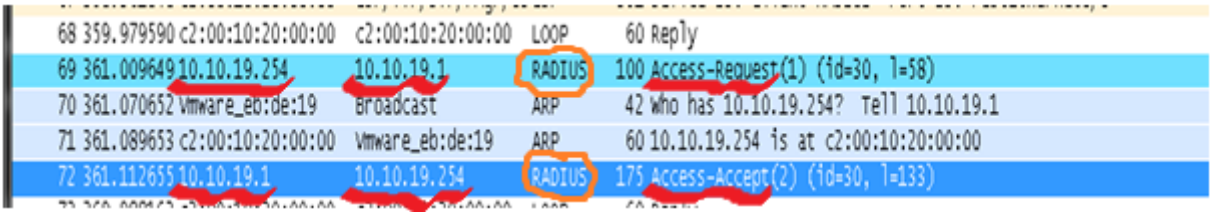


FIGURE 4.64 – Aalyse de transactions de l'authentification 802.1x

1. **Access-Request**

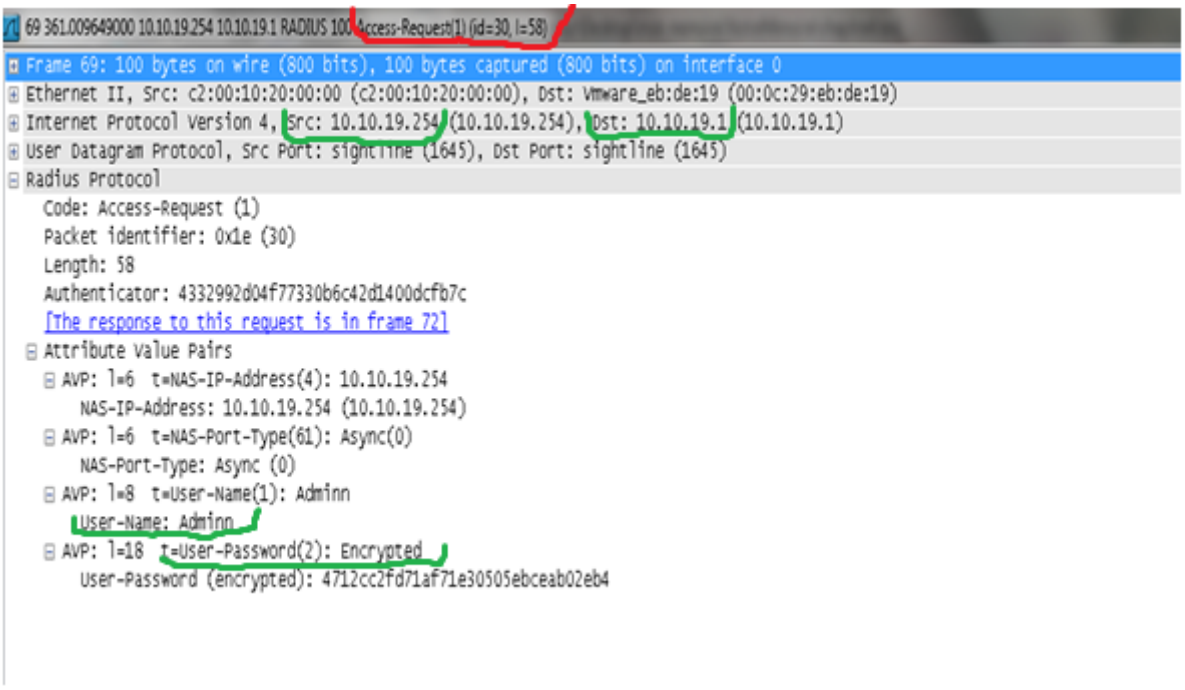


FIGURE 4.65 – Access-Request

2. **Access-Accept**

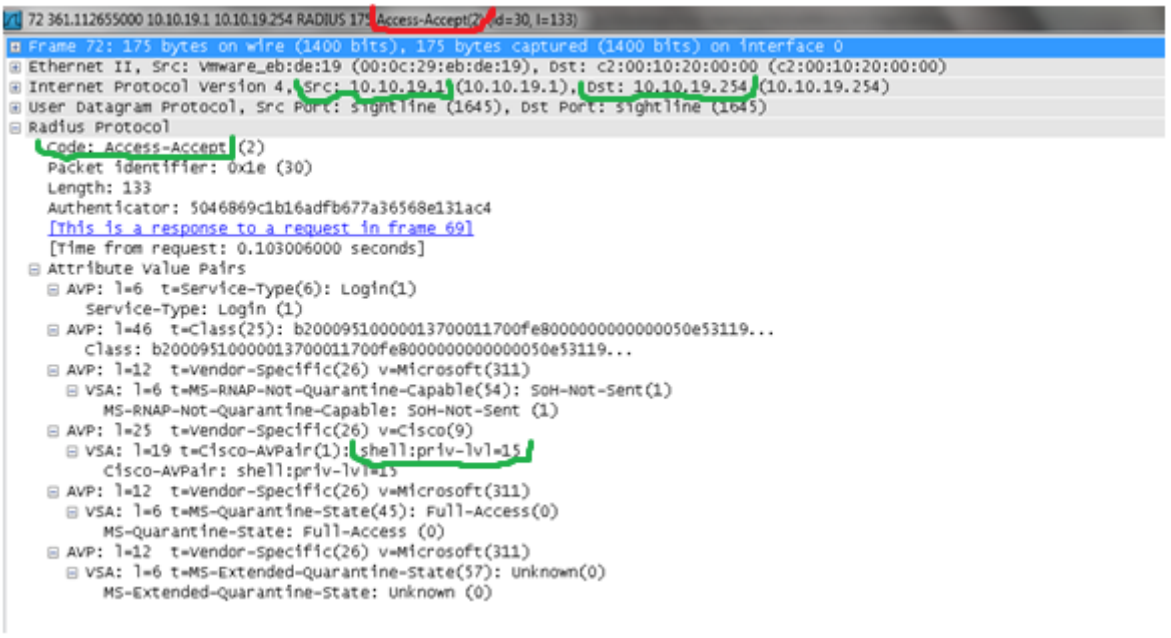


FIGURE 4.66 – Access-Accept

### 4.8.2 Authentification RADIUS

Afin de s'assurer de notre bonne configuration, nous avons effectué des tests en faisant appel à " PUTTY "

- **Putty** :est un client SSH et Telnet, développé à l'origine par Simon Tatham pour la plate-forme Windows. c'est un logiciel (et un protocole) permettant de se connecter à un ordinateur distant de façon sécurisée et permet en particulier d'ouvrir un shell à distance sur le client d'accès. [20]
- **Telnet**(terminale network ou télécommunication network, ou encore telLetype NETwork) :est un protocole permettant d'émuler un terminal à distance, cela signifie qu'il permet d'exécuter des Commandes saisies au clavier sur une machine distante. Il est utilisé notamment pour ouvrir et administrer une session sur une machine distante.
- **SSH**(Secure Shell) :Protocole qui permet de se connecter à une machine distante avec une liaison sécurisée.Les données sont cryptées entre machines, Il permet d'exécuter des commandes sur un serveur distant. SSH chiffre les données transmises alors que Telnet les véhicule en clair.

**Activer le protocole SSH au niveau de switch :**

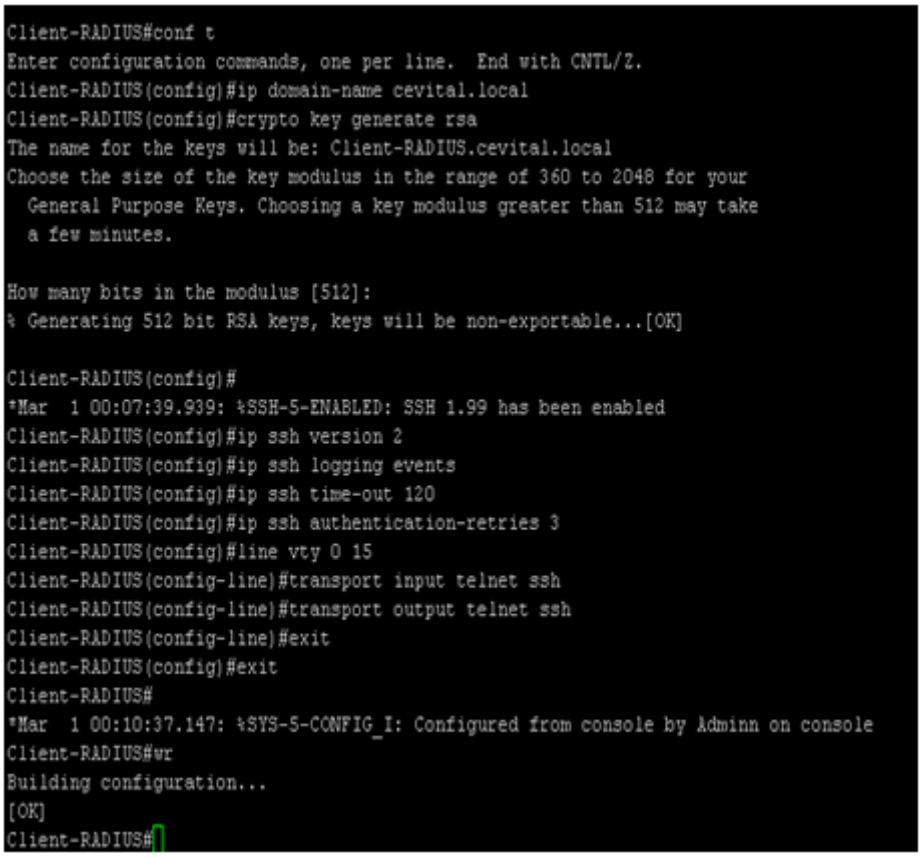


FIGURE 4.67 – Activer le protocole SSH

SSH est maintenant activé. nous pouvons accéder au switch avec un client ssh (dans notre cas putty ).

– **Test de connexion à partir de la machine cliente XP avec Putty au serveur d'accès**

il faut d'abord vérifier que notre machine XP a une adresse IP (attribuer par le serveur DHCP) . une fois l'adresse est attribuée ,le client XP utilise le logiciel putty en telnet ou en SSH pour accéder a son équipement réseau désiré .

– l'accès au switch avec un client SSH

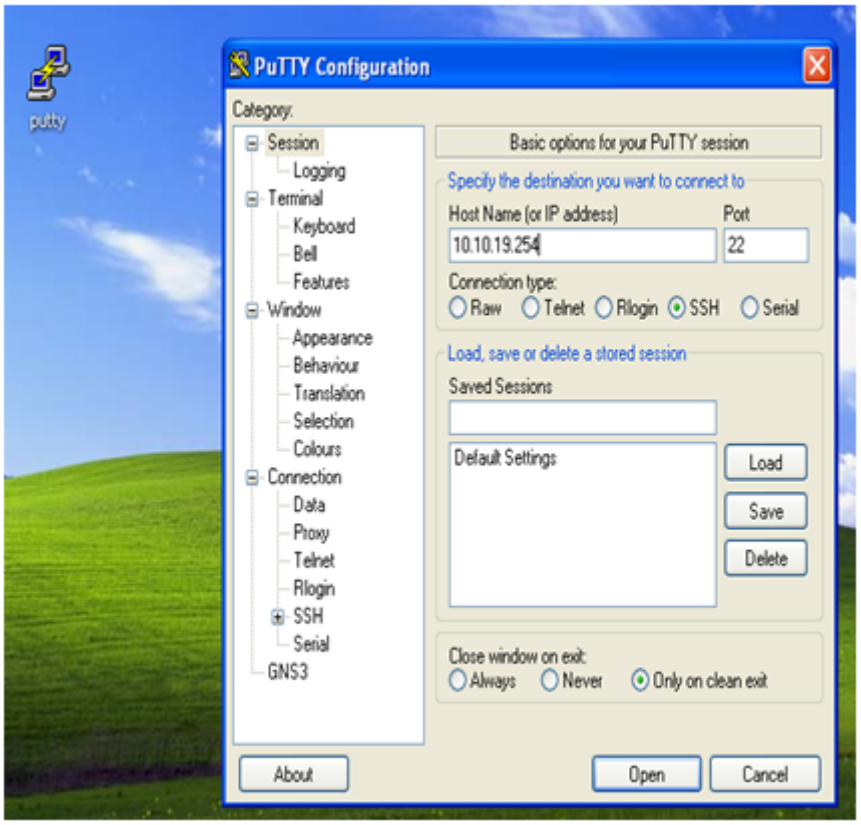


FIGURE 4.68 – l'accès au switch avec un client SSH

Il faut maintenant introduire le nom et le mot de passe pour accéder au switch

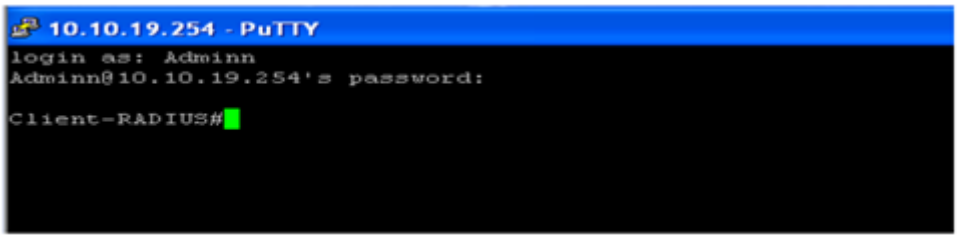


FIGURE 4.69 – L'accès avec login et password

– l'accès au switch avec un client telnet

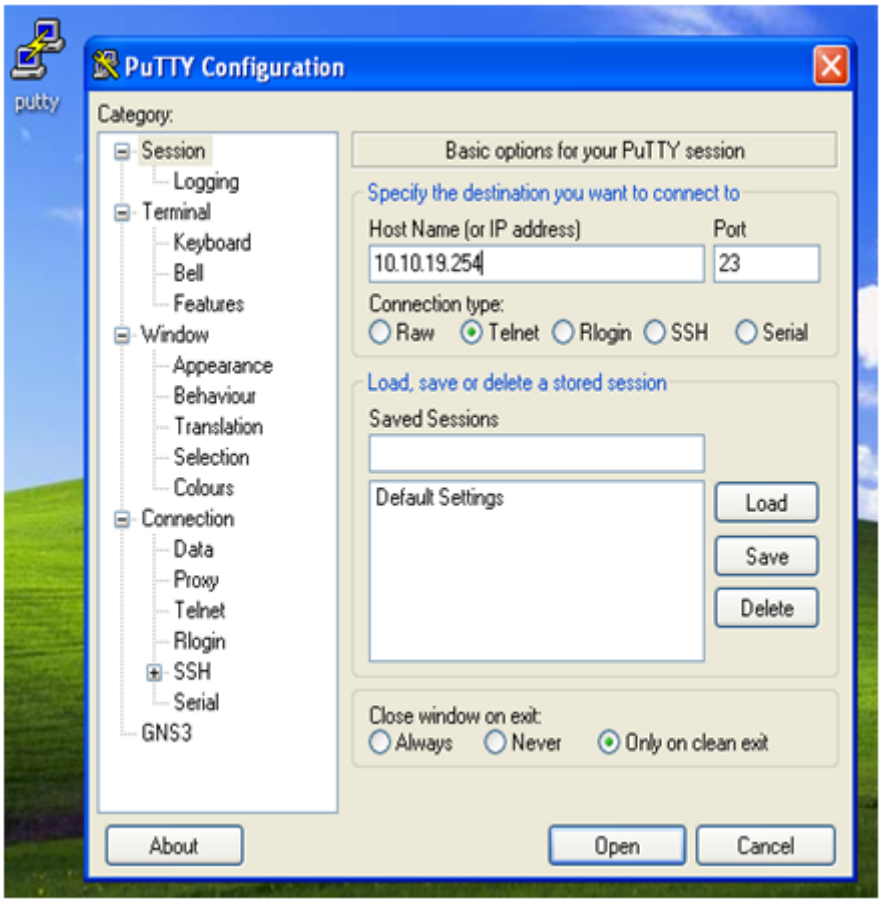


FIGURE 4.70 – l'accès au switch avec un client telnet

Il faut maintenant introduire le nom et le mot de passe pour accéder au switch

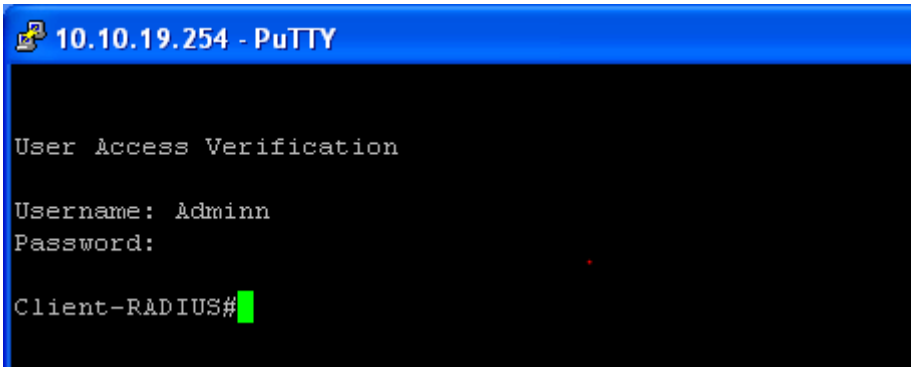


FIGURE 4.71 – L'accés avec Username et password

comme on la vérifier Précédemment l'utilisateur est membre de vlan IT ;Prenant maintenant un utilisateur qui n'est un pas membre de vlan IT(sachant que notre stratégie NPS n'autorize que les utilisateurs qui sont membre de vlan IT).

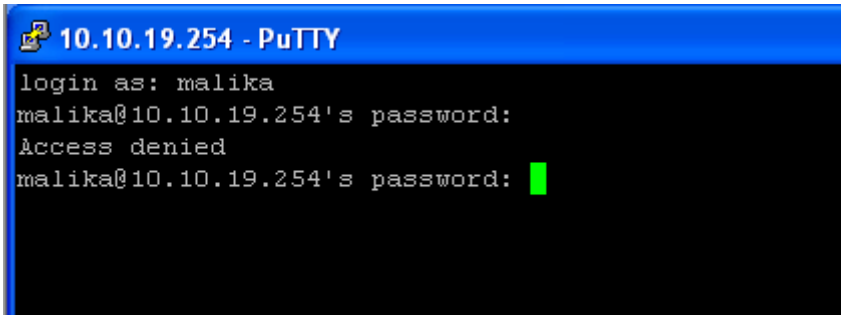


FIGURE 4.72 – L'accès avec Username et password

## Conclusion

Ce chapitre est une réalisation de ce qu'on a étudié dans les chapitres précédents. Nous l'avons débuté par les composantes et les outils nécessaires pour répondre à notre politique de sécurité, après nous avons décrit les étapes de sa réalisation.

De cette manière nous avons pu répondre au besoin ciblé au début de notre projet qui est l'authentification des Utilisateurs au niveau de Cevital en mettant en place un serveur RADIUS au sein de l'entreprise.

# Conclusion et Perspectives

Dans le domaine de la sécurité des réseaux informatiques, Il est difficile de mettre en oeuvre une solution qui répond parfaitement aux besoins ressentis dans une organisation, ce qui oblige les administrateurs réseau de travailler sans cesse afin d'aboutir une solution permettant d'améliorer la sécurité de leur réseau.

Aprés notre étude consacré au mécanisme d'authentification, nous avons constaté l'avantage de celui-ci concernant le contrôle d'accés des utilisateurs aux services demandés pour minimiser le risque des attaques menaçant le réseau.

ce mécanisme s'agit en fait de la mise en place d'une solution d'authentification RADIUS basée sur un serveur RADIUS qui permet d'assurer l'authentification des clients avant tout accés au réseau de Cevital de Bejaia, ainsi de définir les droits d'accés à chacun de ces utilisateurs.

pour la réalisation de service d'authentification RADIUS,nous avons utilisé windows server 2008 qui inclut le serveur d'authentification RADIUS, et qui fait appel à des services de domaines Active Directory permettant d'avoir des controlleurs de domaines.

la mise en oeuvre de ce projet,nous a permis d'apporter une contribution à l'entreprise Cevital de Bejaia. mais aussi d'acquérir de nouvelles connaissances sur le protocole 'authentification RADIUS gràce à une étude détaillée sur son fonctionnement,ses principes et les protocoles qu'il utilise. durant notre formation, nous avons mis en pratique ces connaissances.

Enfin,comme perspectives pour ce projet,nous souhaitons également exploiter mieux les services qu'offre le protocole RADIUS notamment l'authentification des utilisateurs s'appuyant sur le standard 802.1x pour les connexions réseau sans fil.

# Bibliographie

[1] M.Rizcallah , annuaire LDAP, EYROLLES,édition 2002.

[2] L. Mirtain , Service d'annuaire LDAP, édition 1999 .

[3] D .LACHIVER, Utilisation du réseau pédagogique, édition 2013.

[4] Adel RAISSI, Authentification dans les Réseaux Wifi par le protocole radius, édition 2010.

[5] C.CERTA, la sécurité des systèmes d'information.édition 2012.

[6] C.Lyonnais,POLITIQUE DE CERTIFICATION,édition 2001.

[7] Vincent REMAZEILLES, Cisco La sécurité des réseaux,édition 2009 .

[8] M. Robert Brochu, Francis Beaudoin, Jean Laterrière,Politique de sécurité de l'information, édition 2003.

[9] Cours de 3ème année licence académique en informatique.

[10] Cours Master 2 professionnel informatique.

[11] C. Rigney,Livingston, A. Rubens,Remote Authentication Dial In User Service (RADIUS),édition 1997.

[12] Serge Bordères,Authentification réseau avec Radius,EYROLLES,édition 2006.

[13] http ://wapiti.telecom lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesric deprey/pres.htm

[14] http ://technet.microsoft.com/fr-fr/library/bb457039.aspx

[15] K.J,GUIDE DE MISE EN PLACE D'UNE SOLUTION D'AUTHENTIFICATION NIVEAU 2,édition 2010.

[16] Guillaume Piolle, "Protection de l'accès au réseau-802.1X, RADIUS, EAP", édition 2011.

[17] Alain Fernandez, Virtualisation des systèmes,édition 1998.

[18] Darky, Présentation de Windows Server 2008 R2, édition 2011.

[19] Admin,GNS3 ou comment émuler son réseau, édition 2012.

[20] F.Team, Manuel dŠexploitation Clients de transfert de fichiers, édition 2010.

[21] Jérémie Sebban, Analyseur de paquets réseau pour les pros, édition 1997.

**Résumé**

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau filaire ou non filaire, pour cela les administrateurs réseau d'entreprise doivent mettre des mécanismes de sécurité plus robustes.

Notre projet consiste à mettre en oeuvre une solution d'authentification pour le réseau Ethernet de Cevital,assurant le contrôle des accès des utilisateurs ,pour cela,nous avons choisi le protocole RADIUS qui est l'un des protocoles d'authentification les plus performant

Pour la réalisation de ce travail, nous avons fait d'abord un rappel sur les notions de bases de réseau et la sécurité informatique pour bien comprendre les concepts répondant à la problématique, et pour l'implémentation de la solution,nous avons choisi Windows Server 2008 qui inclut le serveur d'authentification RADIUS et la base de données Active Directory pour l'enregistrement des comptes utilisateurs.

**Mots-clés :**authentification,Ethernet,RADIUS, Windows Server 2008,Active Directory.

**Abstract**

Today, computer security is almost indispensable for the proper functioning of a wired or wireless network for that network administrators must make business more robust security mechanisms.

Our project is to implement an authentication solution for the Ethernet network Cevital, ensuring control user access to this, we chose the RADIUS protocol that is one of the most efficient authentication protocols.

For the realization of this work, we have first a reminder of the basic concepts of network and information security to understand the concepts responding to the problem, and for the implementation of the solution, we chose Windows Server 2008, which includes the RADIUS authentication server and the Active Directory database for recording user accounts.

**Keywords :** authentication,Ethernet,RADIUS, Windows Server 2008,Active Directory.