

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement et de la Recherche Scientifique
Université A. Mira - Bejaïa
Faculté des Sciences Exactes
Département Informatique



Mémoire de fin de cycle

En vue de l'obtention d'un diplôme de Master en Informatique
Option : Administration et Sécurité des Réseaux

Thème

**Elaboration d'un mécanisme de sécurité basé sur le standard
802.1X sous WINDOWS Server 2012 R2**
Cas d'études : SONATRACH Branche de Transport par Canalisation

Réalisé par :

ATTABI Sonia & BAKOURI Souhila

Soutenu le 27 juin 2018 Devant le Jury composé de :

Président	: ATMANI Mouloud	Maitre de conf. B	U.A/Mira Bejaia.
Encadreur	: LARBI Ali	Maitre Ass. A	U.A/Mira Bejaia.
Examineur	: AKILAL Abdalleh	Maitre Ass. A	U.A/Mira Bejaia.
Examineur	: BOUCHABAH Fateh	Maitre Ass. A	U. A/Mira Bejaia.

Promotion : 2017/2018.

Remerciement

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

Nous remercions notre encadreur Monsieur LARBI ALI d'avoir accepté de rapporter ce mémoire. Nous le remercions pour sa lecture attentive du manuscrit, pour ses corrections et pour ses remarques qui nous ont permis d'améliorer le document final.

Nos remerciements à Monsieur TIAB AHMED qui nous a aidé à organiser ce stage au sein de l'entreprise SONATRACH branche de Transport par Canalisation et d'avoir accepté de nous encadrer et de nous avoir fait travailler sur un sujet très intéressant qui nous a beaucoup apporté. Nous le remercions d'avoir toujours été disponible. Nous le remercions pour toutes ses remarques, ses conseils qui nous ont aidé dans la réalisation de notre modeste travail.

Un grand merci à Monsieur DJEBBARI YACINE pour tous ces conseils et son aide très précieux. Nous lui sommes très reconnaissantes d'avoir partagé son savoir-faire et d'avoir été toujours disponible.

Nos remerciements les plus vifs à nos très très chers parents qui nous ont soutenus tout au long de notre parcours scolaire et universitaire. Merci papa, merci maman d'avoir subvenu à tout nos besoins, merci pour les valeurs nobles, l'éducation et le soutien permanent venu de vous.

Nous tenons à remercier tous ceux qui nous ont soutenu et aidé dans la réalisation de ce mémoire de près ou de loin. Nous remercions, enfin, les membres de jury qui ont accepté d'évaluer ce mémoire.

Dédicace

Nous remercions le bon dieu de nous avoir donné le courage, la santé, la volonté afin de mener à bien ce modeste travail.

Nous dédions ce modeste travail :

A nos parents. Aucun hommage ne pourrait être à la hauteur de l'amour Dont ils ne cessent de nous combler. Que dieu leurs procure bonne santé et longue vie ;

A nos frères et sœurs ;

A nos cousins et cousines ;

A nos chers amis (e)...

Sonia & Souhíl

Table des matières	i
Liste des figures	vi
Liste des tableaux	x
Liste des abréviations	v
Introduction générale	vii
1. Généralités sur les réseaux locaux et la sécurité informatique	2
1.1 Introduction.....	2
1.2 Réseaux locaux	2
1.2.1. Définition	2
1.2.2. Equipements d'un réseau local.....	2
1.2.3. Interconnexion d'un réseau local.....	3
1.3. Support de transmission.....	3
1.3.1. Technologie de filaire.....	3
1.3.2. Technologie sans fil.....	5
1.4. Topologie d'un réseau local.....	5
1.4.1. Topologies physiques.....	5
1.4.2. Topologie logique.....	7
1.5. Architectures protocolaires.....	8
1.5.1. Définition d'un protocole.....	8
1.5.1.1. Modèle de référence OSI.....	8
1.5.1.2. Modèle tcp/ip.....	8
1.6. Adressage IP.....	9
1.6.1 Classé adressage IP.....	9
1.6.2 Adresses IP privées.....	10
1.7. Sécurité informatique.....	10
1.7.1. Définition de la sécurité.....	10
1.7.2. Les principes de la sécurité.....	10
1.7.3. Vocabulaire de base de la sécurité informatique.....	10
1.7.4. Quelques attaques bien connus.....	12
1.7.5. Principales technologies de défenses.....	13
1.10. Conclusion.....	15
2. Etudes de l'existant	16
2.1. Introduction.....	16

2.2 Présentation de l'organisme d'accueil.....	16
2.2.1 Présentation de SONATRACH.....	16
2.2.2 Organigramme.....	16
2.2.3. Présentation de la direction régionale de transport de Béjaia (RTC).....	16
2.2.3.1. Structure de la RTC.....	17
2.2.3.2. Présentation du centre informatique.....	17
2.2.3.2.1 Organisation du centre informatique.....	18
2.2.3.2.2. Rôle de chaque service dans l'entreprise.....	18
2.3. Présentation du réseau de RTC.....	19
2.3.1. Equipements et matériels réseau.....	21
2.3.1.1. Infrastructure du réseau de RTC.....	21
2.3.1.2. Les commutateurs utilisés dans le réseau de la DRGB.....	22
2.3.1.3. Les routeurs utilisés dans le réseau de la DRGB.....	23
2.3.1.4. Définition d'autres équipements réseau.....	24
2.3.2. Les VLANs utilisés dans la RTC.....	24
2.4. Service de la sécurité de la RTC.....	25
2.4.1. Serveur antivirus "F-Secure".....	25
2.4.2. Serveur filtrage web.....	26
2.4.3. Serveur reporting.....	26
2.4.4. Firewall Juniper SSG 550.....	26
2.5. Câblage informatique.....	27
2.6. Problématique.....	27
2.7. Conclusion.....	27
3. Solution proposée	28
3.1. Introduction.....	28
3.2. Authentification.....	28
3.3. Structure générale de notre solution.....	28
3.3.1. Déroulement de notre solution	30
3.4. Le protocole RADIUS.....	32
3.4.1. Le protocole RADIUS dans le modèle OSI.....	34
3.4.2. Format des paquets RADIUS	34
3.5. La technologie du standard 802.1X.....	35

3.5.1 Description du protocole IEEE 802.1X.....	36
3.6. Le protocole d'authentification EAP.....	37
3.7. Vue d'ensemble et fonctionnement.....	37
3.8. Active directory.....	37
3.8.1. Les avantages d'Active Directory.....	37
3.9. DNS (Domain Name System)	40
3.10. Serveur DHCP (Dynamic Host Configuration Protocol)	40
3.10.1. Fonctionnement de DHCP.....	41
3.11. Conclusion.....	42
4. Implémentation et test	44
4.1 Introduction	44
4.2. Outils utilisés.....	44
4.3. Simulation du réseau local de SONATRACH.....	44
4.4. Le modèle hiérarchique.....	44
4.4.1. Configuration du switch.....	45
4.4.2. Configuration du Windows serveur 2012.....	47
4.4.2.1. Configuration tcp/ip du serveur	47
4.4.2.2. Configuration d'active directory et DNS.....	48
4.4.2.3. Configuration du serveur DHCP.....	50
4.4.2.4. Organisation des clients AD en unités organisationnelles.....	51
4.4.2.5. Joindre le pc au domaine	53
4.4.2.6. Configuration du serveur RADIUS.....	54
4.4.2.7. Création d'une stratégie.....	61
4.5. Tests de fonctionnement de notre solution.....	62
4.6. Conclusion.....	
Conclusion générale.....	68
Liste des références.....	69
ANNEXE A. Installation et ajout des rôles	69
1. Installation de Windows server 2012.....	71
2. Gestionnaire de serveur.....	72
3. Installation de l'active directory.....	72
4. Installation du service DHCP.....	73
5. Ajout du rôle NPS (Network Policy Server)	74
6. Joindre le pc au domaine	74
7. Activer l'authentification 802.1x pour PC.....	77
ANNEXE B. Configuration de base d'un switch	79
1. Mode privilégié.....	79
1.1. Afficher la configuration de base.....	79
1.2. Supprimer une configuration.....	79

1.3. Sauvegarder une configuration.....	79
2. Mode d'exécution globale	79
2.1. Configuration de hostname.....	80
2.2. Configuration des VTP.....	80
2.3. Configuration de l'étherchannel.....	80
2.4. Configuration du SSh.....	80
2.5. Configuration lignes VTY.....	80
2.6. Configuration des lignes consoles.....	81
2.7. Utilisation de la commande « do »	82

Liste des figures

1.1	La coupe d'un câble pair torsadé.....	4
1.2	La coupe d'un câble coaxial.....	4
1.3	La coupe d'un câble fibre optique.....	5
1.4	Schéma réseau d'une topologie en bus.....	6
1.5	Schéma réseau d'une topologie en étoile.....	7
1.6	Schéma réseau d'une topologie en anneau.....	7
1.7	Schéma réseau d'une topologie en maille.....	9
1.8	Les deux modèles de communication.....	9
2.1	Les différentes classes d'adressage.....	17
2.2	Les branches de Sonatrach.....	17
2.3	Organigramme de la direction régionale de Bejaia.....	18
2.4	Organigramme du centre informatique.....	19
2.5	Liaison entre l'ancien et le nouveau bâtiment.....	21
2.6	Catalyst Cisco 3750.....	23
2.7	Catalyst Cisco 3550.....	23
2.8	Catalyst Cisco 2950.....	24
2.9	Routeur Cisco 1700.....	24
2.10	Routeur wimax.....	24
2.11	Routeur wifi 4400.....	25
2.12	Routeur téléphonies IP 3825.....	25
3.1	Déroulement de notre solution.....	30
3.2	Messages RADIUS.....	31
3.3	Le protocole RADIUS au sein du modèle OSI.....	32
3.4	Encapsulation du Protocole RADIUS.....	32
3.5	Format des trames RADIUS.....	32
3.6	Les trois entités qu'interagissent dans le protocole 802.1X.....	34
3.7	Fonctionnement de la 802.1X.....	36
3.8	Fonctionnement de DHCP.....	39
4.1	Topologie reproduite de l'entreprise RTC.....	44
4.2	Création des Vlans.....	45

4.3	Assigner une adresse IP a l'interface du vlan 10.....	45
4.4	Configuration de l'interface du trunk.....	46
4.5	Activation du service AAA et spécification du groupe d'authentification.....	46
4.6	Attribution d'une adresse et d'un mot de passe au serveur radius.....	46
4.7	Configuration de l'authentification basée sur le port.....	46
4.8	Configuration de l'affectation dynamique des vlans.....	47
4.9	Réception du vlan adéquat.....	47
4.10	Affectation du vlan isolation aux utilisateurs non 802.1x.....	47
4.11	Affichage des message dot1x.....	47
4.12	Permutation des VLANs.....	47
4.13	Activation du 802.1x.....	48
4.14	Configuration TCP/IP du Serveur.....	48
4.15	Création du domaine Sonatrach.....	49
4.16	Sélection du niveau fonctionnel de la forêt et du domaine.....	49
4.17	Ouverture de la session Administrateur.....	50
4.18	Exemple de création d'un étendue DHCP.....	50
4.19	Ajout d'exclusion DHCP.....	51
4.20	L'ensemble des plages d'adresses utilisées.....	51
4.21	Création d'une unité d'organisation.....	52
4.22	Ajout d'utilisateur.....	52
4.23	Création des sessions utilisateur.....	53
4.24	Modifier les paramètres du PC.....	53
4.25	Inscrire le serveur NPS dans active directory.....	54
4.26	Configuration d'un client radius.....	55
4.27	Spécification du standard RADIUS.....	55
4.28	Configuration du 802.1x.....	56
4.30	Connexion câblée sécurisé.....	56
4.31	Spécification des commutateur 802.1X.....	57
4.32	Configuration du type de protocole EAP pour la stratégie.....	57
4.33	Fixation de Nombre de tentative d'authentification.....	58
4.34	Spécification des groupes d'utilisateurs	58
4.35	Configuration des attributs RADIUS.....	59
4.36	Désactivation et création de stratégies.....	60

4.37	Le contenu d'une stratégie.....	61
4.38	Test de routage inter Vlan et DHCP relais	61
4.39	Test du routage inter Vlan.....	62
4.40	Exemple d'authentification d'un utilisateur.....	62
4.41	Cas d'une authentification réussite.....	63
4.42	Exemple des messages échangés dans le client RADIUS et le serveur RADIUS....	64
4.43	Test du vlan 40.....	64
4.44	Exemple d'une authentification non réussite.....	65
4.45	Cas d'une authentification non réussite.....	65
A.1	Installation de Windows serveur 2012.....	69
4.29	Gestionnaire de serveur.....	69
4.30	Ajout du service AD DS	70
A.1	Promouvoir du serveur en contrôleur de domaine.....	70
A.2	Installation du serveur DHCP.....	71
A.3	Ajout du rôle NPS.....	72
A.4	Modifier le nom du domaine.....	72
A.5	Saisie du nom et du mot de passe.....	73
A.6	Boîte de dialogue.....	73
A.7	Notification pour redémarrer de pc.....	73
A.8	Démarrage du service	74
A.9	Authentification au tant qu'administrateur.....	74
A.10	Démarrage et activation du service 802.1x.....	75
A.11	Activation du standard IEEE 802.1x.....	75
A.12	Affectation de l'adresse IP après authentification.	76
B.13	Mode privilégié.....	77
A.14	Afficher la configuration de base dans un switch.....	77
B.1.	Supprimer une configuration dans un switch.....	74
B.1.1	Mode privilégié.....	77
B.1.2	Sauvegarder une configuration dans un switch.....	77
B.1.3	Mode d'exécution globale.....	78
B.2	Configuration de hostname.....	78
B.2.1	Configuration de vtp.....	78
B.2.2	Configuration d'etherchannel.....	78

B.2.3	Configuration du ssh.....	79
B.2.4	Configuration des lignes vty dans un switch.....	79
B.2.5	Sauvegarder la configuration dans un switch.....	80
B.2.6	Configuration des lignes consoles.....	76
B.2.7	Sauvegarder la configuration dans un switch.....	77

Liste des tableaux

1.1 Les différentes classes d'adressage.....	8
1.2 Les classes d'adresses privées.....	9
2.1 La liste des équipements et armoires du la RTC.....	20
2. 2 La liste des VLANs du réseau local de l'entreprise RTC.....	24
3.1 Listes des VLANs utilisés dans la nouvelle architecture.....	29

Liste des Abréviations

AAA	Authentication Authorization Accounting
ACL	Access Control List
AD	Active Directory
BDD	Base De Donnée.
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DMZ	Demilitarized Zone.
DRGB	Direction Régionale de Bejaia
EAP	Extensible Authentication Protocol
EBIOS	Expression des Besoins et Identification des Objectifs de sécurité.
EAP-Fast	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAPOL	Extensible Authentication Protocol Over the LAN
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
FQDN	Fully Qualified Domain Name
GNS3	Graphical Network Simulator.
HP	Hewlett-Packard
HTTP	HyperText Transport Protocol.
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IDS	Intrusion Detection System
IP	Internet Protocol

IOS	Internetwork Operating System
ISO	International Standards Organization
Ipsec	Internet Protocol Security
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAP	Network Access Protection
NAS	Network Access Server
NPS	Network Policy Server
OSI	Open Systems Interconnection
OU	Organizations Unit
PAE	Port Access Entity
PC	Personnel Computer
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RFC	Les requests for comments
RSTP	Rapid Spanning Tree protocol.
RTC	transport des hydrocarbures de la SONATRACH
SI	Système d'information
SIQ	Ingénieur système.
SPD	ingénieur système distribués

SSL	Sécure Socket Layer
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VMware	Virtual Machine
VPN	Virtual Private Network
VTP	Vlan Trunking Protocol
VTY	Virtual Terminal
WAN	Wide Area Network

Introduction générale

L'utilisation des réseaux informatiques dans les entreprise et leurs interconnexions à internet est en pleine effervescence, ce qui laisse émerger beaucoup de préoccupations sécuritaires. En effet, Vu le grand nombre de ressources, des fichiers et des systèmes d'informations, Il est indispensable d'éviter toute menace nuisant à la confidentialité des données. La sécurité des systèmes informatiques se cantonne à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leurs ont été octroyés, Notre objectif est donc de prévoir une solution d'authentification permettant de sécuriser l'accès des utilisateurs au réseau local de l'entreprise "SONATRACH branche de transport par canalisation".

Pour atteindre cet objectifs nous avons à notre disposition, plusieurs méthodes d'authentification parmi lesquelles, nous avons choisi celle basée sur le protocole d'authentification RADIUS (Remote Access Dial In User Services) qui s'appuie à la fois sur le standard 802.1X et sur le protocole EAP (Extensible Authentication Protocole).

La solution adoptée nécessite une combinaison de plusieurs outils (Switch, Routeur), notamment un annuaire (Active Directory) pour contenir l'ensemble des utilisateurs ainsi qu'un serveur RADIUS intégré sous Windows server 2012 R2 pour assurer l'authentification de ces derniers.

Dans le présent mémoire, nous mettrons en évidence les étapes que nous avons suivi pour réaliser notre travail, articulé en quatre chapitres organisés comme suit :

Le premier chapitre s'intitule « généralités sur le réseau local et la sécurité informatique » où nous présenterons quelques concepts de base sur les réseaux locaux, et les différentes notions de la sécurité informatique notamment celles qui sont liées à l'authentification.

Le deuxième chapitre s'intitule « étude de l'existant », dans ce dernier, nous avons étudié les éléments de base qui compose le réseau LAN de l'entreprise SONATRACH, ainsi que les différents équipements et les ressources informatiques dont elle dispose. Par la suite, nous avons énumérer les différents problèmes qui peuvent nuire au bon fonctionnement du réseau, dans l'intérêt de parvenir à une solution efficace pour y remédier.

Le troisième chapitre s'intitule « solution proposée », ce dernier aura pour objectif de décrire le fonctionnement général de notre solution, en définissant tout d'abord les éléments de base, le mécanisme de son fonctionnement et les protocoles essentiels sur lesquels elle est fondée, pour enfin passer à l'étape d'implémentation.

Dans le quatrième et dernier chapitre, nous nous somme occupé de l'« Implémentation et test » dans lequel nous avons introduit les outils et logiciels ayant servie pour concevoir notre solution, par la suite nous présenté en détail les étapes suivies.

Enfin, nous avons clôturé notre mémoire par une conclusion générale et quelques perspectives futures.

Chapitre 1

Généralités sur les réseaux locaux et la sécurité informatique

1.1 Introduction

L'expansion et l'importance grandissante des réseaux informatiques, ont engendré beaucoup de problèmes de sécurité des systèmes d'information. Il s'avère alors indispensable de renforcer les mesures de sécurité, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques. Pour mieux aborder notre sujet, il est essentiel de commencer par un aperçu des technologies et des mécanismes liés aux systèmes informatiques en général et les réseaux locaux en particulier.

Ce chapitre sera consacré pour aborder et expliquer le fonctionnement et les concepts de bases des réseaux locaux ainsi que la sécurité informatique.

1.2 Réseaux locaux

1.2.1. Définition

Un réseau local ou LAN (de l'acronyme anglais Local Area Network) est un ensemble d'ordinateurs interconnectés dans une zone géographique restreinte. Les LAN correspondent en général aux réseaux intra entreprises, ou encore aux réseaux des particuliers. Ils permettent aux divers ordinateurs de partager des données et des ressources : imprimante, connexion Internet... [1]

On distingue deux modes de fonctionnement pour les **réseaux LAN** [15] :

- Un environnement **peer to peer**, c'est-à-dire d'égal à égal où chaque ordinateur joue un rôle similaire.
- Un environnement **client/serveur**, où un ordinateur central fournit des services réseaux aux autres utilisateurs.

1.2.2. Equipement d'un réseau local

Les différents matériaux du réseau local sont [2] :

- **L'ordinateur** : c'est un appareil électronique capable de traiter des informations de façon automatique. Il fournit à l'utilisateur d'un réseau l'ensemble des possibilités presque illimitées (manipulation des logiciels, traitement des données, utilisation de l'Internet).

- **Le serveur** : c'est un logiciel ou ordinateur très puissant choisit pour coordonner, contrôler et gérer les ressources d'un réseau. Il met ses ressources à la disposition des autres ordinateurs sous la forme des services.
- **Imprimante** : c'est une unité d'impression, un périphérique capable de reproduire les Caractères et /ou des symboles et des graphiques prédéfinis sur un support comme papier, bande, tissus,... Il existe des imprimantes réseau et des imprimantes en réseau.

1.2.3. Interconnexion d'un réseau local

Un réseau local a pour objectif d'interconnecter les équipements informatiques de la dimension d'une entreprise, toutefois cette dernière peut se composer de plusieurs LAN qui doivent être reliés et cela grâce à des équipements intermédiaires [2] :

- **Les répéteurs** : appelés aussi hub, ce sont les équipements qui permettent de répéter automatiquement un signal reçu sur un port d'entrée vers un port de sortie tout en le régénérant. Leurs finalités sont donc d'allonger le support physique.
- **Les switches** : ce sont des dispositifs qui contiennent plusieurs ports. Ils permettent de relier plusieurs machines entre elles.
- **Les ponts** : ils sont utilisés pour interconnecter deux réseaux utilisant le même protocole, ils se basent sur l'adresse MAC et le nom de la station sur le réseau, pour savoir si la trame doit traverser le pont ou non. En d'autres termes, les informations ne passeront le pont, que si elles doivent aller d'un réseau à un autre. En général, un pont permet de passer d'un réseau vers un autre de même type, mais il est possible d'avoir des ponts qui transforment la trame pour l'adapter au réseau raccordé.
- **Les routeurs** : c'est des équipements permettant d'acheminer les paquets envoyés d'un réseau à un autre de façon optimale.
- **La passerelle** : c'est un système logiciel et matériel permettant le passage entre deux réseaux hétérogènes.

1.3. Support de transmission

Pour transmettre les informations d'une station à une autre, un média de transmission est indispensable. Généralement on distingue deux catégories, les supports filaires (les paires torsadées, les câbles coaxiaux, les fibres optiques, ou autres) et les supports sans fil (l'infrarouge, les ondes radio,...) [2].

Dans ce qui suit, nous allons présenter quelques technologies filaires et sans fil utilisées [2].

I.3.1. Technologie filaire

a) **Câbles à paires torsadées** : une paire torsadée est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre [17].

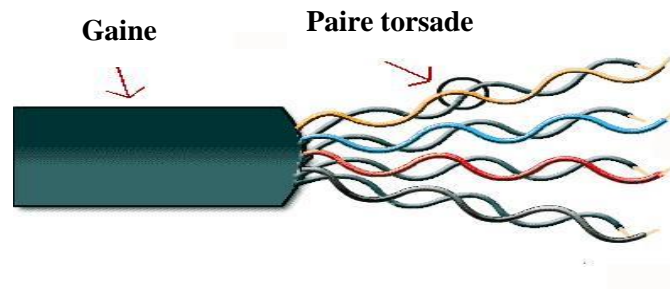


Figure 1.1: La coupe d'un câble pair torsadé

b) **Les câbles coaxiaux** : Ils se composent d'un conducteur central en cuivre, entouré d'une enveloppe isolante (diélectrique) et un conducteur extérieur (tresse, ruban ou tube). Les câbles coaxiaux, peuvent couvrir des distances plus longues que les paires torsadées avec plus de performances. En revanche les câbles coaxiaux ont tendance à disparaître dans les nouveaux plans de câblage [2].

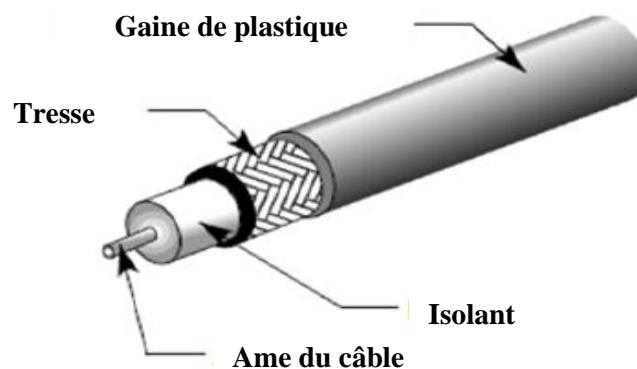


Figure 1.2 : La coupe d'un câble coaxial

c) **La fibre optique** : La fibre optique est un fil en verre ou en plastique très fin (sa largeur ne dépasse pas un cheveu). Elle permet de transmettre la lumière entre deux extrémités distantes avec une bande passante très élevée.

La fibre optique peut se présenter selon deux modes [16] :

- **Monomode (SMF)** : dans ce mode, le noyau a un diamètre si petit, ce qui fait la Lumière ne peut entrer que dans un seul angle.

- **Multimode (MMF)** : contrairement au monomode, le multimode a un large diamètre qui permet à la lumière de pénétrer dans des angles différents.

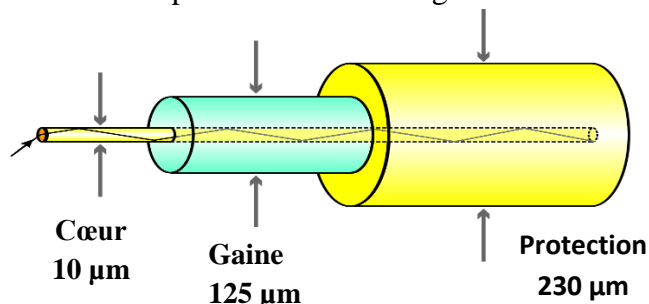


Figure 1.3 : La coupe d'un câble fibre optique

1.3.2. Technologie sans fil

La technologie sans fil permet à différents types d'appareils électroniques, comme des ordinateurs portatifs, des téléphones mobiles ou des périphériques de toutes sortes, d'échanger entre eux, sur une courte distance des messages vocaux ou des données.

a) La technologie infrarouge : Les liaisons infrarouges permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par secondes. Cette technologie est largement utilisée pour la domotique.

b) Les ondes radio : Les ondes radio sont un type de rayonnement électromagnétique, utilisé pour la communication : télévision, téléphones, radios. En effet, les ondes radios reçues seront convertit en vibrations mécaniques dans l'enceinte, dans le but de créer des ondes sonores qui peuvent être entendus [18].

1.4. Topologie d'un réseau local

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, liaisons sans fil, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelée topologie physique. On distingue généralement deux types de topologie : la topologie physique et la topologie logique [3].

1.4.1. Topologies physiques

La topologie physique désigne la manière dont les équipements sont interconnectés en réseau. Dans cette topologie nous avons trois grandes topologies qui sont [2] :

- **Topologie en bus** : C'est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par

l'intermédiaire de câbles, généralement de type coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

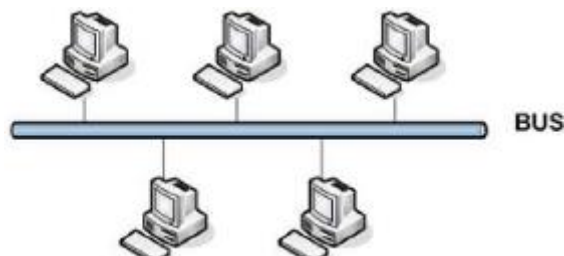


Figure 1.4: Schéma réseau d'une topologie en bus

- **Topologie en étoile :** Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur. Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions. Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur).

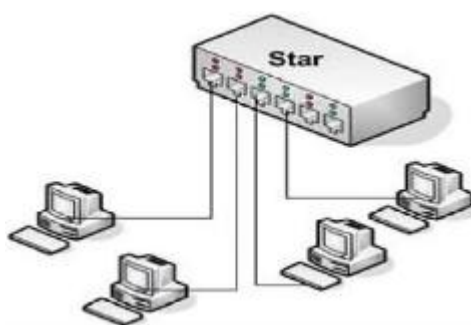


Figure1.5: Schéma réseau d'une topologie en étoile

- **Topologie en anneau :** Dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à leur tour. Les deux principales topologies logiques utilisant cette topologie physique sont Token Ring (anneau à jeton) et FDDI (Fiber Distributed Data Interface).

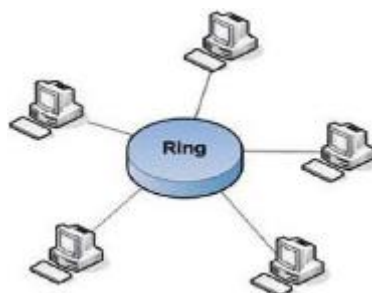


Figure 1.6 : Schéma réseau d'une topologie en anneau.

- **Topologie maillée :** La topologie maillée permet de connecter tous les équipements, nœuds, entre eux afin d'obtenir une redondance et, donc, une tolérance aux pannes. Elle est utilisée sur les réseaux étendus (WAN) pour interconnecter les réseaux locaux. La mise en œuvre de la topologie maillée est difficile et onéreuse [4].

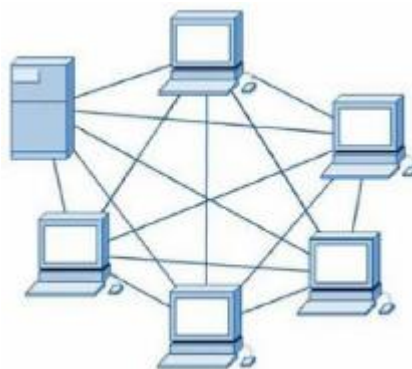


Figure 1.7 : Schéma réseau d'une topologie en maillé

1.4.2. Topologie logique

Les dispositifs matériels mis en œuvre ne sont pas suffisants à l'utilisation du réseau local. En effet, il est nécessaire de définir une méthode d'accès standard entre les ordinateurs, afin que ceux-ci sachent de quelle manière les ordinateurs échangent les informations, notamment dans le cas où plus de deux ordinateurs se partagent le support physique. Cette méthode d'accès est appelée topologie logique.

La topologie logique est réalisée par un protocole d'accès au médium. Les protocoles d'accès les plus utilisés sont Ethernet et Token Ring [3].

- **Ethernet :** La technologie Ethernet est utilisée pour connecter de nombreux périphériques différents, tels que des ordinateurs et des imprimantes. Il permet à toutes les machines connectées de partager des ressources, d'envoyer et de recevoir des fichiers et d'accéder à la même connexion Internet. Les données qui seront envoyées sur un réseau Ethernet sont divisées en petits bits appelés paquets, puis envoyés afin de destina-

tion la machine. Ethernet est une technologie beaucoup plus fiable et rapide que d'autres protocoles tels que Token Ring en raison de sa détection de collision avancée.

- **Token Ring :** Le protocole Token Ring est le deuxième protocole le plus utilisé sur les réseaux locaux après Ethernet. Le protocole IBM Token Ring a conduit à une version standard, spécifiée en tant que IEEE 802.5.

1.5. Architectures protocolaires

En plus du matériel qui assure la connectivité et l'échange des signaux sur le support physique, il est nécessaire d'utiliser des règles de communication. Ces protocoles permettent de donner un sens au signal qui circule entre les postes et gérer l'accès au support partagé [2].

1.5.1. Définition d'un protocole

Un protocole est un ensemble de règles destiné à une tâche de communication particulière, deux ordinateurs doivent utiliser le même protocole pour pouvoir communiquer entre eux, en d'autres termes ils doivent parler le même langage pour se comprendre.

Un gestionnaire de protocole est un programme qui met en œuvre un protocole particulier. Il existe plusieurs familles de protocoles ou modèles [2].

1.5.1.1. Modèle de référence OSI

Le modèle OSI (Open System Interconnexion) a été mis en place par l'ISO (International Standard Organisation) afin de normaliser les communications entre les ordinateurs d'un réseau. En effet, aux origines des réseaux chaque constructeur avait un système propre et de nombreux réseaux incompatible coexistaient. Ce modèle a permis de standardiser la communication entre les machines afin que les différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles [3].

1.5.1.2. Modèle tcp/ip

Le sigle TCP/IP signifie "Transmission Control Protocol/Internet Protocol". Comme son nom l'indique, il provient des deux protocoles majeurs TCP et IP, qui représentent d'une certaine façon l'ensemble des règles de communication sur Internet et se base sur la notion d'adressage IP. En d'autres termes, c'est le fait de fournir des adresses IP à chaque machine du réseau afin d'acheminer des paquets de données. C'est un modèle inspiré du modèle OSI, il reprend l'approche en couches, mais en contient uniquement quatre, dont chacune correspond une ou plusieurs couches du modèle d'ouverture d'interconnexions des systèmes ouverts [3].

La figure (1.8) résume les deux modèles de communication ainsi que les différents rôles de chaque couche [1].

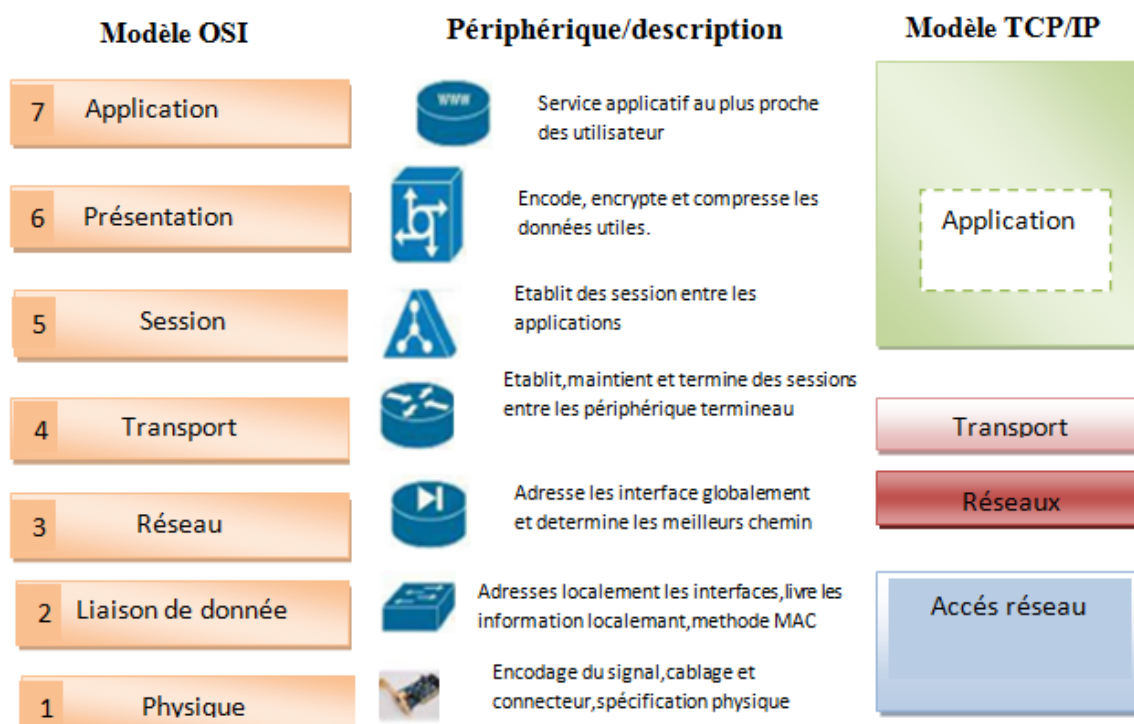


Figure 1.8: Les deux modèles de communication.

1.6. Adressage IP

Pour qu'une machine utilise les protocoles de la pile TCP/IP, elle doit contenir une adresse IP unique sur le réseau logique auquel elle appartient. C'est ce qu'on appelle l'adressage. L'objectif premier d'adressage est d'éviter la duplication accidentelle des adresses IP.

1.6.1 Classe d'adressage IP

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser l'acheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

Le tableau (1.10) résume les différentes classes d'adressage IP [19].

Classe	Plage d'adresse	Masque
A	1.0.0.0-127.255.255.255	255.0.0.0
B	128.0.0.0 – 191.255.0.0	255.255.0.0
C	192.0.0.0- 223.255.255.255	255.255.255.0
D	224.0.0.0-239.255.255.255	240.0.0.0
E	240.0.0.0-255.255.255.255	Non défini

Tableau 1.1 : Les différentes classes d'adressage.

1.6.2 Adresses IP privées

Ce sont des adresses utilisées dans le réseau local d'une entreprise, de plus les adresses IP privées ne peuvent pas être utilisées sur internet (car elles ne peuvent pas être routées). Chaque des classes A, B, C comprend une plage d'adresses IP privées comme suit :

Classes	Plage d'adresses
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Tableau 1.2 : Les classes d'adresses privés.

1.7. Sécurité informatique

De nos jours, la sécurité informatique est devenue un problème majeur dans la gestion des systèmes informatiques, en effet, ces derniers connaissent une grande évolution sur les plans d'échange d'informations et ouverture sur le monde extérieur [5].

1.7.1. Définition de la sécurité

La sécurité informatique est l'ensemble des moyens matériels et logiciels mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Cela explique une confidentialité dans les données [4].

1.7.2. Les principes de la sécurité

Les solutions de sécurité doivent contribuer à satisfaire au moins les critères suivants : authentification, confidentialité, intégrité, disponibilité et la non-répudiation [4].

- **L'authentification** : Elle consiste à vérifier l'identité présumée d'un utilisateur.
- **La confidentialité** : Elle garantit que les données ne soient lisibles et compréhensibles que par les personnes autorisées.
- **L'intégrité** : Elle assure que les informations ne sont pas altérées lors de la transmission.
- **La disponibilité** : C'est le fait qu'un utilisateur légitime doit pouvoir à un instant donné accéder aux ressources.
- **La non-répudiation** : Un utilisateur ayant effectué une action ne peut pas la nier après.

1.7.3. Vocabulaire de base de la sécurité informatique

Nous allons présenter dans ce qui suit, quelques mots clé qui sont abordé dans la littérature informatique lorsque la sécurité est abordée [5]:

- **Menace** : Evènement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage à un système donné.
- **Vulnérabilité** : C'est une faiblesse dans un système, qui peut être exploitée pour l'atteindre. Les vulnérabilités peuvent être dues à une erreur de configuration, de conception, ...etc.
- **Risque** : Association d'une menace aux vulnérabilités qui permettent sa réalisation [10].
- **Attaques** : Elles représentent les moyens employés pour exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité. Les attaques peuvent être classées en deux catégories [20] :
 - a) **Les attaques passives** : Dans ce genre d'attaques l'intrus intercepte les informations sans effectuer une modification.
 - b) **Les attaques actives** : Contraire mentaux attaques passives, dans le cas d'une attaque active l'intrus intercepte les informations et effectue l'une des actions suivantes :
 - **Interruption** : C'est une attaque liée à la disponibilité des informations. Dans ce cas l'intrus interrompt l'information.

- **Modification** : C'est un problème lié à l'intégrité des données car l'intrus modifie le contenu du message.
- **Fabrication** : C'est une attaque liée à l'authentification des individus. L'intrus fabrique un message et l'envoie à un utilisateur B se faisant passer pour A.
- **Politique de sécurité** : Pour assurer les services déjà cités, il est nécessaire de spécifier un ensemble de règles et d'outils servant à protéger les ressources et les informations contre toutes intrusions [20].

La politique de sécurité utilise un catalogue de fonctions de sécurité parmi lesquelles, nous pouvons trouver :

- L'identification des besoins en termes de sécurité.
 - La détection de vulnérabilité des systèmes.
 - La définition des actions à entreprendre en cas de menace.
 - L'évaluation du coût d'une intrusion réussite.
- **Mécanisme de sécurité** : Fonction de protection particulière, logicielle ou matérielle, mise en vigueur dans le cadre d'une politique de sécurité informatique.

1.7.4. Quelques attaques connues

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. Elles touchent généralement les trois composantes d'un système : la couche réseau, le système d'exploitation et la couche application. De plus, beaucoup d'attaques peuvent impacter le réseau de manière directe ou indirecte, en voici quelques-unes [6]:

- a) **Le DHCP Spoofing** : Le DHCP Spoofing est une fausse conation du serveur DHCP dans un environnement LAN qui alloue des adresses IP erronées. Le but de ce type d'attaques est de forcer un utilisateur à utiliser un faux serveur DHCP. Pour se faire un intrus va le simuler sur sa machine afin de répondre aux requêtes des clients avant que le vrai serveur le fasse. Donc il va configurer le client avec une fausse adresse IP, adresse de la passerelle et du serveur DNS. Pour l'adresse de la passerelle et du serveur DNS, il va utiliser l'adresse IP de sa machine. A ce moment à chaque fois qu'un client envoie un paquet, il va le recevoir.
- b) **Le sniffing** : Le but de ce type d'attaques est de récolter le maximum d'informations transitant sur le réseau (noms d'utilisateurs, mots de passe, . . .). En émet toute information transitée à travers le réseau peut être interceptée.

- c) **L'attaque par recherche exhaustive de la clé (brute force attack):** Un système Cryptographique ne cherche pas décrypter les informations. Il manipule un ensemble fini de clés (espace de clés), si ce dernier est petit alors un analyste peut les essayer une par une jusqu'à ce qu'il trouve la bonne clé.
- d) **L'attaque par dictionnaire :** C'est une méthode souvent utilisée en complément de l'attaque par force brute. Elle consiste à essayer une série de mots de passe contenus dans un dictionnaire en espérant trouver celui utilisé pour le chèrement, si ce n'est pas le cas, alors l'attaque échouera.
- e) **L'attaque de Middle Man (MM) :** C'est une attaque qui vise à intercepter les communications entre deux utilisateurs sans que ces deux derniers s'en aperçoivent. De ce fait l'attaquant peut lire, modifier les messages interceptés.
- f) **L'attaque par déni de service :** C'est une attaque qui a pour but de rendre un service offert par un serveur (web ou autres), un routeur ou un firewall indisponible, cela par la surcharge de la machine cible par des requêtes, jusqu'à ce qu'elle ne puisse plus traiter celles des utilisateurs.
- g) **Attaque du protocole ARP (ARP poisoning) :** Cette technique est utilisée pour rediriger le trafic réseau d'une ou plusieurs machines vers la machine du pirate en utilisant une faille du protocole ARP. Celui-ci permet de résoudre une adresse IP en une adresse MAC.

1.7.5. Principales technique de défenses

Tout appareil informatique qui contient des informations sensibles sera toujours sujet à une quelconque faiblesse qui pourra avec assez de moyens être exploitée par des forces malveillantes. Pour cela plusieurs niveaux de sécurité sont pris en mesure, tels que [21] :

- **Authentification** Est un mécanisme de sécurité qui consiste à assurer l'identité d'un utilisateur, ou d'une machine voulant accéder au système, ainsi on vérifie que la station ou la personne, est bien celle qu'elle prétend être. En effet dans la plupart de temps, l'authentification s'agit du couple « nom d'utilisateur/mot de passe », c'est un mécanisme qui constitue une sécurité relativement fiable lorsqu'il est bien mis en œuvre.
- **Le cryptage ou le chiffrement des données :** C'est aussi un mécanisme de sécurité, qui consiste à traduire un message clair, dit originel en un message incompréhensible, inintelligible. Le résultat du processus de cryptage est appelé « texte chiffré ou message codé », le processus de cryptage reposent à la fois sur des algorithmes puissants et sur les paramètres appelés clés.

- **Firewalls** : Afin de filtrer les échanges entre l'extérieur et l'intérieur des entreprises, celles-ci mettent en œuvre un ou plusieurs firewalls (pare-feu).
- **Audit** : Examen des renseignements et activités dans le but de s'assurer qu'ils respectent les contrôles établis et les procédures opérationnelles.
- **Logiciels anti-virus** (2/3 des attaques sont des virus) : Un antivirus est un **logiciel** informatique destiné à identifier et à effacer des logiciels malveillants (malwares en anglais), également appelés virus, Chevaux de Troie ou vers selon les formes.
- **Détection d'intrusions** : Est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.
- **Les VPNs (Virtual Private Network)** : Ce sont des systèmes permettant de créer un tunnel dédié aux utilisateurs distants a finalité d'échanger des données d'une manière confidentielle. Le mot tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc incompréhensibles par les personnes externes.
- **Les ACLs (Access Control List)** : Ce sont des fonctionnalités utilisées pour le contrôlée le filtrage du trafic circulant via une interface du routeur, en lui indiquant les types de paquets à accepter ou à rejeter. L'autorisation et le refus sont basés sur un ensemble de règles définit par un administrateur.
- **Les VLANs (Virtual Local Area Network)** : Ce sont des technologies qui permette de segmenter un réseau physique en réseaux logiques permis par le commutateur. Ce qui donne aux machines connectées à ce dernier d'agir indépendamment de leurs localisations. Les VLANs ont comme objectifs :
 - ✓ Augmentation de la sécurité.
 - ✓ Meilleure bande passante (diminuer le trafic inutile).
 - ✓ Faciliter l'administration du réseau.
 - ✓ Diminuer les collisions en augmentant les domaines de diffusion.

Plusieurs types de VLANs sont définis, selon le critère de commutation et le niveau auquel ils s'exécutent :

- **VLAN par port** : Appelé aussi VLAN de niveau 1. C'est le fait d'affecter les ports d'un commutateur à un VLAN.

- **VLAN par adresses MAC** : Nommé aussi VLAN niveau 2. Dans ce type, on éjectera a chaque VLAN, une ou plusieurs adresses MAC des machines connectées.
- **VLAN par sous réseau** : Qualifie VLAN de niveau 3. Ils associent des sous-réseaux IP par masque ou adresse. Les utilisateurs sont affectés dynamiquement à un ou plusieurs VLANs.
- **Port Security** : Afin de se protéger contre les attaques de type "switch ooding", CISCO à mis en place cette fonctionnalité qui consiste à restreindre l'entrée aux interfaces en limitant et en identifiant les adresses MAC des stations autorisées à accéder aux ports.
- **Les Certificats** : Ce sont des structures de données qui sont numériquement signées par une autorité de certification (CA : Certificat authority) Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification. Les certificats sont des petits fichiers divisés en deux parties : la partie contenant les informations et la partie contenant la signature de l'autorité de certification [4].

I.8. Conclusion

Dans ce chapitre, nous sommes partis des généralités sur les réseaux locaux, en suite, nous avons donné une vue globale sur la sécurité des réseaux informatique. Nous avons énuméré quelques attaques capables de porter atteinte à la disponibilité, l'intégrité ou la confidentialité d'un système. Nous avons donné les mécanismes, ainsi que les dispositifs de sécurité qu'une entreprise ou une organisation peut envisager mettre en place, dans l'objectif de fournir à son système un niveau de sécurité plus ou moins rassurant. Ces derniers sont appelés à être utilisés dans l'entreprise SONATRACH branche de transport par canalisation (RTC de Bejaïa) que nous présenterons dans le chapitre qui suit.

Chapitre 2

Etude de l'existant

2.1. Introduction

Sonatrach est l'une des entreprises les plus puissantes en Algérie et ce, grâce à son potentiel humain, matériel et au réseau informatique dont elle dispose.

Ce chapitre constitue pour nous l'une des parties essentielles de notre étude, qui consiste particulièrement à analyser les éléments qui composent le réseau local de l'entreprise SONATRACH branche de transport par canalisation (RTC de Bejaïa), ainsi que les problèmes qui ont une incidence sur son bon fonctionnement et sa sécurité.

A cet effet, selon les besoins nous pouvons concevoir une solution adéquate à implémenter.

2.2 Présentation de l'organisme d'accueil

2.2.1 Présentation de Sonatrach

SONATRACH créée le 31 décembre 1963 est vue comme étant la plus grande compagnie d'hydrocarbures en Algérie et en Afrique. Elle intervient dans l'exploration, la production, Le transport par canalisation, ainsi que la transformation et la commercialisation des hydrocarbures et de leurs dérivés. C'est un Groupe pétrolier et gazier qui détient en totalité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à industrie pétrolière tel que le forage et le raffinage. En 2004, SONATRACH s'est classée 1ère en Afrique et 12ème dans le monde parmi les compagnies pétrolières avec une production de 1,8 million de barils/jour et un chiffre d'affaire de 31,5 milliards de dollars. SONATRACH, entreprise citoyenne, œuvre à resserrer les liens sociaux, aider les populations dans le besoin, promouvoir la recherche et les activités scientifiques, aider la création artistique, promouvoir la pratique sportive, contribuer à la préservation de la nature et à la sauvegarde du patrimoine culturel et historique. Aujourd'hui SONATRACH ne conçoit pas de développement économique sans un développement durable [22].

2.2.2 Organigramme

Pour atteindre ses objectifs et optimiser son fonctionnement, l'entreprise Sonatrach a dégagé dès 1992 cinq secteurs d'activités de base résumées dans l'organigramme suivant :

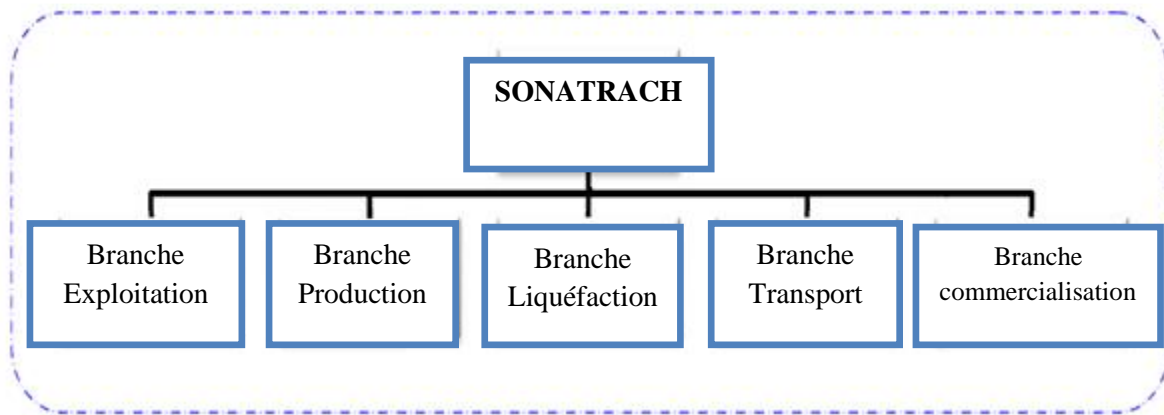


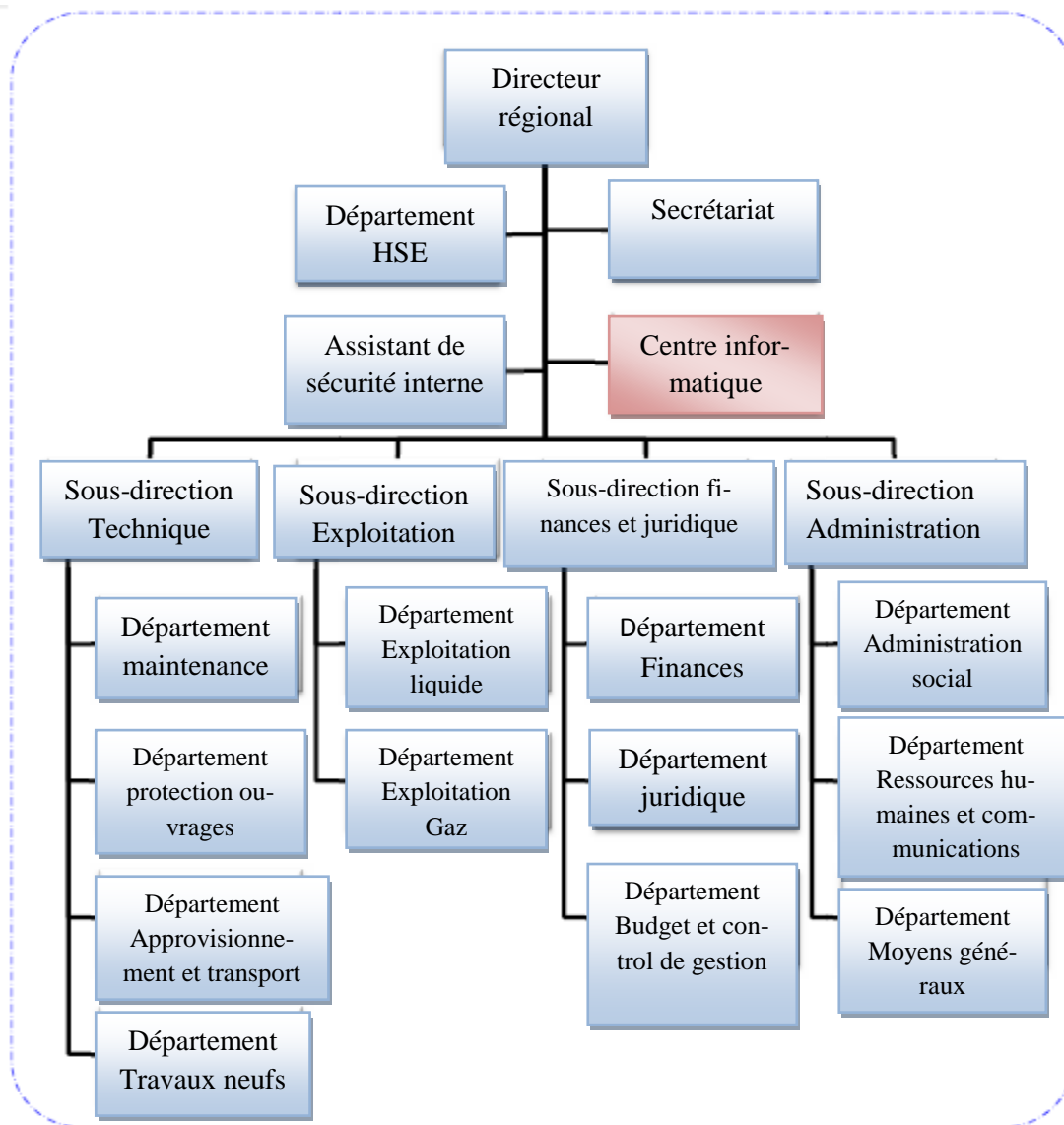
Figure 2.1 : Les branches de Sonatrach

La SONATRACH possède six directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Béjaia).
- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-EL-Hamra.
- La direction régionale d'Ain Amenas.
- La direction régionale Tebssa.

2.2.3. Présentation de la direction régionale de transport de Béjaia (RTC) (Branche de Transport par Canalisation)

La direction régionale de transport de Béjaia (RTC) est l'une des six directions régionales de transport des hydrocarbures de la SONATRACH.

a. Structure de la RTC**Figure 2.2 : Organigramme de la direction régionale de Bejaia**

Cette filiale se divise en 21 services, dont le service centre informatique sur lequel porte notre étude.

b. Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques afin d'assurer la gestion de la direction régionale de Bejaia(RTC) et des autres régions.

Le centre informatique de la RTC dispose de :

- ✓ 01 chef du centre informatique : Ingénieur système (SIQ).

- ✓ 01 chef de service système et réseau : Ingénieur système (SIQ) qui chapote un ingénieur système distribués (SPD) et un ingénieur informatique industriel (SIQ).
- ✓ 01 chef de service BDD (Base de données) et logiciel (Service développement) : Ingénieur SI qui chapote 04 ingénieurs systèmes d'information (SI).
- ✓ Chef de service Support technique (Service Exploitation) : Ingénieur (SI)

1. Organisation du centre informatique

L'organisation du centre ne cesse de subir des changements, et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois, afin de subvenir aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique est organisé en trois services tels qu'ils sont schématisés sur la figure II.3 :

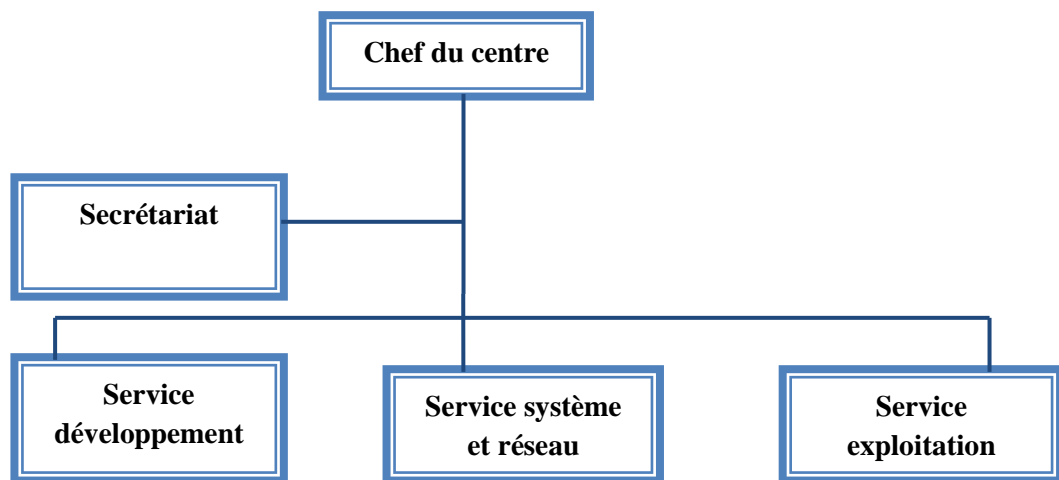


Figure 2.3 : Organigramme du centre informatique

2. Rôle de chaque service dans l'entreprise

Chaque service a des rôles et des tâches bien spécifiques :

- **Service développement**

Il est chargé de bénéficier des nouvelles technologies qu'il acquière tout en optimisant leurs utilisations, ainsi que la prise en charge des besoins des différentes structures de la direction en matière de développement de nouveaux systèmes d'informations :

- ✓ Analyse et conception ;
- ✓ Réalisation d'applications informatiques ;
- ✓ Administration des bases de données de l'entreprise.

- **Service système et réseaux**

Il est chargé d'assurer les tâches suivantes :

- ✓ L'administration des serveurs ;
- ✓ Administration des bases de données de l'entreprise ;
- ✓ Installation des logiciels sur les serveurs ;
- ✓ Gestion des performances système et réseau ;
- ✓ Gestion de la sécurité et des utilisateurs connectés au réseau (droits d'accès) ;
- ✓ Gestion du parc informatique ;
- ✓ La prise en compte et résolution des pannes ;
- ✓ Planification et ordonnancement des travaux ;
- ✓ Sauvegarde et restauration des données ;
- ✓ Gestion des espaces disques ;
- ✓ Exploitation (saisie, validation, traitement) des anciennes applications batch pour la DRGB et les autres directions régionales.

- **Service exploitation**

Ce service a pour rôle d'exploiter les anciennes applications qui tourne sur COBOL, la Centralisation des bilans pour la branche transport et la gestion de la paie des temporaires.

2.3 Présentation du réseau de RTC

Le réseau informatique de la RTC de Bejaïa est constitué de deux bâtiment (figure2.4), l'ancien bâtiment qui dispose d'une topologie physique en étoile étendue (voir figure II.4), et le nouveau bâtiment dont la topologie physique est hybride (en étoile et en annaux). Le type de lien entre ces deux derniers est la fibre optique.

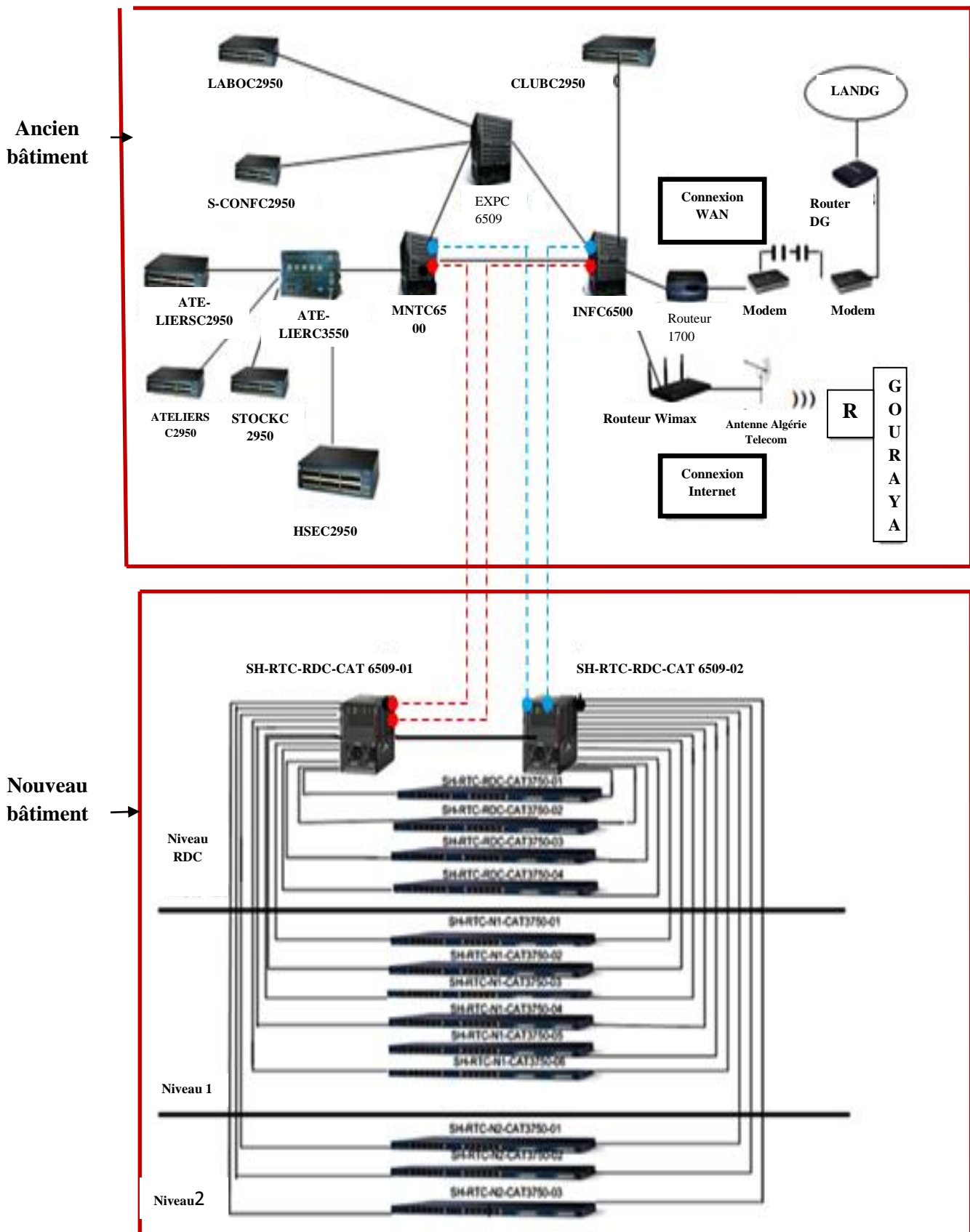


Figure 2.4 : Liaison entre l'ancien et le nouveau bâtiment.

2.3.1. Equipements et matériels réseau

Nous allons présenter les équipements réseaux de la RTC de Bejaïa.

2.3.1.1. Infrastructure du réseau de RTC

Le tableau suivant montre la liste des équipements et armoires du réseau de la RTC:

BLOC	ARMOIRE	EQUIPEMENT
Bloc principale	ARM 01 (Salle informatique)	Cisco cat 6500 + un Routeur d'accès à distance
Bloc principale	ARM 02 (Salle n°)	Cisco cat 6500 et Cisco cat 2950
Bloc principale	ARM 03	Cisco cat 6509
Bloc atelier	ARM 04(l'atelier)	Cisco cat 3550
Le club	ARM 05(bloc de club)	Cisco cat 2950
La salle des conférences	ARM 06(salle de réfé- rence)	Cisco cat 2950
Laboratoire	ARM 07(Laboratoire)	Cisco cat 2950
Le stock	ARM 08(bloc de stock)	Cisco cat 2950
Le bloc PTO	ARM 09(bloc de PTO)	Cisco cat 2950

Tableau 2.1 : La liste des équipements et armoires du la RTC.

Tous les équipements actifs (catalyst 6509, catalyst 3750, routeur voix, routeur internet, serveur ACS, voie mail) sont physiquement installés à ce niveau.

- ✓ Les équipements réseaux sont hébergés dans une armoire de brassage équipée (câblage, ventilation, espacement, . . .).
- ✓ Un USP est installé dans chaque armoire afin de protéger les équipements réseaux installés (Switch, routeur, serveur).
- ✓ Chaque salle qui héberge les armoires de brassage est dotée d'une climatisation suffisante.

2.3.1.2. Les commutateurs utilisés dans le réseau de la DRGB (Direction Régionale de Transport de Bejaia)

Le réseau de la DRGB contient deux types de commutateurs :

- **Des commutateurs intelligents**

En plus de leur fonction ils peuvent faire le routage. Dans le réseau de la DRGB, on trouve trois exemples de ce type qui sont :

- **Catalyst 6500**

C'est une gamme de commutateurs CISCO qui offre des performances et une densité de ports évolutives sur un large choix de configurations de châssis et d'interfaces LAN/WAN/MAN.

- **Catalyst 3750**

C'est une gamme de commutateurs CISCO qui améliore l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables.



Figure 2.5 : Catalyst Cisco 3750

- **Catalyst 3550**

C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation du réseau.



Figure 2.6 : Catalyst Cisco 3550

- **Des commutateurs non intelligents (hub)**

Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la DRGB (Direction Régionale de Bejaia) contient le type suivant :

- **Catalyst 2950**

C'est une gamme de commutateurs CISCO destinée à la commutation d'étages d'édifiée Ethernet 10/100/1000 Mbits/s fixe, offrant des performances, une souplesse et une administration exceptionnelles.



Figure 2.7 : Catalyst Cisco 2950

2.3.1.2. Les routeurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB contient les deux types de routeurs suivants :

- **CISCO 1700**

C'est une gamme de routeurs d'accès modulaires souples et s'sécurisés utilisée lorsqu'il s'agit de réseaux WAN.



Figure 2.8 : Routeur Cisco 1700

- **CISCO 800**

C'est une gamme de routeurs à services intégré haut d'débit qui permet aux petits bureaux d'exploiter des services sécurisés simultanés comme le pare-feu, les VPN et les réseaux LAN sans fil.

- **Routeur wimax**

Wimax est un standard de transmission sans fil à haut débit, il est prévu pour connecter les points d'accès Wi-Fi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut-débit vers de multiples utilisateurs.



Figure 2.9 : Routeur wimax

II.3.1.3. Définition d'autres équipements réseau

- **Routeur wifi 4400**

Les contrôleurs WLAN CISCO 4400 sont particulièrement adaptés au déploiement des réseaux locaux sans fil d'entreprise, et fournissent à l'ensemble du système des fonctions WLAM comme les politiques de sécurité, les préventions d'intrusions, la gestion RF, la qualité de service (QoS) et la mobilité



Figure 2.10 : Routeur wifi 4400

- **Routeur téléphonie IP 3825**

La téléphonie IP est un mode de téléphonie dans lequel la voie est numérisée puis acheminée par le protocole TCP/IP sous forme de paquet de données. Dans la téléphonie IP 3825 tous les téléphones/user sont gérés directement en IOS, on peut gérer les droits d'appels, supervision de lignes, groupement de poste, par contre pas de redondance, on ne peut pas mettre énormément de téléphones, c'est orienté PME à fond.



Figure 2.11 : Routeur téléphonies IP 3825

2.3.2. Les VLAN utilisés dans la RTC

Pour faciliter la gestion, le réseau local est segmenté en plusieurs VLANs, dont chacun est assigné à un emplacement géographique, à un serveur ou par service comme représenté dans le tableau (II.2). Concernant l'adressage IP, l'entreprise utilise une plage d'adresses publiques de classe A héritée de l'association partenaire étrangère British Pétroleum (BP). Pour des raisons de sécurité exigée par l'entreprise, on ne peut pas divulguer l'adressage.

Les VLANS	Description
1	Serveur LMS
2	Assistant de sécurité interne
3	Département HSE
4	Centre informatique
5	Sous-Direction technique
6	Sous-Direction exploitation
7	Sous-Direction administration
8	Sous-Direction finance et juridique
9	La Direction
10	Serveur (application, active directory, messagerie et fichier)
11	Print serveur
12	Club, Salle de conférence, laboratoire, Atelier, PTO et Stock
13	IVR et call manager
14	Serveur Web
15	WIFI
16	Serveur (websense et Proxy)
17	Serveur de BDD

Tableau 2.2 : La liste des VLANs du réseau local de l'entreprise RTC.

2.4. Service de la sécurité de la RTC

Les administrateurs réseau de la RTC ont veillé à la sécurité de celui-ci et cela dans différentes approches :

- ✓ Sécurité des locaux.
- ✓ Sécurité du réseau local.
- ✓ Contrôle d'accès applicatif.
- ✓ Contrôle de l'intégrité des données.
- ✓ Confidentialité des données.
- ✓ Disponibilité des données.
- ✓ La sécurité logique des équipements.
- ✓ Les plans de secours.
- ✓ Les plans de sauvegarde.
- ✓ Authentification.
- ✓ Contrôle d'accès.
- ✓ Configuration des logiciels.
- ✓ La maintenance.

2.4.1. Serveur antivirus " F-Secure "

Les solutions de sécurité F-Secure pour serveurs protègent contre les virus et autres menaces et empêchent les machines infectées de propager leurs virus sur le réseau. Le serveur F-Secure offre la possibilité de gestion à distance à partir d'un emplacement central unique.

C'est cette gestion qu'utilise la RTC pour effectuer des mises à jour à partir d'un seul poste centralisé et de les transmettre à tous les autres postes via ce serveur.

II.4.2. Serveur filtrage web

Permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires dans le site de l'entreprise RTC.

II.4.3. Serveur reporting

C'est un outil complet et de rapport faciles à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise RT C.

II.4.4. Firwall juniper SSG 550

Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements de bureau régional et de leurs branches.

- **La zone strust**

C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confié son réseau LAN.

- **La DMZ (Demilitarized Zone)**

C'est une zone tampon d'un réseau de l'entreprise, située entre le réseau local et Internet derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Pour des besoins d'administration et d'organisation, la zone DMZ de la RTC est partitionnée en trois sous zones :

- ✓ **La DMZ administrateur (admin) :** Contient une station administrateur.
- ✓ **La DMZ filtrage :** Contient un proxy Blue Coat qui est une fonction destinée essentiellement aux environnements LAN. Il stocke les pages les plus demandées et apporte les avantages suivants :
 - Authentification des utilisateurs et gestion des droits d'accès.
 - Optimisation de la bande passante entre le provider et votre réseau.
 - Amélioration des temps d'accès aux sites.
- ✓ **La DMZ renverse proxy :** Fonction destinée aux environnements d'hébergement. Le cache est déployé en amont des serveurs et permet d'adresser une requête directement sur le cache sans solliciter les serveurs (les rendant ainsi plus disponibles pour des tâches plus valorisantes telles l'accès aux bases de données, le backup et l'accès aux pages dynamiques, . . .).

2.5. Câblage informatique

Le système de câblage informatique installé au bloc de SONATRACH est conçu pour fonctionner de façon optimale pour permettre des évolutions futures. Tout équipement informatique existant dans la société est interconnecté via le câblage de type paire torsadé catégorie 6.

2.6. Problématique

L'accès au réseau filaire de l'entreprise examinée est autorisé pour toute personne que ce soit : employé, consultant, missionnaire, visiteurs, stagiaires, etc. En effet, une personne peut brancher un périphérique non géré dans le lieu de travail (point d'accès, ordinateur personnel ou autres), alors que ceci constitue une faille de sécurité telle que l'accès illégal aux données confidentielles ou même causée de graves perturbations dans le fonctionnement du réseau.

Vu la dispersion des utilisateurs dans les différents locaux de l'entreprise, les liaisons réseaux sont présentes un peu partout, et leur nombre est en perpétuelle évolution, ce qui rend l'accès au réseau facile et donc difficile à contrôler et à sécuriser.

La solution actuelle, est un boîtier (Appliance Cisco ASC 4.0) qui gère l'authentification 802.1X sur les équipements, les points d'accès wifi et le réseau filaire en corrélation avec active directory 2003 server.

Les impératifs de veille technologiques, oblige l'entreprise à migrer AD 2003 vers AD 2016. Cette opération aura un impact direct sur l'authentification 802.1X, tant, l'Appliance CISCO ASC 4.0 ne prend pas en charge AD 2016. Aussi et pour répondre à cette problématique, il nous a été demandé de mettre en œuvre la solution d'authentification 802.1X en tenant compte de la dite migration.

Pour ce faire, notre choix c'est vite posé sur l'implémentation d'une solution basée sur les services NPS ; Le serveur de stratégie réseau (NPS, Network Policy Server) nous permet de configurer et de gérer des stratégies réseau de manière centralisée à l'aide des trois composants suivants : serveur RADIUS, proxy RADIUS et serveur de stratégie de Protection d'accès réseau. La communication avec active directory est assurée de façon implicite.

2.7. Conclusion

Ce chapitre a été consacré pour la présentation de l'organisme d'accueil de SONATRACH. En effet, nous avons présenté la RTC et sa structure, l'Organigramme du centre informatique et le Rôle de chaque service. Par la suite, Nous avons mis en relief les points faibles de la sécurité que présentent ces structures pour proposer ensuite une solution.

Cette solution est détaillée dans le chapitre qui suit.

Chapitre 3

Solution proposée

3.1 Introduction

L'information étant une ressource stratégique pour l'entreprise, sa protection est indispensable. Ainsi la sécurisation du Système d'Information de celle-ci repose sur des solutions ou des équipements qu'elle-même maîtrise. Malgré tout, il reste la possibilité d'une connexion à partir d'un ordinateur personnel sur le réseau de l'entreprise.

Il est donc obligatoire de mettre en place une solution permettant de se connecter au système d'information tout en assurant la sécurité de celui-ci.

L'entreprise SONATRACH souhaite que la solution à sa problématique réponde à l'objectif suivant : vérifier l'identité des équipements voulant se connecter à son réseau afin de les autoriser ou non à se connecter. Cette identification va être rendue possible par l'utilisation du standard 802.1X qui effectue une authentification de l'équipement client au moment de la connexion physique au réseau.

Dans le cadre de ce chapitre, nous allons décrire le fonctionnement de la solution de sécurité proposée, nous décrirons également les différents protocoles qui interagissent pour assurer l'authentification.

3.2. Authentification

L'authentification consiste en l'identification et la vérification de l'identité. Dans le contexte des réseaux informatiques, authentifier une entité permet de s'assurer que l'entité est bien celle qu'elle prétant être [7].

L'autre aspect que doit garantir l'authentification est la confidentialité entre les entités. Les échanges entre les deux entités doivent être protégées pour éviter le vol d'identité. Nous utilisons généralement EAP (RFC 3748) comme protocole de cryptage [7].

Il existe plusieurs protocoles utilisant des mécanismes d'authentifications [7] :

- IP sec.
- SSL : Secure Socket Layer.
- 802.1X.
- EAP.

Notre solution s'appuie sur l'authentification basé sur le standard IEEE 802.1X.

3.3. Structure générale de notre solution

La structure de notre solution s'articule autour d'un certains nombre de vlans qui sont décrits comme suit :

- **Vlan 99** : C'est le vlan nommé management. Il est assigné à l'administrateur réseau pour qu'il fasse les configurations nécessaires dans le réseau. Ce vlan accorde un accès à toutes les ressources du système.
- **Vlan 10** : C'est le vlan qualifié d'Isolation. Ce dernier est le vlan dans lequel sont placés les postes de travail enregistrés qui violent la politique de sécurité. Comme son nom l'indique, les postes de travail de ce VLAN sont isolés et n'ont pas accès au réseau.
- **Vlan 20** : C'est le vlan nommé no-authenticated-vlan, il est assigné aux utilisateurs dont le standard IEEE 802.1X est désactivé. Dans ce cas, le client aura un accès limité au réseau.
- **Vlan 30** : C'est le vlan baptisé authentication-vlan. Il est assigné aux utilisateurs conforme (dans notre cas, conforme veut dire appartenir au domaine et 802.1X activé) qui auront un accès au réseau.
- **Vlan 40** : C'est le vlan nommé Guest, il est assigné aux visiteurs (Ils n'appartiennent pas au domaine, par contre le 802.1X est activé). Ils auront, dans ce cas, un accès limité au réseau .

Le tableau (3.1), résume l'ensembles des vlans avec l'adresse ip affectée à chacun d'eux.

ID VLAN	Nom VLAN	ADRESSE IP	MASQUE
99	Management	10.10.99.0	255.255.255.0
10	Isolation	10.10.10.0	255.255.255.0
20	NO-Authenticated-vlan	10.10.20.0	255.255.255.0
30	Authenticated-vlan	10.10.30.0	255.255.255.0
40	Guest-vlan	10.10.40.0	255.255.255.0

Tableau 3.1 : Liste de vlans utilisés dans la nouvelle architecture.

3.3.1. Déroulement de notre solution

Lorsqu'un client branche un câble à son ordinateur, ce dernier ne possède pas une adresse IP et avant toute authentification, le supplicant (client filaire) ne peut communiquer qu'avec le

switch (système authentificateur). Le protocole utilisé pour cette communication est le protocole EAPoL (Extensible Authentication Protocol Over LAN).

Après cette communication, dans le cas de notre solution, plusieurs scénarios peuvent se présenter selon le cas du client :

Scenarios1 :

Le supplicant (suppliant) n'est pas configuré pour la 802.1x, l'authentificateur ne reçoit pas de réponse à ses requêtes d'identité, après un temps d'attente, il récupère l'adresse MAC du demandeur qui sera envoyé au serveur d'authentification(RADIUS dans notre cas) via une communication basée sur le protocole IP (message radius) qui a son tour, répond par un « radius reject », le client est alors assigné à un vlan isolation (vlan10), Ou par un « radius accept », dans cette dernière situation, selon notre solution, 3 scénarios se présentent :

Scenarios 2 :

Si le demandeur appartient au domaine et le protocole IEEE 802.1X est activée (client conforme),ce dernier sera alors assigné au vlan « authenticated-vlan » là où il aura accès au réseau(selon ses droits d'accès).

Scenarios 3 :

Dans le cas où le demandeur appartient au domaine, par contre la 802.1x n'est pas activée, il sera non authentifié. Dans ce cas, le supplicant sera alors assigné au vlan « no-authenticated-vlan » dont l'accès réseau est limité (vlan 20 dans notre cas).

Scénarios 4 :

Le demandeur est un PC qui n'est pas du domaine ni d'un employé qui a un compte utilisateur. Dans ce cas il est assigné à un VLAN "guset" (vlan40).

L'organigramme dans la figure (3.1) résume le déroulement de notre solution.

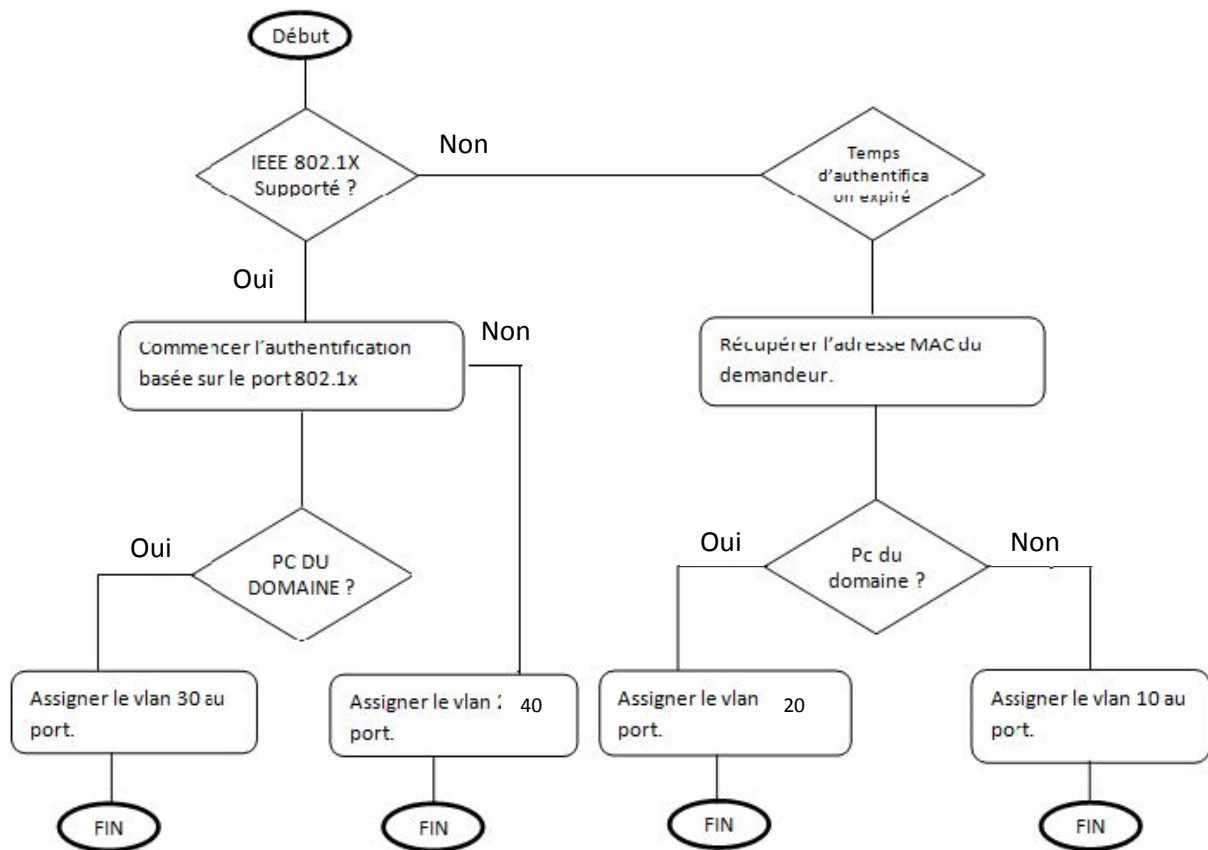


Figure 3.1 : Déroulement de notre solution.

3.4. Le protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-IN User Service), est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients [8].

Le protocole Radius repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Serveur), l'ensemble des transactions entre l'utilisateur final et le serveur RADIUS sont chiffrées et authentifiées grâce à une clé partagée [8].

Le fonctionnement du protocole RADIUS (figure 3.2) est basé sur un scénario proche de celui-ci [7] :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.

- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénarios d'identification demandé pour l'utilisateur, soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

Le serveur RADIUS retourne ainsi une des trois réponses suivantes :

- **ACCEPT** : L'identification a réussi.
- **REJECT** : L'identification a échouée.
- **CHALLENGE** : Le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose ainsi « un défi ».

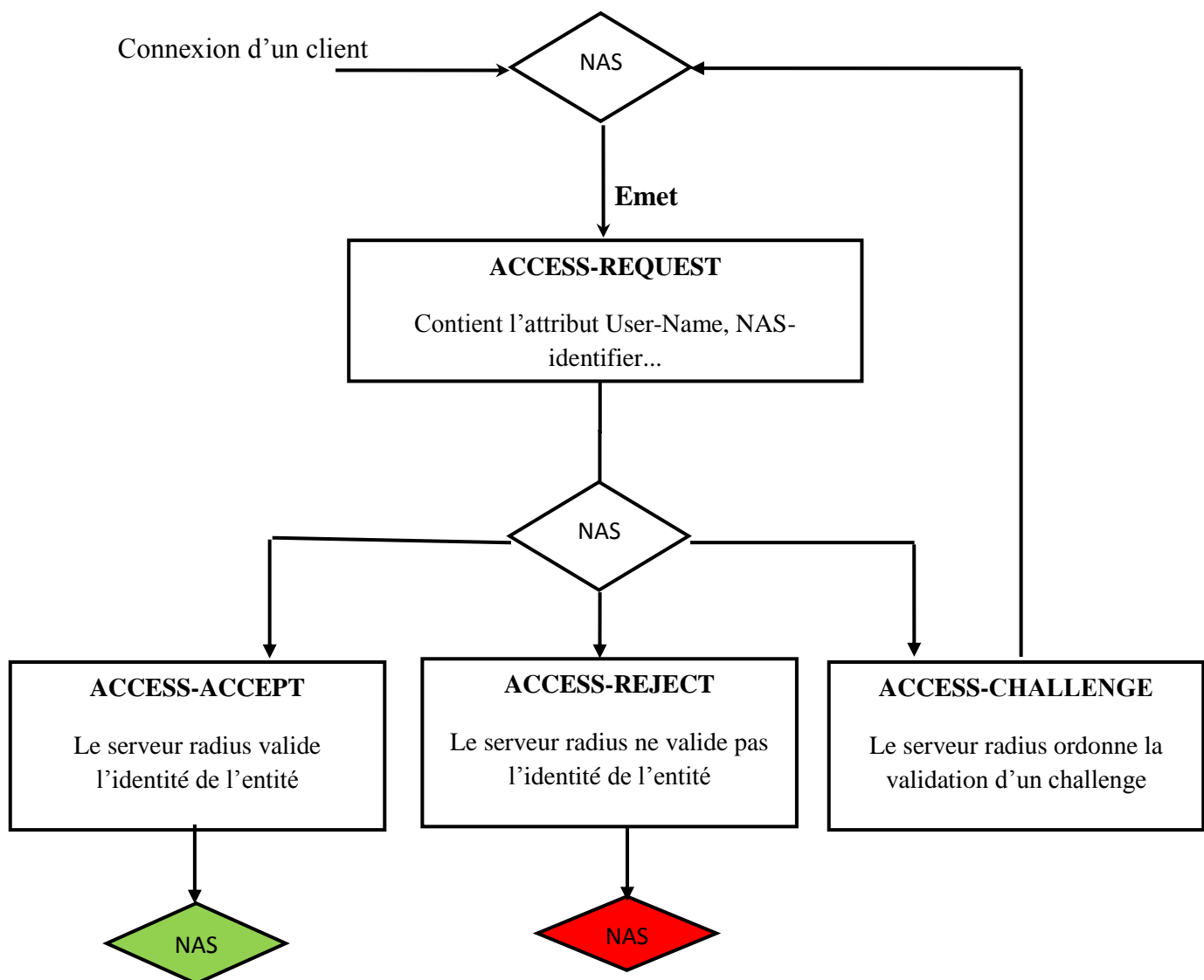


Figure 3.2 : Messages RADIUS.

3.4.1. Le protocole RADIUS dans le modèle OSI

Le protocole RADIUS se situe au niveau des couches hautes, dans la couche applicative du modèle OSI. Il se place au-dessus de la couche transport. Les données du protocole RADIUS sont acheminées par des segments du protocole UDP et encapsulées dans des paquets IP. Les ports d'écoute UDP utilisés pour accéder aux services proposés par le protocole RADIUS sont les suivants [6] :

- 1812, reçoit les requêtes d'authentification et d'autorisations ;
- 1813, reçoit les requêtes d'«accounting » (comptabilité).

La figure (3.3) illustre le format d'un paquet RADIUS.

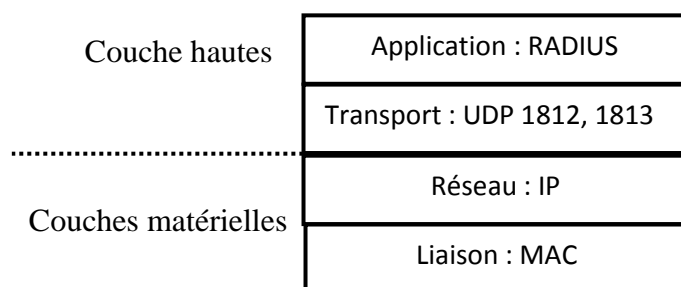


Figure 3.3 : Le protocole RADIUS au sein du modèle OSI.

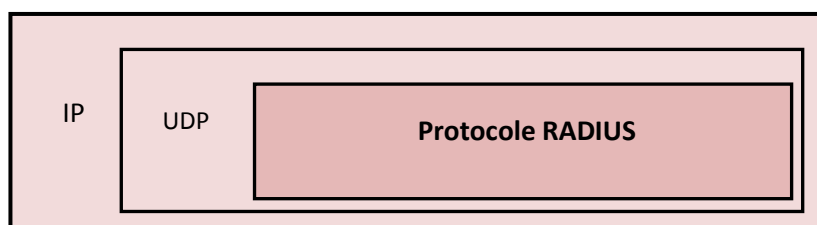


Figure 3.4 : Encapsulation du Protocole RADIUS.

3.4.2. Format des paquets RADIUS

Le protocole RADIUS utilise un format de paquet bien défini pour réaliser les transactions d'authentifications, d'autorisations et de comptabilités. Le modèle des données RADIUS contient les champs ci-contre (figure 3.5) [9]:

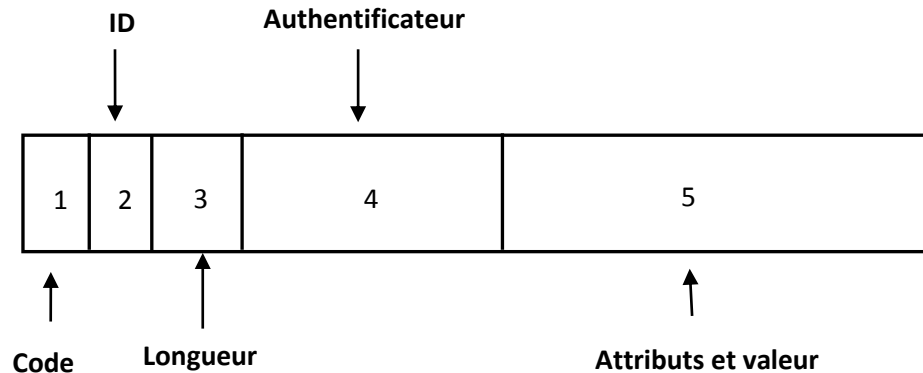


Figure 3.5 : Format des trames RADIUS.

1. **Code** : Ce champ identifie le type du paquet RADIUS. Il existe plusieurs types, mais nous allons citer juste ceux qui nous intéressent dans notre projet :
 - Lorsque la valeur du code est à 1, alors le paquet est de type "Access-Request" ;
 - Valeur=2, le paquet est de type "Access-Accept" ;
 - Valeur=3, le paquet est de type "Access-Reject" ;
 - Sinon, si la valeur est égale à 11 alors le paquet est de type "Access-Challenge".
2. **ID** : Ce champ permet au client RADIUS d'associer à chaque valeur du code la réponse qui convient.
3. **Longueur** : Ce champ contient la longueur totale des données RADIUS.
4. **Authentificateur** : Ce champ permet de vérifier l'intégrité des paquets envoyés par le serveur RADIUS. Il est calculé de manière aléatoire à partir d'un secret partagé (mot de passe connu par le serveur et le client) entre le client et le serveur. Ainsi, le client RADIUS peut s'assurer que la réponse lui provient bien du serveur RADIUS.
5. **Attributs et Valeurs** : Ce champ contient la charge utile du protocole RADIUS. Il est de longueur variable en fonction des couples d'attributs/valeurs envoyés par le client RADIUS en requête ou par le serveur RADIUS en réponse.

3.5. La technologie IEEE 802.1x

La norme 802.1X est un standard qui a été créé dans le but de sécuriser les réseaux locaux filaires ou sans-fil. Il a été mis au point par l'IEEE en 2001. Il est mis à jour régulièrement, d'ailleurs sa dernière révision date de 2010. L'objectif de 802.1X est de délivrer, ou non, un droit d'accès au réseau, ceci sans se soucier du support physique utilisé. En effet, 802.1X travaille au niveau de la couche 2 du modèle OSI et ne requiert pas l'utilisation de la couche 3 (couche IP). En général, l'accord du droit d'accès permet ensuite

d'utiliser le protocole Ethernet et de permettre également l'accès à divers mécanismes d'auto-configuration, que ce soit un démarrage depuis le réseau ou une configuration IP attribuée automatiquement [10].

3.5.1 Description du protocole IEEE 802.1x

Le protocole 802.1x est composé de trois entités qui interagissent pour le processus d'authentification [11]:

- **Le système à authentifier (Supplicant)** : C'est l'utilisateur final connecté directement au switch qui demande l'autorisation d'accéder au réseau. Il peut être un PC bureau, un PC portable ou un téléphone IP, etc.
- **Le système authenticateur (Authenticator)** : C'est un équipement réseau (commutateur, routeur, borne wifi ...) qui agit comme une barrière de sécurité entre le Supplicant et le réseau protégé. Il sert de relais entre le Supplicant et le serveur d'authentification et gère le PAE (Port Access Entity) qui permet au Supplicant d'accéder ou non au réseau.
Le système authenticateur surveille l'état d'un support physique dans l'attente d'un client à authentifier qui souhaite disposer des ressources associées à ce même support. Une fois la demande reçue, il fait le relais avec le serveur d'authentification sans s'immiscer dans le dialogue client/serveur, il ne fait qu'attendre la décision du serveur qui lui est destinée [10].
- **Le serveur d'authentification (Authentication Server)** : Il s'agit d'un serveur RADIUS, qui applique les règles d'accès qui ont été définies. Ces règles sont nécessaires pour la prise de décision d'autorisation sous forme d'une réponse (acceptation ou rejet) [11].

La figure (3.6) illustre les trois entités qui interagissent dans le protocole 802.1X [6].

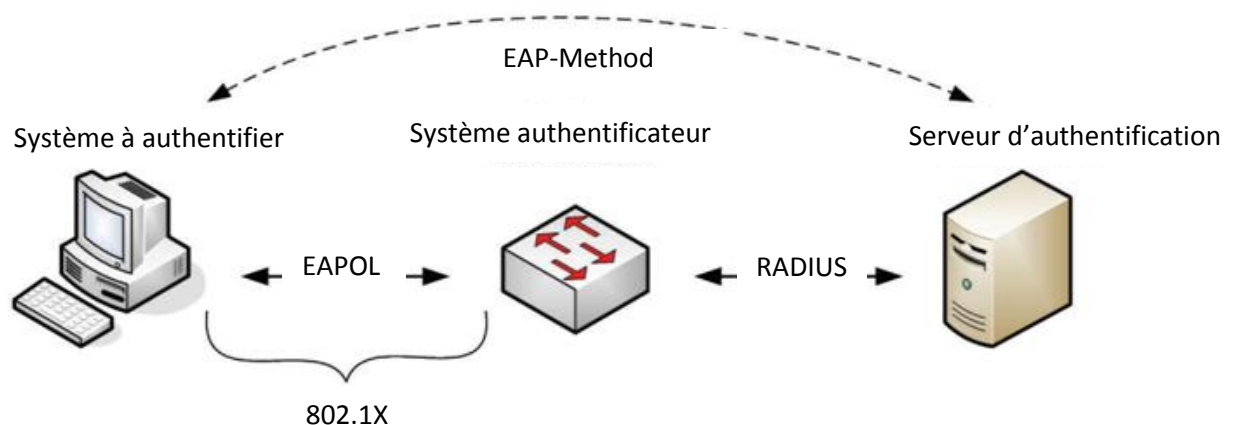


Figure 3.6 : Les trois entités qui interagissent dans le protocole 802.1X.

3.6. Le protocole d'authentification EAP

Extensible Authentication Protocol a été prévu à l'origine pour fournir une authentification (extensible) pour PPP. Il ne nécessite pas de couche IP pour fonctionner. Il a ensuite été utilisé pour 802.1X, et les réseaux sans-fil. EAP étant comme son nom l'indique extensible, nous allons rapidement parler de ses déclinaisons [10].

- **LEAP** : LEAP signifie « Light Extensible Authentication Protocol », qui se traduit par : version allégée de EAP. C'est une implémentation propriétaire d'EAP développée par Cisco. Lorsque que les mots de passes utilisés sont complexes, il est également très sûr. Ce qui a été mis en doute en cas d'utilisation d'un mot de passe faible. On préférera donc à sa place PEAP, EAP-TLS ou EAP-FAST pour l'aspect plus sécurisé de ces implémentations. LEAP n'est d'ailleurs pas supporté sur Windows sans l'ajout d'un client spécifique. Il est cependant largement supporté sur les points d'accès Wifi.
- **PEAP** : PEAP signifie « Protected Extensible Authentication Protocol ». PEAP est une des implémentations d'EAP les plus utilisées. Elle utilise le protocole CHAP pour authentifier de façon sécurisée un client grâce au challenge request/response. Windows Server utilise cette version d'EAP et elle est utilisée dans notre projet.
- **EAP-TLS** : EAP-TLS utilise un système d'authentification avec certificats. C'est donc l'un des meilleurs en termes de sécurité. Son désavantage réside dans le fait qu'un certificat doit être obligatoirement installé chez le client.
- **EAP-TTLS** : EAP-TTLS fonctionne sur le même principe que la version ci-dessus, à la différence que le client ne nécessite pas de certificat de son côté. Un tunnel encrypté est créé à l'aide du certificat du serveur afin d'échanger les informations d'authentification.
- **EAP-FAST** : FAST veut dire « Flexible Authentication via Secure Tunneling ». C'est une version améliorée de LEAP qui utilise PAC (Protected Access Credential), un set d'informations d'authentification qui ne peut pas être copié d'une machine à une autre. Il corrige le manque de sécurité qu'on attribue souvent à LEAP.

3.7. Vue d'ensemble et fonctionnement

La 802.1X est un mécanisme basé sur l'authentification au niveau des ports physiques. En effet dans ce mécanisme les ports physiques sont scindés en deux ports virtuels. Le premier permet l'accès au réseau, il est contrôlé et il peut être fermé ou ouvert à la communication [12].

Le second port est dédié aux trames 802.1X. Il permet la communication avec le serveur d'authentification. Un port fermé n'autorise que les trames EAPOL. Les trames EAPOL seront enfin réencapsulées grâce à l'authentificateur direct dans des trames RADIUS compréhensibles par le serveur d'authentification [12].

Le chronogramme dans la figure (3.7), résume les points abordés dans les parties précédentes. Nous avons représenté une authentification qui réussit [7].

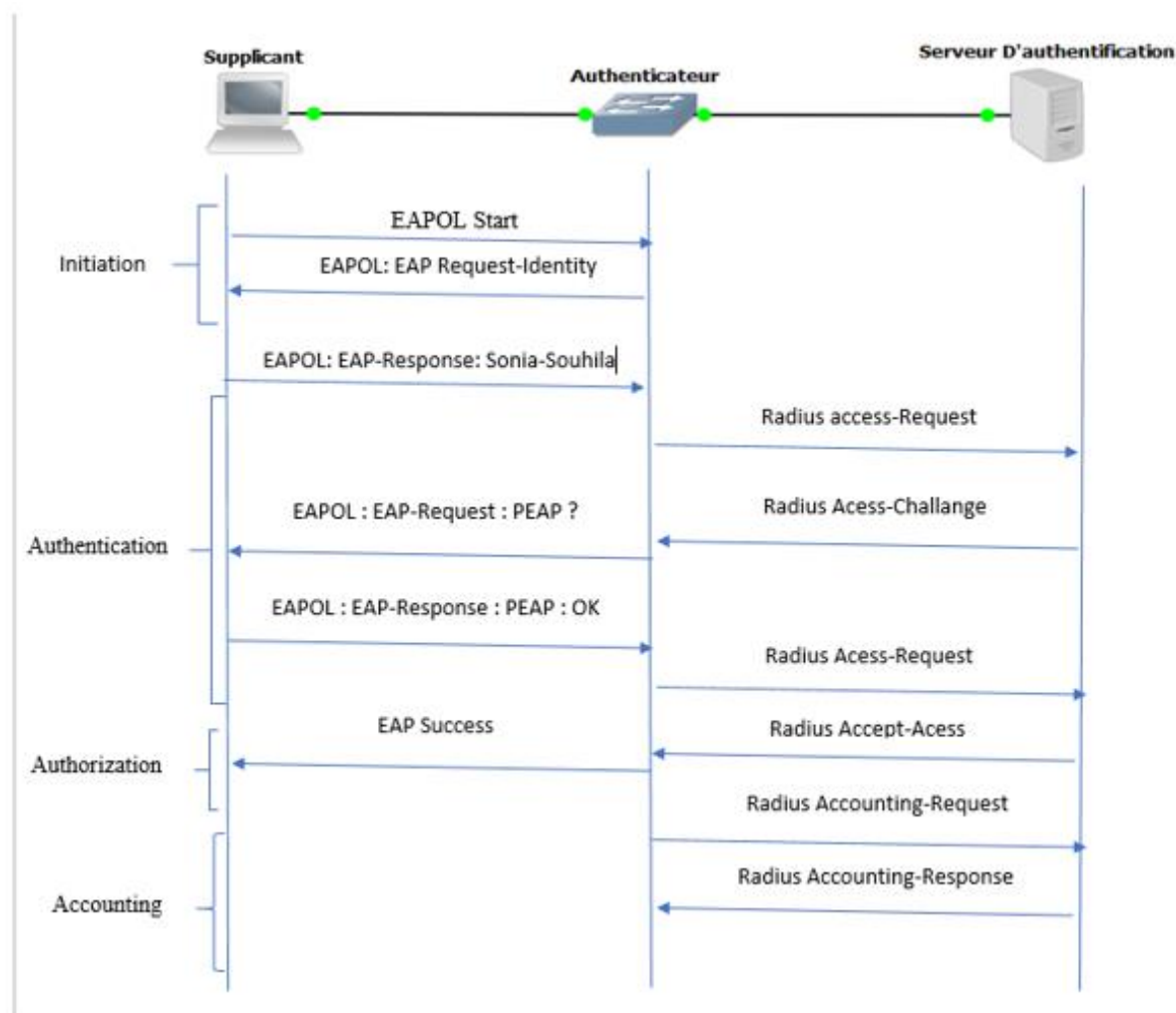


Figure 3.7 : Fonctionnement de la 802.1X.

Comme nous pouvons le constater sur la figure (3.7), trois entités interagissent dans le fonctionnement du protocole 802.1X.

Un périphérique (supplicant) branché au switch (authentificateur direct) n'a pas un accès au réseau standard jusqu'à ce qu'il soit authentifié. Concrètement, une communication s'établit entre ces deux grâce au protocole EAP qui permet de transporter les trames EAPOL vers le commutateur pour qu'elles soient enfin réencapsulées dans des trames RADIUS

compréhensibles par le serveur d'authentification. A noter que l'authentificateur direct enlève l'en-tête de la trame EAPOL et aucun changement du contenu durant l'encapsulation. Une fois que le serveur d'authentification vérifie l'identité du demandeur, il répond par des trames RADIUS à l'authentificateur direct qui place le client dans le VLAN adéquat. En revanche, le fonctionnement de la 802.1X se fait en quatre étapes et selon quatre types de messages EAP qui permettent de réaliser l'authentification d'un client sur un serveur [12].

1. Initiation (initiation) :

C'est l'étape essentielle où le demandeur prend contact avec son authentificateur direct. L'initiation se déclenche une fois que le switch détecte qu'un demandeur est branché sur l'un de ses ports contrôlés. A ce moment il va envoyer une requête "EAP Request-identity" pour lui demander son identité. Si ce dernier ne répond pas, il va retransmettre la requête après un temps d'attente.

L'initiation peut se déclencher par le demandeur en envoyant une requête "EAPOL Start « dans l'un des cas suivants:

- Le supplicant n'est pas prêt pour recevoir les requêtes "EAP Request", par exemple dans le cas où le PC est en cours de démarrage.
- Il n'existe pas un lien direct entre le demandeur et le switch (le demandeur est connecté indirectement au switch via un hub).

2. Authentification (authentication) :

Avant de commencer, il faut savoir que le serveur d'authentification et l'utilisateur final se sont mis d'accord sur l'une des méthodes EAP (dans notre cas nous avons choisi PEAP).

Dans cette étape, le switch achemine les messages EAP entre l'utilisateur final et le serveur d'authentification en les encapsulant dans des trames EAPOL ou RADIUS.

3. Autorisation (authorization) :

Lors de cette étape, si le demandeur soumet une identification valide, le serveur d'authentification lui accepte l'accès et renvoie un message « RADIUS Access-Accept", qui contient des instructions de politiques d'accès telles que (le VLAN ou l'ACL) pour indiquer au commutateur que le demandeur est autorisé à accéder au port.

Dans le cas où le demandeur soumet des informations d'identification non valides il n'a pas le droit d'accéder au réseau, le serveur d'authentification refuse l'accès en envoyant « RADIUS Access-Reject" au commutateur qui bloque le port.

4. Traçabilité (Accounting) :

La dernière étape est désignée par le terme "accounting", qui peut être traduit par traçabilité. Elle commence une fois que l'utilisateur final est authentifié ce qui implique qu'il a obtenu une autorisation d'accès au réseau. De ce fait on peut suivre ces événements, dans ce cas on dit que les actions de l'utilisateur sont loguées, un administrateur réseau pourra ainsi suivre ces actions. De même, il peut retrouver celui qui a effectué une telle ou telle action.

La traçabilité est très importante pour assurer une bonne sécurité et une intervention rapide en cas de problèmes. Car un utilisateur fera attention à ces actions en sachant qu'il est suivi, et si un problème survient on va facilement le localiser.

3.8. Active directory

Active Directory est un composant essentiel aujourd'hui à n'importe quel réseau d'entreprise. En effet, c'est un annuaire d'entreprise capable de recenser des utilisateurs et des informations des concernant. Cet annuaire est surtout compatible avec tous logiciels utilisant LDAP. Du coup Active Directory peut communiquer avec un certain nombre de services. Ce qu'il fait qu'aujourd'hui un bon Active Directory peut simplifier un réseau et surtout le rendre très efficace [14].

3.8.1. Les avantages d'Active Directory

L'active directory a plusieurs avantages [13] :

- Le regroupement et la gestion de tous les utilisateurs et ordinateurs d'un réseau ainsi qu'un contrôle total de l'administrateur sur leurs sessions.
- La possibilité de l'interconnecter à un autre Active Directory d'un site distant et de gérer celui-ci avec les droits suffisants.
- Gérer la redondance dans un même système avec 2 Active Directory ou plus

3.9. DNS (Domain Name Système)

Se souvenir de beaucoup d'adresse IP associées à la machine s'avère très difficile pour l'utilisateur de l'internet. C'est donc le travail du serveur DNS. En effet, il permet d'associer un nom à chaque machine et de créer un mécanisme qui permet de trouver l'adresse IP correspondante au nom d'hôte.

Le système de noms de domaine (DNS) est un système de nommage hiérarchique construit sur une base de données distribuée. Ce système transforme les noms de domaine en adresses IP et permet d'attribuer des noms de domaine à des groupes de ressources et d'utilisateurs Internet, indépendamment de l'emplacement physique des entités [23].

3.10. Serveur DHCP (Dynamic Host Configuration Protocol)

Le serveur DHCP est un serveur qui permet d'attribuer d'une manière dynamique des adresses IP aux machines lors de leurs connexions au réseau, grâce à une plage d'adresse [14]. Les avantages de DHCP sont [22] :

- Simplifier l'installation d'un grand nombre de machines.
- Grande souplesse pour les utilisateurs mobiles. Ils peuvent passer d'un réseau à un autre sans avoir à modifier leur paramètre réseau.

- Centralisation de la base effectuant la correspondance entre adresses IP et MAC.

3.10.1. Fonctionnement de DHCP

Lorsqu'un client DHCP démarre, il contacte un serveur DHCP et lui demande de louer une adresse IP, le serveur DHCP lui répond en sélectionnant une adresse IP disponible dans une étendue (plage d'adresses) dont IUL a la charge. Le serveur loue ensuite l'adresse sélectionnée au client pour une durée déterminée, lui donne le masque de sous-réseau associé à l'adresse et lui fournit en option un certain nombre d'informations (des adresses de serveur DNS et la passerelle par défaut). Lorsque le client a obtenu son bail [14].

Le client doit renouveler périodiquement sa demande pour ne pas perdre son adresse courante. Si le client s'arrête correctement, il annule son bail et dans ce cas le serveur DHCP peut offrir cette même adresse à un client différent, sauf si cette adresse a été réservée spécifiquement au client original [14].

Le fonctionnement du serveur DHCP (figure 3.8) se déroule en quatre phases [14] :

- **DHCP-DISCOVER** : Ce paquet est diffusé par le client dès que celui-ci démarre. Il contient l'adresse MAC ainsi que le nom de l'ordinateur client. Ce paquet est répété toutes les cinq minutes tant que le client n'a pas obtenu de réponse positive.
- **DHCP OFFER** : Ce paquet est diffusé par un serveur DHCP en réponse à un paquet DHCP-DISCOVER. Il contient l'adresse MAC du client DHCP qui a envoyé le Paquet DHCP-DISCOVER, l'adresse IP et le masque du sous réseau offerts au client, la durée du bail et l'adresse IP du serveur DHCP.
- **DHCP-REQUEST** : Ce paquet est diffusé par le client en réponse à la première offre de bail qu'il reçoit. Le paquet DHCP-REQUEST inclut l'adresse ip du serveur DHCP ayant proposé de bail et il signifie de la façon la plus simple « j'accepte le bail que vous me proposez ». Dans ce cas, le serveur DHCP va enregistrer cette dernière dans son cache tout en mentionnant que l'adresse est réservée.
- **DHCP-ACK** : c'est une requête envoyée par le serveur DHCP, une fois que l'adresse IP allouée est enregistrée dans le cache.

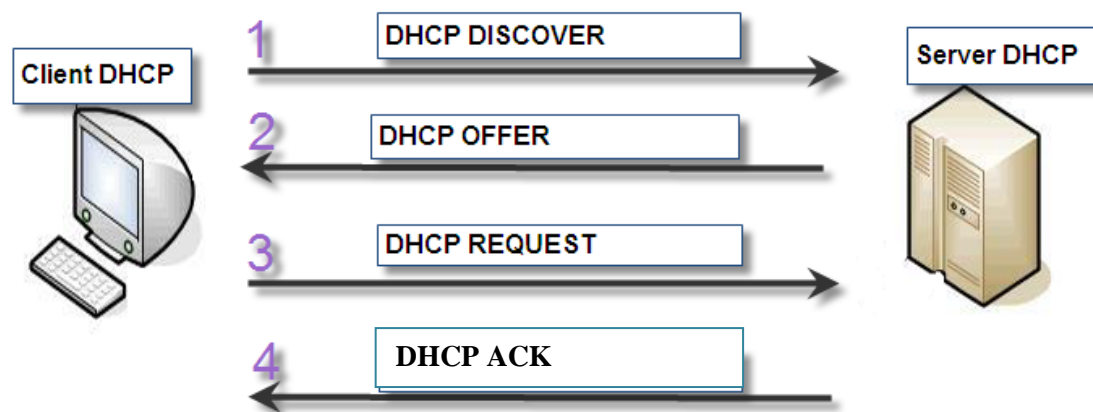


Figure 3.8 : Fonctionnement de DHCP.

3.11. Conclusion

Dans ce chapitre nous avons décrit les principaux concepts liés au fonctionnement du protocole d'authentification IEEE 802.1x. En effet, c'est un protocole robuste qui permet par l'intermédiaire des protocoles préexistants d'assurer l'authentification : EAP et Radius.

Ce Protocole permet également d'empêcher des trames de source inconnue de circuler sur le réseau grâce au contrôle de port qu'il adopte. S'il est employé avec des VLAN 802.1q, alors il permet d'obtenir un réseau local sécurisé à partir de la couche liaison de données.

L'implémentation de cette solution sera présentée dans le chapitre suivant, où toutes les étapes suivies sont explicitées.

Chapitre 4

Implémentation et test

4.1. Introduction :

Après avoir décrit le fonctionnement et les mécanismes de notre solution basée sur la norme 802.1X, dans le chapitre précédent, l'étape de l'implémentation et test sera décrite dans ce qui suit.

Ce chapitre sera consacré à la réalisation d'un mécanisme, permettant aux machines de s'authentifier avant tout accès au réseau. Les étapes d'installations et de configurations seront également décrites.

4.2. Outils utilisés

La phase de réalisation et de mise en œuvre a nécessité l'installation de plusieurs outils :

1. **GNS3 (Graphical Network Simulator)** : C'est un logiciel libre, disponible pour Windows, Linux et MacOS X, il permet de simuler une architecture physique ou logique grâce aux [31] :
 - Dynamips qui est un émulateur IOS Cisco.
 - Dynagen qui est une interface en mode texte pour Dynamips.
2. **VMware Workstation 2012** : La machine virtuelle est utilisée pour importer tous nos logiciels utilisés dans notre environnement
3. **Windows server 2012** : C'est un système d'exploitation serveur complet, polyvalent et puissant qui se base sur les améliorations que Microsoft a apporté à Windows serveur 2008 R2. Au niveau de ce dernier, nous avons installé les différents rôles (DHCP, AD, NPS) permettant de réaliser notre travail.
4. **Windows server 2007** : Le client se connectant au réseau d'entreprise reçoit une adresse IP correspondant au VLAN sur lequel il est placé. La connexion du client au switch est contrôlée par le système d'authentification 802.1X.

1. **Wireshark** : C'est un analyseur de paquets réseau, Qui capture les paquets réseau et affiche ces données de paquets aussi détaillées que possible.
2. **Putty** : C'est une implémentation gratuite de SSH et Telnet pour Windows et Unix.

4.3. Simulation du réseau local de SONATRACH

Afin de configurer le nouveau réseau local de SONATRACH, nous l'avons reproduit sous l'émulateur GNS 3.

La figure (4.1) montre la topologie reproduite. Et vu que le fonctionnement de la totalité de la topologie nécessite beaucoup de ressource (RAM, processeur), nous ne sommes contentées de la partie encadrée pour effectuer nos différents tests.

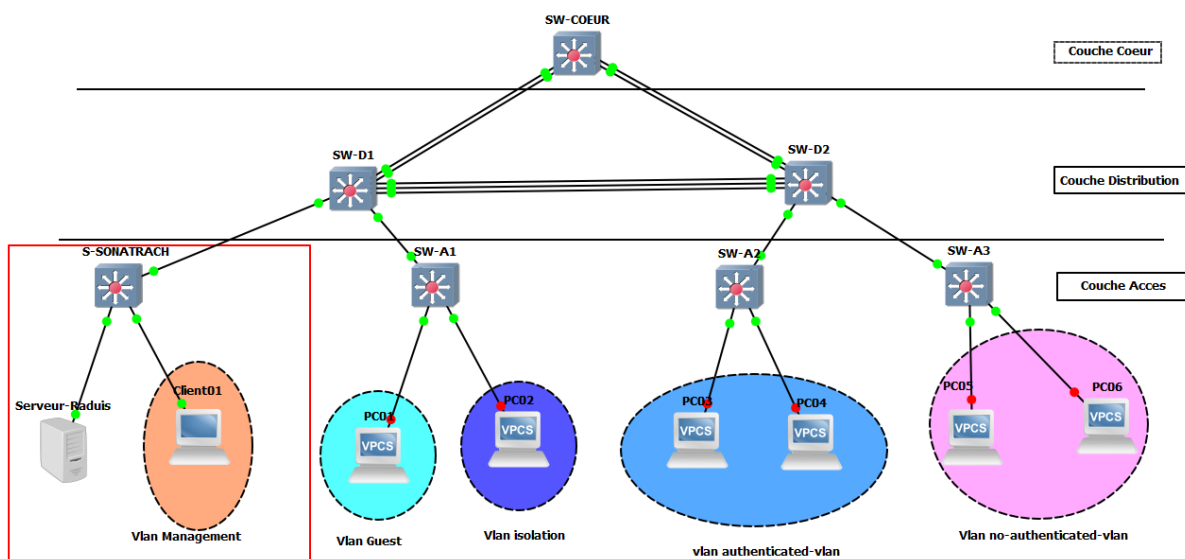


Figure 4.1 : Topologie reproduite de l'entreprise RTC.

Comme nous pouvons le voir sur la figure (4.1), nous avons reproduit cette topologie suivant un modèle hiérarchique.

4.3.1. Le modèle hiérarchique

Le modèle hiérarchique est composé de trois couches présentées dans la figure (4.1) :

- **La couche cœur** : Elle est considérée comme le backbone du réseau, parce que toutes les autres couches sont reliées à elle. Son objectif est de réduire le temps de latence des paquets.
- **La couche distribution** : Située entre la couche cœur et la couche accès. Elle assure les fonctions du routage, ainsi que les politiques d'accès au réseau.
- **La couche d'accès** : C'est la dernière couche du modèle, elle sert à connecter les périphériques au réseau. Elle communique avec la couche distribution en vue d'exécuter les fonctions de base du réseau à savoir la qualité de service et la sécurité.

4.3.2. Configuration du switch

Pour la configuration du switch, nous avons énumérés les commandes importantes et expliquer leurs utilités dans le contexte de notre travail. Les commandes secondaires sont vues en détail dans l'annexe B.

1. Création des VLANs

Les VLANs doivent être créés avant que le switch n'affecte aucun de ces ports à un vlan spécifique. La figure (4.2) illustre les commandes de base pour la création de ces derniers dans le switch.

Comme on peut le voir sur la figure (4.2), nous avons créés 5 VLANs.

```
SWD-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWD-01(config)#vlan 99
SWD-01(config-vlan)#name management
SWD-01(config-vlan)#vlan 10
SWD-01(config-vlan)#name isolation
SWD-01(config-vlan)#vlan 20
SWD-01(config-vlan)#name no-authenticated-vlan
Warning: Vlan 20 name length exceeded the recommended length of 20 characters.
SWD-01(config-vlan)#name no-authenticated-vln
SWD-01(config-vlan)#vlan 30
SWD-01(config-vlan)#name authenticated-vlan
SWD-01(config-vlan)#vlan 40
SWD-01(config-vlan)#name guest
```

Figure 4.2 : Création des VLANs.

2. Assigner une adresse IP à l'interface d'un vlan et configuration de l'agent relais :

On affecte une adresse IP à l'interface d'un vlan, dans le but de l'utiliser comme une passerelle par défaut.

Une adresse IP-helper est utilisée afin de se connecter au serveur DHCP, dans le cas où un client sollicite une adresse IP (Relier le DHCP Discover vers le serveur).

Dans la figure (4.3), nous avons pris l'exemple du vlan 99 et du vlan 30.

```
S-SONATRACH(config)#interface vlan 99
S-SONATRACH(config-if)#ip address 10.10.99.1 255.255.255.0
S-SONATRACH(config-if)#ip helper-address 10.10.99.99
S-SONATRACH(config-if)#no shutdown
S-SONATRACH(config-if)#interface vlan 30
S-SONATRACH(config-if)#ip helper-address 10.10.99.99
*Mar 1 00:25:08.031: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
S-SONATRACH(config-if)#ip address 10.10.30.1 255.255.255.0
S-SONATRACH(config-if)#ip helper-address 10.10.99.99
S-SONATRACH(config-if)#no shutdown
```

Figure 4.3 : Assigner une adresse IP à l'interface d'un vlan.

3. Configuration de l'interface du trunk

- La première commande dans la figure (4.4) permet de spécifier l'interface à configurer.
- La seconde permet d'indiquer une méthode d'encapsulation.
- Tandis que la troisième permet d'activer le mode trunk.

```
SW-COEUR(config)#interface ethernet 0/0
SW-COEUR(config-if)#switchport trunk encapsulation dot1q
SW-COEUR(config-if)#switchport mode trunk
```

Figure 4.4 : Configuration de l'interface du trunk.

4. Activation du AAA sur le switch

On configure le nouveau modèle AAA, en indiquant que l'authentification se fera en 802.1x grâce au serveur RADIUS.

- La première commande dans la figure (4.5) sert à activer les services Authentification, Autorisation et Accounting (Traçabilité) AAA.
- Tandis que la seconde permet de spécifier le groupe à utiliser pour authentifier les utilisateurs.

```
S-SONATRACH(config)#aaa new-model
S-SONATRACH(config)#aaa authentication dot1x default group radius
```

Figure 4.5: Activation du service AAA et spécification du groupe d'authentification.

On indique ensuite l'adresse IP de notre serveur RADIUS, les ports qu'il utilise pour communiquer ainsi que le mot de passe (figure 4.6)

```
S-SONATRACH(config)#dot1x system-auth-control
S-SONATRACH(config)#radius-server host 10.10.99.99 auth-port 1812 acct-port 1813 key sonatrach.lan
```

Figure 4.6 : Attribution d'une adresse et d'un mot de passe au serveur radius.

5. Configurer l'authentification basée sur le port

- La première commande (figure 4.7) permet de spécifier l'interface.
- La seconde permet de configurer le port en mode Access.
- Tandis que la dernière, sert à activer l'authentification 802.1x sur le port spécifié.

```
S-SONATRACH(config)#interface fastEthernet 1/1
S-SONATRACH(config-if)#switchport mode access
S-SONATRACH(config-if)#dot1x port-control auto
```

Figure 4.7: Configuration de l'authentification basée sur le port.

La commande dans la figure (4.8) permet d'affecter les VLANs d'une façon dynamique aux utilisateurs.

```
S-SONATRACH(config)# aaa authorization network default group radius if-authenticated
```

Figure 4.8: Configuration de l'affectation dynamique des VLANs.

Les utilisateurs authentifiés dans Active Directory recevront le VLAN conformément à la politique que nous avons configuré sur le serveur NPS (voir la figure 4.9).

```
S-SONATRACH(config)#aaa authorization network default group radius
```

Figure 4.9: Réception du vlan adéquat.

f. Configuration des utilisateurs non 802.1X

Si l'authentification ne fonctionne pas, l'utilisateur sera positionné dans le VLAN 10 (isolation). La commande sur la figure (4.10) illustre la commande à utiliser.

```
S-SONATRACH(CONFIG-IF) # dot1x Guest-vlan 10
```

Figure 4.10: Affectation du vlan isolation aux utilisateurs non 802.1

6) Affichage des messages d'authentification RADIUS

- La première commande dans la figure (4.11) permet d'afficher les différents messages 802.1X.
- La seconde permet d'afficher Les messages d'authentification.
- Tandis que la troisième permet d'afficher des informations sur l'autorisation.

```
S-SONATRACH#debug dot1x all (1)
S-SONATRACH#debug aaa authentication (2)
AAA Authentication debugging is on
S-SONATRACH#debug aaa authorization (3)
AAA Authorization debugging is on
```

Figure 4.11 : Affichage des message dot1x

7) Permutation des VLANs

La commande dans l figure (4.12) nous permet de renforcer la sécurité des VLANs et d'autoriser l'accès seulement au vlan désigné, elle permet également de bloquer la vlan natif (vlan 1) par défaut.

```
S-SONATRACH(config-if)#switchport trunk allowed vlan 10,20,30,40,99
```

Figure 4.12 : Permutation des VLANs.

8)Activation du 802.1x

La commande illustrée dans la figure (4.13) permet d'activer le 802.1x sur le port du switch.

```
S-SONATRACH(config-if)#dot1x port-control auto
S-SONATRACH(config-if)#
```

Figure 4.13 : Activation du 802.1x.

4.4. Configuration du Windows serveur 2012 R2

1. Configuration tcp/ip du serveur

La configuration de TCP/IP est faite statiquement afin d'éviter la relation entre le DHCP et le serveur RADIUS. La figure (4.14) présente la configuration TCP/IP du serveur RADIUS.

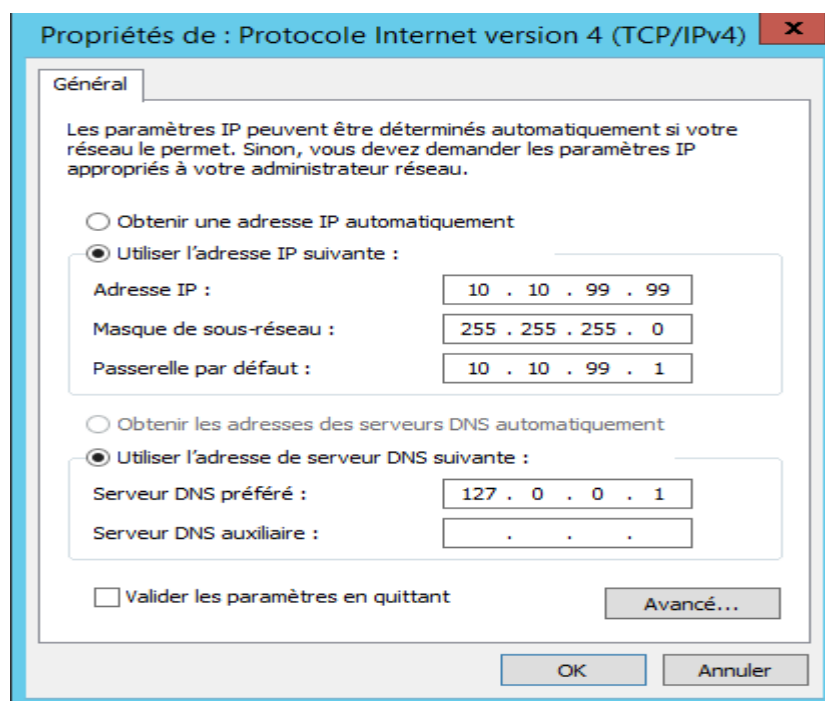


Figure 4.14 : Configuration TCP/IP du Serveur

2. Configuration d'active directory et DNS

Avant toute configuration, au préalable le rôle Active Directory devra être ajouté. En effet il n'y a pas une configuration du DHCP, ou une installation d'une autorité de certification sans Active Directory. Nous ferons mention de la procédure d'ajout du rôle Active Directory dans l'annexe A.

Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en couchant sur Ajouter une nouvelle forêt et en spécifiant le nom de notre domaine « sonatrach.lan » (figure 4.15).

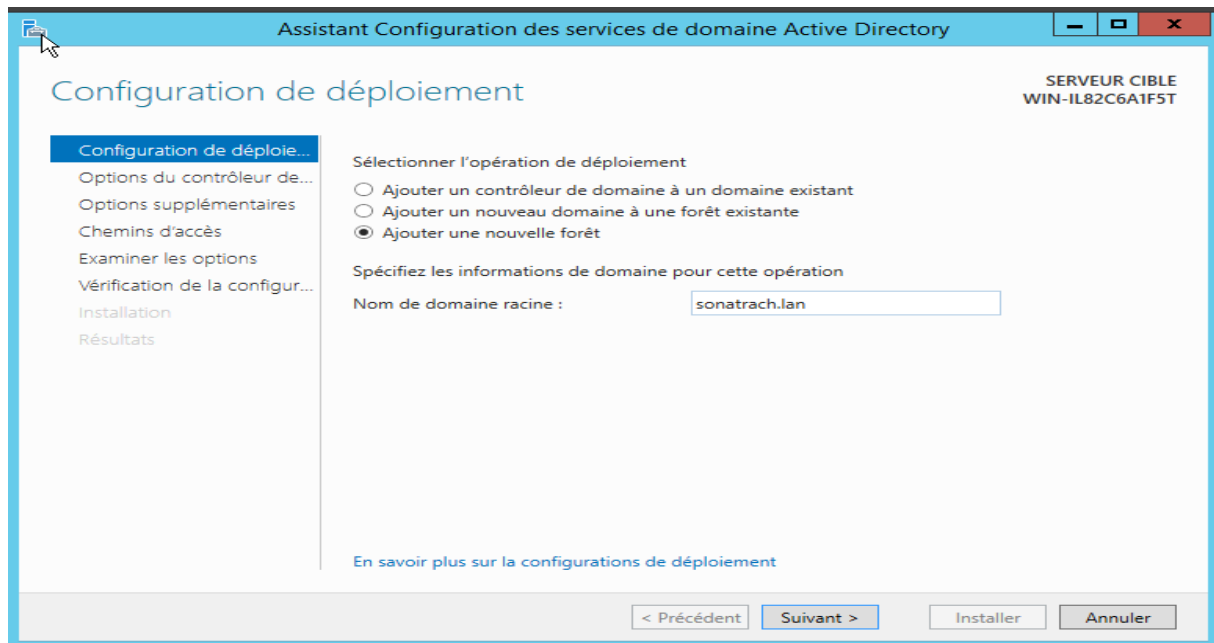


Figure 4.15 : Création du domaine Sonatrach.

L'étape suivante consiste à choisir le niveau fonctionnel de la forêt ou du domaine.

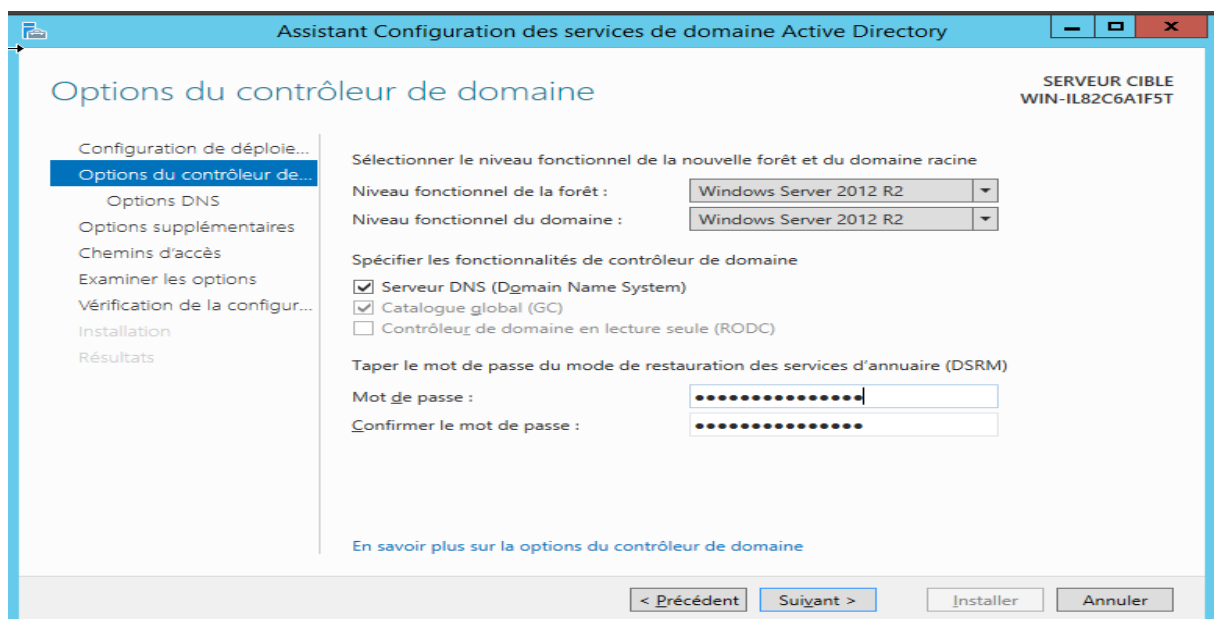


Figure 4.16 : Sélection du niveau fonctionnel de la forêt et du domaine.

Une fois les services du domaine Active Directory installés (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS. La zone DNS résultante est intégrée à AD DS. Après configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu outil, notre domaine est créé, et l'ouverture d'une session 'exécute avec le compte d'administrateur du domaine SONATRACH\Administrateur, voir la figure (4.17).

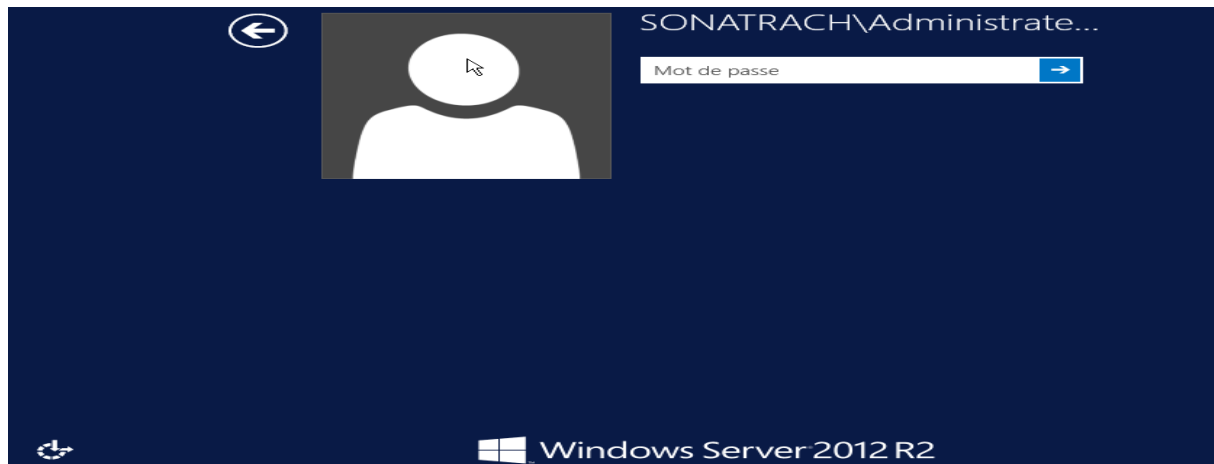


Figure 4.17 : Ouverture de la session Administrateur.

3. Configuration du serveur DHCP

Pour que les PC et les serveurs communiquent, nous devons leur donner une adresse IP, un masque de sous réseau, une passerelle et un serveur DNS qui est obligatoirement un DNS d'Active Directory. Nous ferons mention de la procédure d'installation du rôle DHCP dans l'annexe A.

La création de nos étendues DHCP (figure 4.18) se fait à l'aide de la console d'administration DHCP qui a été lancée depuis le menu Outils du gestionnaire de serveur.

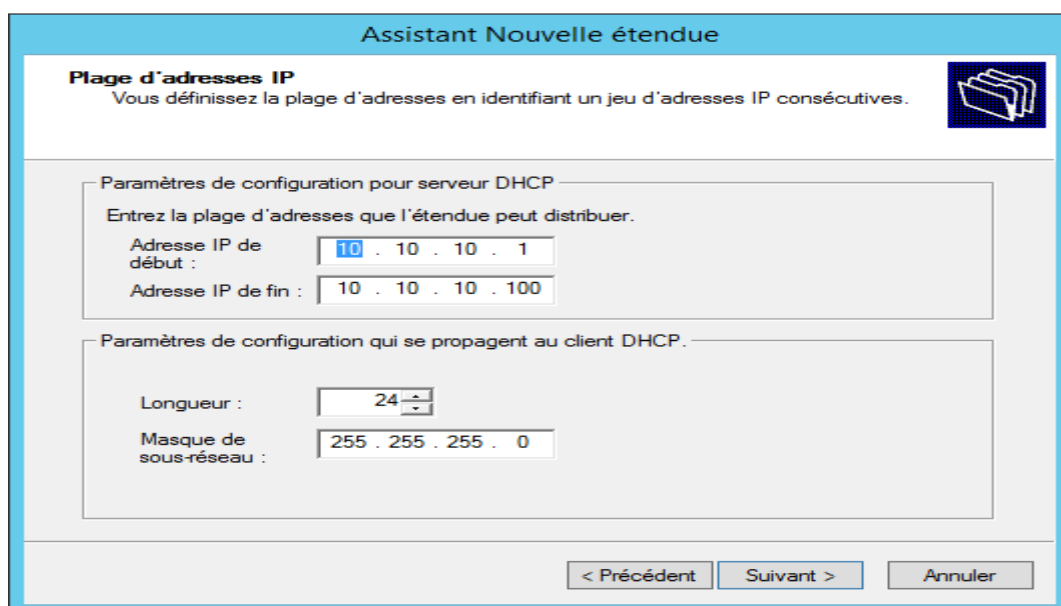


Figure 4.18 : Exemple de création d'un étendue DHCP.

Ajouter d'éventuelles exclusion (figure 4.19) afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP, PC en adresse fixe, serveur. . .).

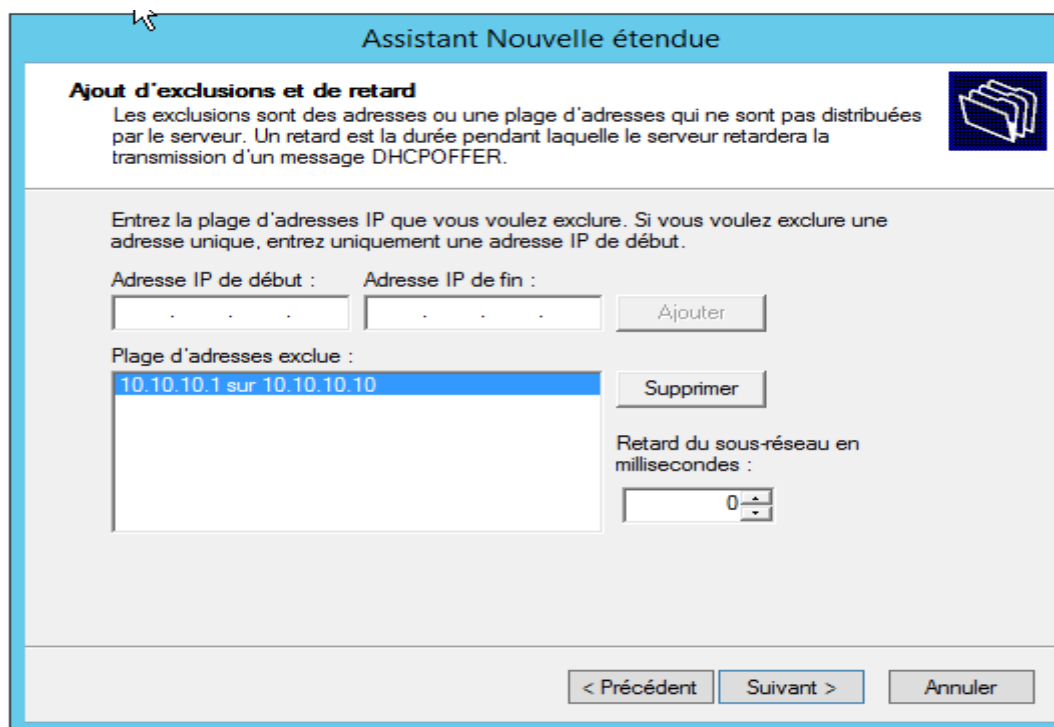


Figure 4.19: Ajout d'exclusion DHCP.

La figure (4.20) illustre l'ensemble des ententes que nous avons créés.

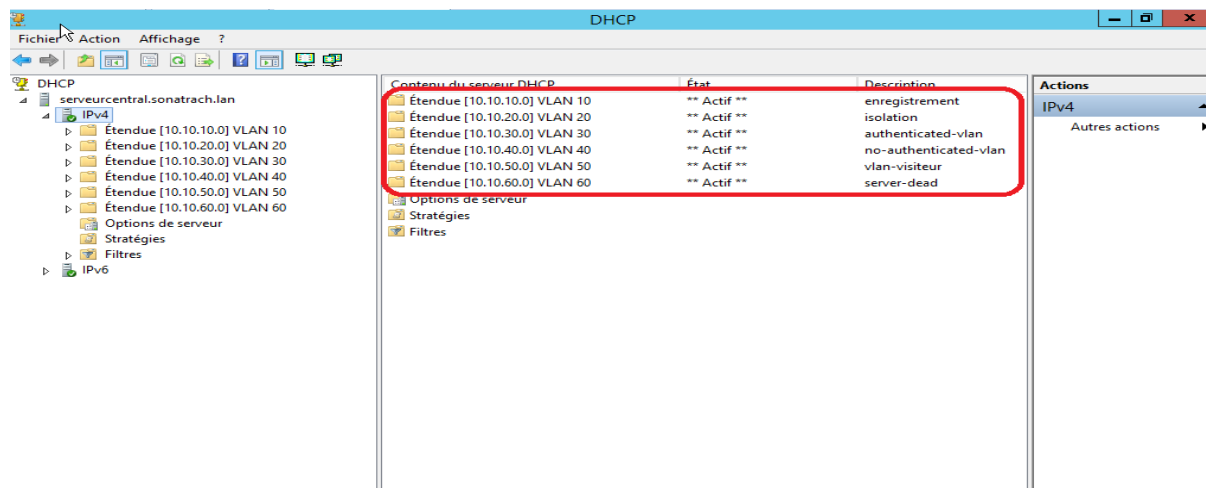


Figure 4.20 : L'ensemble des plages d'adresses utilisées.

4. Organisation des clients AD en unités organisationnelles

Nous allons commencer de peupler notre Active Directory (figure 4.21). Pour ce faire, nous devons lancer la console Utilisateur et ordinateur Active Directory. On peut la lancer depuis le Gestionnaire de serveur puis sous la rubrique AD DS.

Nous allons créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes, pour cela on se place dans l'arbre à la hauteur de notre domaine sonatrach.lan et sur le menu, nous choisissons l'option Unité d'organisation.

Cette procédure nous a permis de regrouper des ordinateurs ou des utilisateurs dans une seule unité afin qu'on puisse leurs appliquer des procédures et des stratégies de groupe.

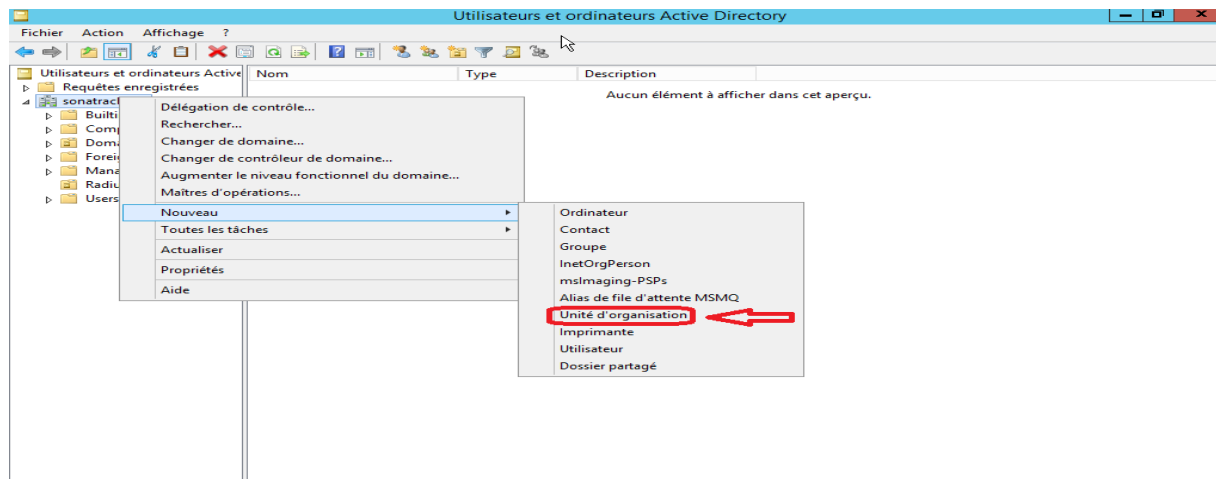


Figure 4.21 : Création d'une unité d'organisation.

Après avoir créé les unités organisationnelles relatives à notre entreprise, nous pouvons maintenant créer les premiers utilisateurs qui seront inclus dans les groupes et commencer à peupler nos unités. Nous avons répété la même procédure pour tous les nouveaux utilisateurs, comme illustré dans la figure (4.22) :

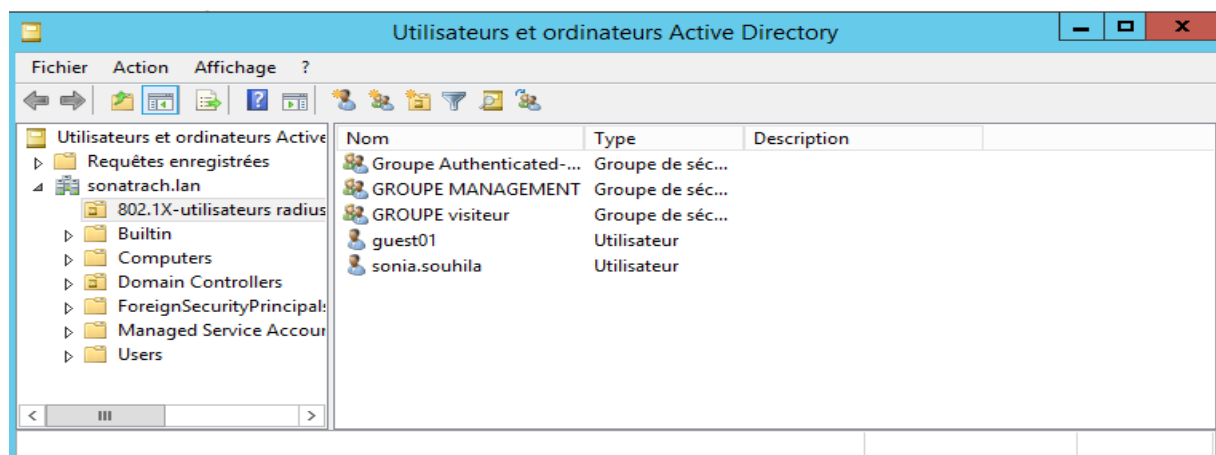


Figure 4.22: Ajout d'utilisateur.

Pour chaque UO (Unité Organisationnelle), nous avons créé des comptes utilisateurs avec un identifiant unique de la forme sonia.souhila@sonatrach.lan (Figure 4.23).

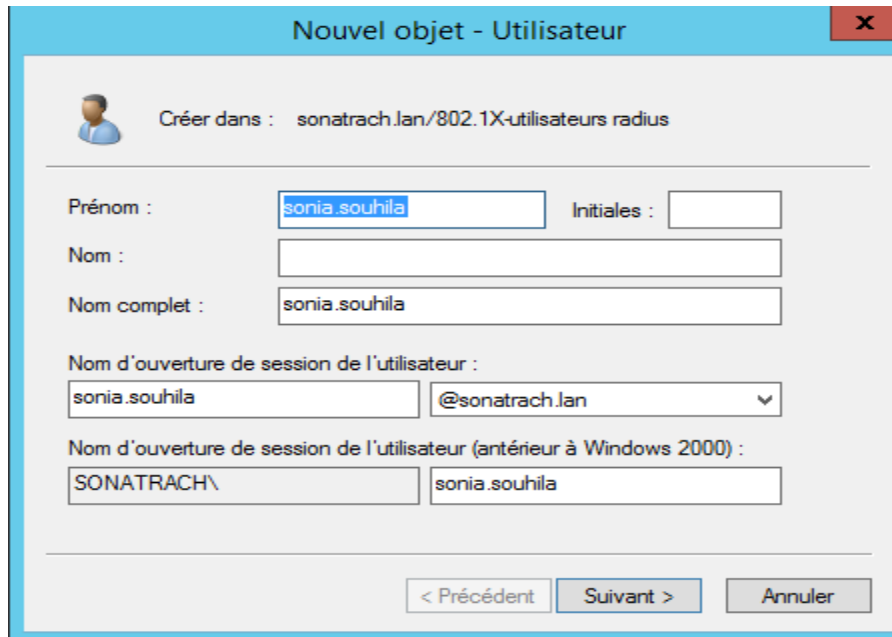


Figure 4.23 : Création des sessions utilisateurs.

5. JOINDRE UN PC AU DOMAINE

Dans cette partie, nous avons intégré un ordinateur dans un domaine Active Directory sur l'ordinateur Windows 7, Afin d'accéder aux différents paramètres de la carte réseau, pour cela on clique sur « modifier les paramètres réseaux de ma carte » Comme illustrée dans la figure (4.24). La suite de la procédure sera détaillée dans l'annexe A.

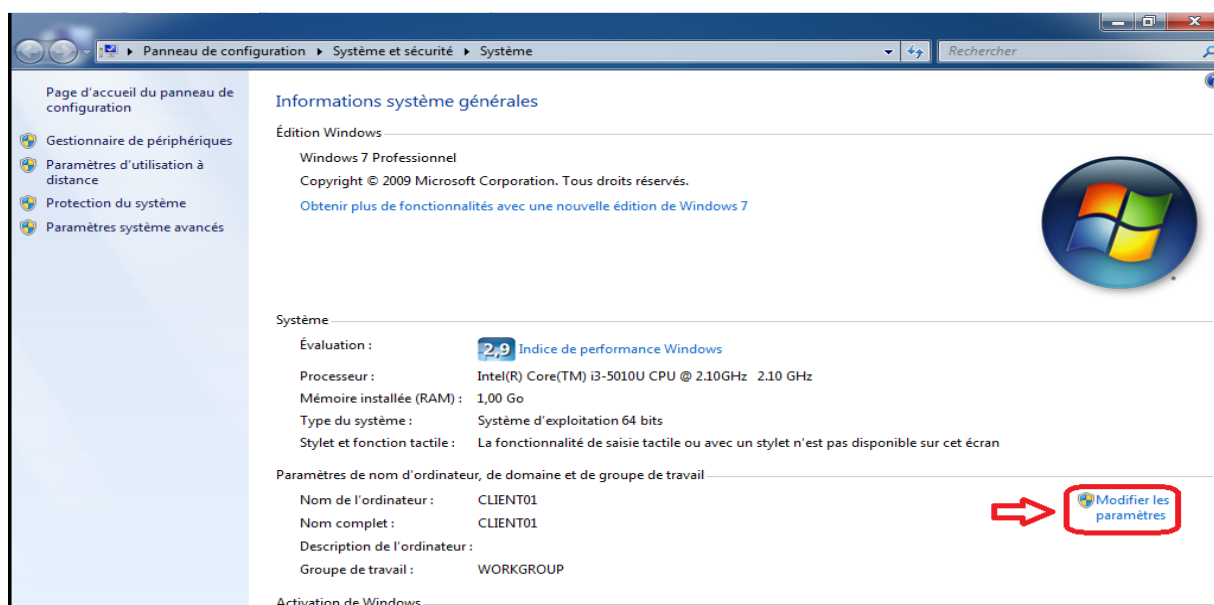


Figure 4.24 : Modifier les paramètres du PC.

6. Configuration du serveur RADIUS

Le serveur RADIUS est dans notre cas Network Policy Server (NPS). Il permet de créer et de mettre en œuvre 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 connexions.

- **La configuration initiale du serveur NPS**

Le serveur NPS nous permet de créer et de mettre en application sur l'ensemble du réseau de notre organisation des stratégies d'accès réseau portant sur l'intégrité des clients, ainsi que sur l'authentification et l'autorisation des demandes de connexions.

Dans la figure (4.25) nous avons inscrit le serveur NPS dans l'active directory.

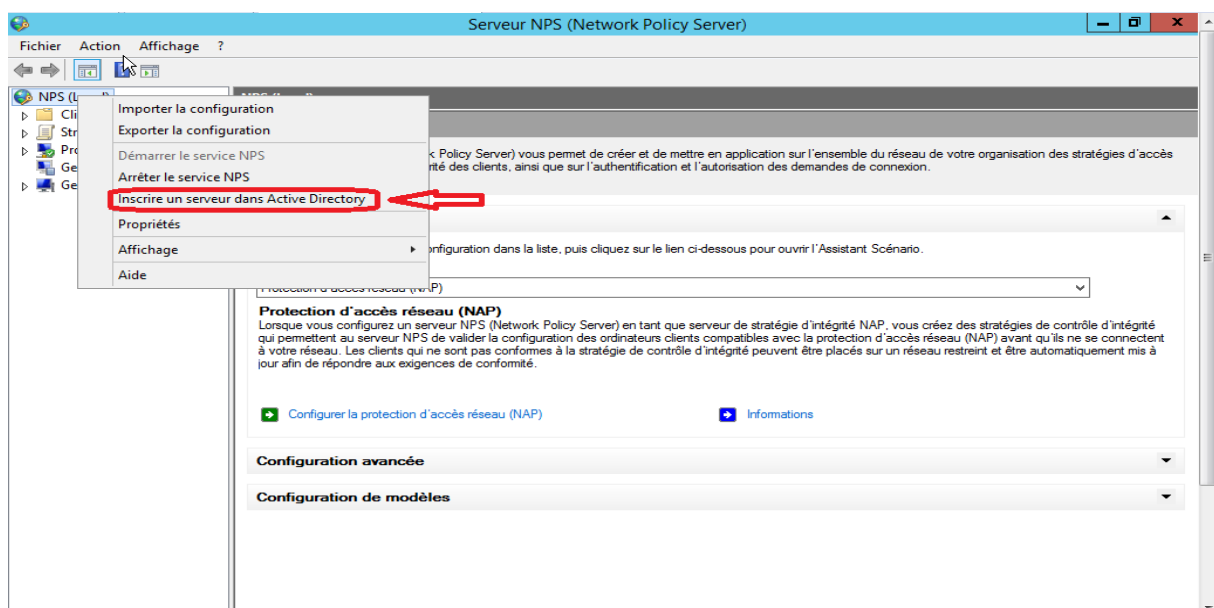


Figure 4.25 : Inscrire le serveur NPS dans Active Directory.

- **Configuration d'un client RADIUS**

Le client RADIUS garantit la communication entre le serveur d'authentification et l'utilisateur final. La configuration du client RADIUS est illustrée dans la figure (4.26).

En premier lieu, nous cochons la case qui nous permet d'activer le client RADIUS. Puis, on fait entrer le nom du commutateur et l'adresse IP. Le mot de passe doit être saisi dans la case « Secret partagé », ensuite confirmé (le secret partagé c'est une clé de cryptage entre le client et le serveur Radius).

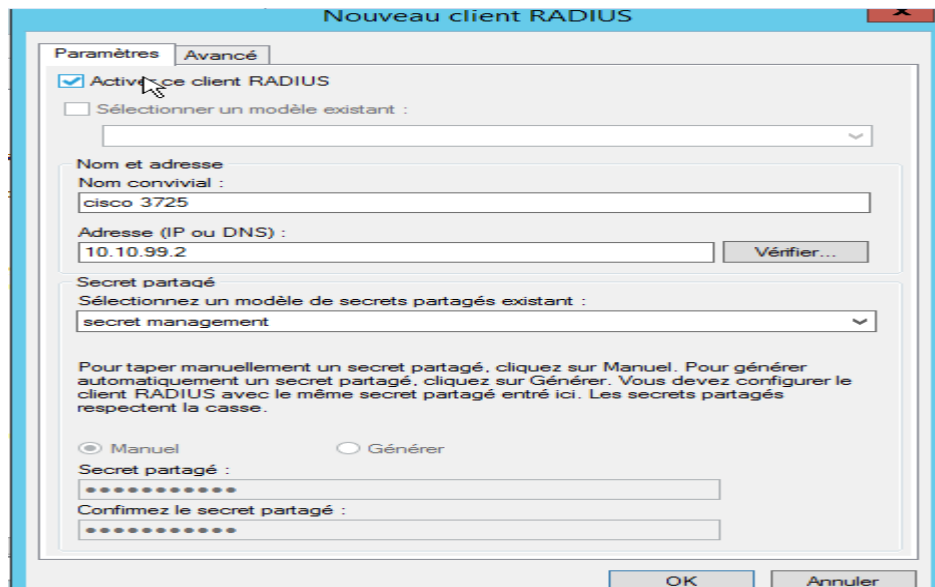


Figure 4.26 : Configuration d'un client radius.

Afin de rendre le client RADIUS compatible avec le NAP (Network Access Point), Dans l'onglet Avancé, nous allons cocher « le client RADIUS est compatible avec la protection d'accès réseau (NAP) » (voir la figure 4.27).

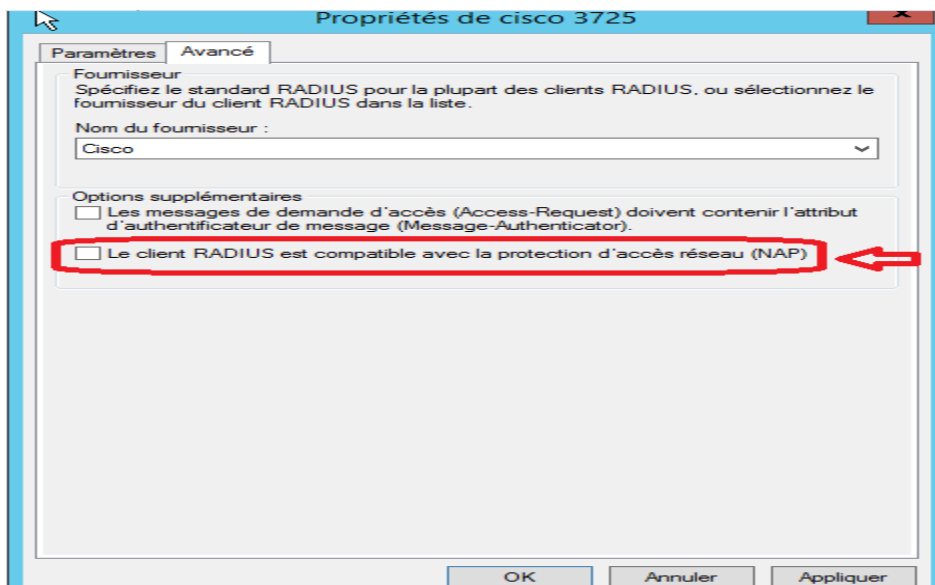


Figure 4.27 : Spécification du standard RADIUS.

Dans la figure (4.28), nous choisissons « serveur Radius pour la connexion câblées ou sans fil 802.1x » afin de configurer le protocole 802.1X.

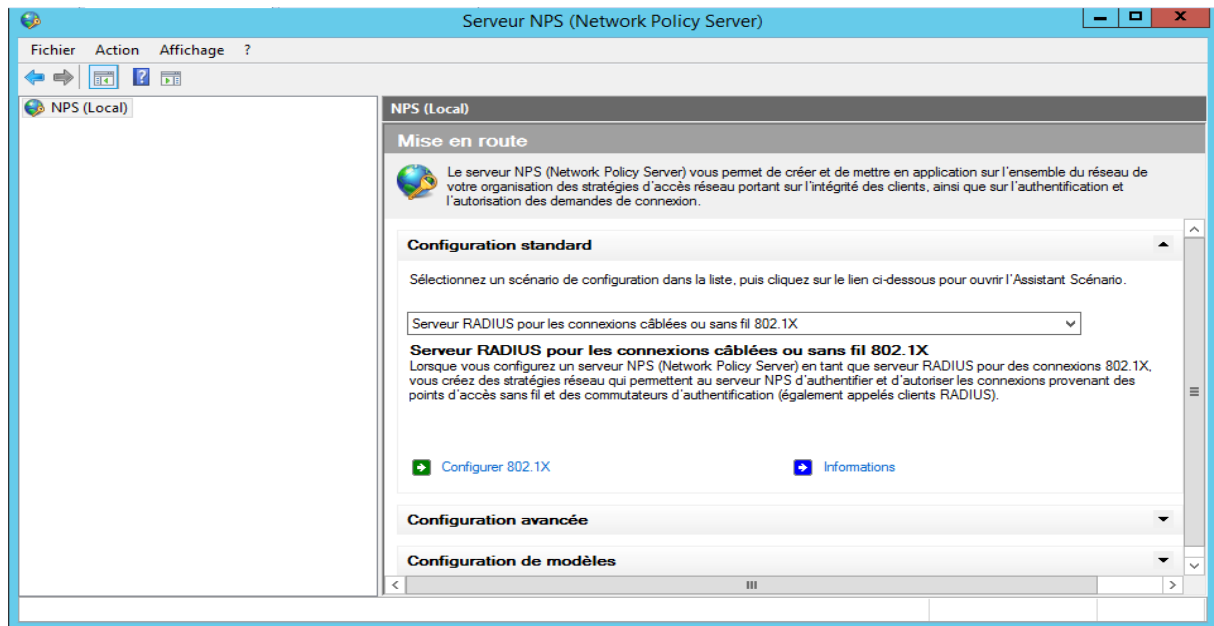


Figure 4.28 : Configuration du 802.1x.

Nous cliquons ensuite sur « configurer 802.1X », ça nous permet d'authentifier et d'autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.

Par la suite, il faut choisir le type de connexion, dans notre cas nous choisissons la connexion câblée (figure 4.29).

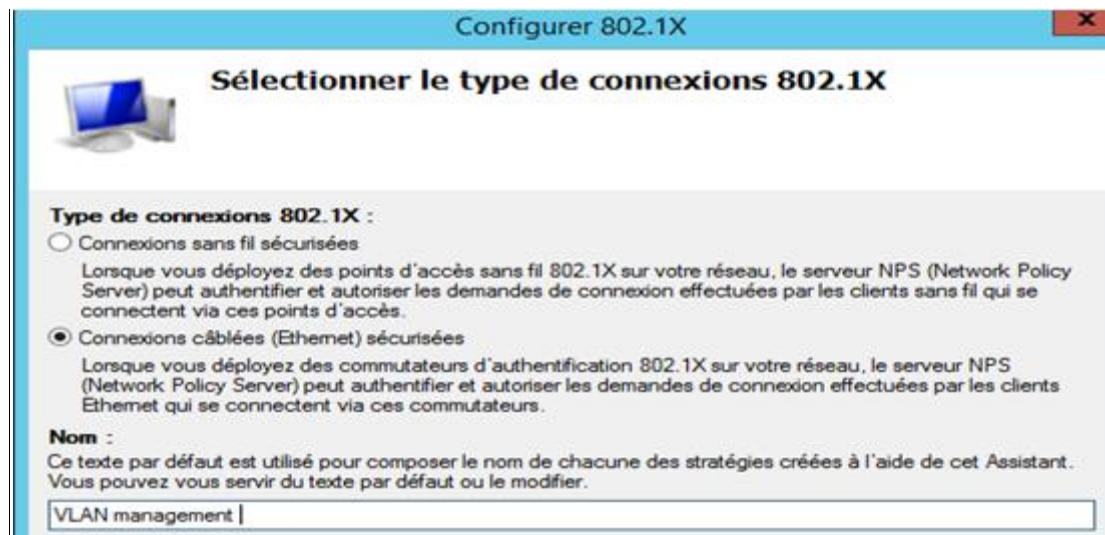


Figure 4.29: Connexion câblée sécurisé

Ensuite nous devons spécifier un client RADIUS (figure 4.30).



Figure VI.30 : Spécification des commutateur 802.1X.

Dans cette partie, on aura besoin d'un mécanisme d'authentification de l'utilisateur qui souhaite se connecter au réseau. EAP (ou plus précisément Protected EAP) est le protocole idéal dans notre cas : il permet au point d'accès d'interroger un serveur d'identification (Radius) avant d'autoriser l'utilisateur à accéder aux ressources réseau de l'entreprise. Le serveur Radius, lui se chargera d'interroger l'Active Directory pour savoir si les informations d'authentification (login + password) sont valides ou pas, La version de PEAP utilisée fait appel à un mécanisme d'authentification MSCHAPv2 : le nom réel de la solution sera donc PEAP-EAP-MSCHAPv2 où l'authentification est faite par le couple login/password.

Afin que nous puissions activer le protocole PEAP, le service de certificat active directory doit être installée. Une fois ce rôle est activé, le PEAP sera activé comme illustrée dans la figure (VI.31).

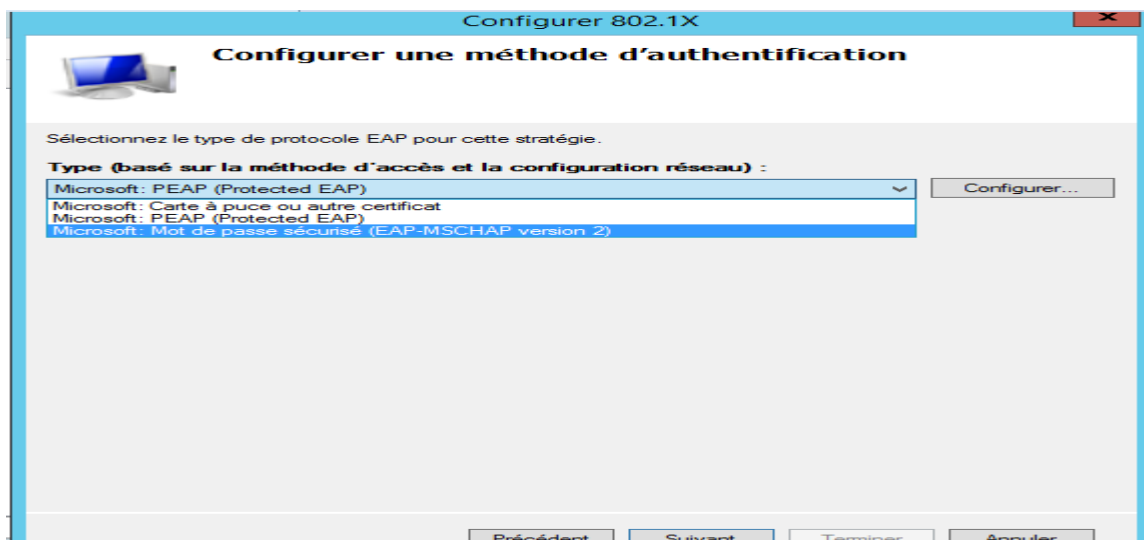


Figure 4.31 : Configuration du type de protocole EAP pour la stratégie.

La figure (4.32) montre la sélection du type de protocole EAP pour cette stratégie et ainsi le nombre de nouvelles tentatives d'authentification :

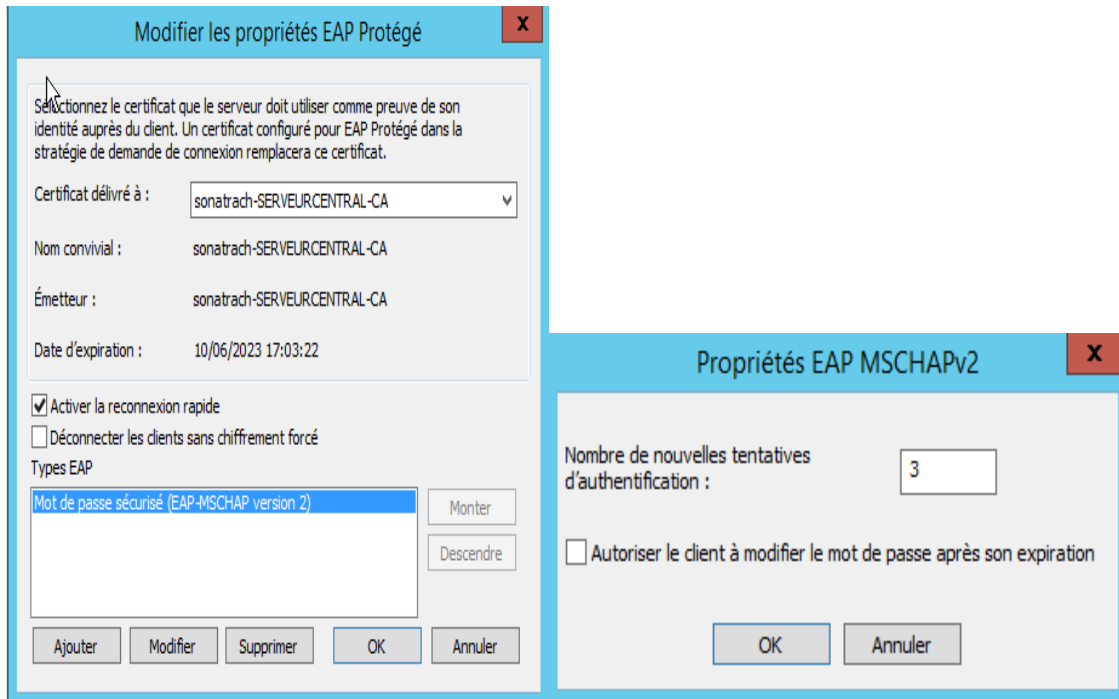


Figure 4.32 : Fixation de nombre de tentative d'authentification.

Dans ce cas, L'accès des utilisateurs membre du groupe sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau. Dans dans la Figure (4.33) nous avons sélectionné le groupe authenticated-vlan.

Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.



Figure 4.33: Spécification des groupes d'utilisateurs.

Les ports du VLAN doivent correspondre dynamiquement au domaine utilisateur. Nous devons définir les attributs suivants (figure 4.34) :

- Tunnel-Pvt-Group-ID : 30. Ceci est le VLAN qui sera accordé au groupe de domaine "Authenticated-vlan".
- Tunnel-Type : réseaux locaux virtuels (VLAN).
- Tunnel-Medium-Type : 802 (inclut tous les supports 802 plus le format canonique Ethernet).

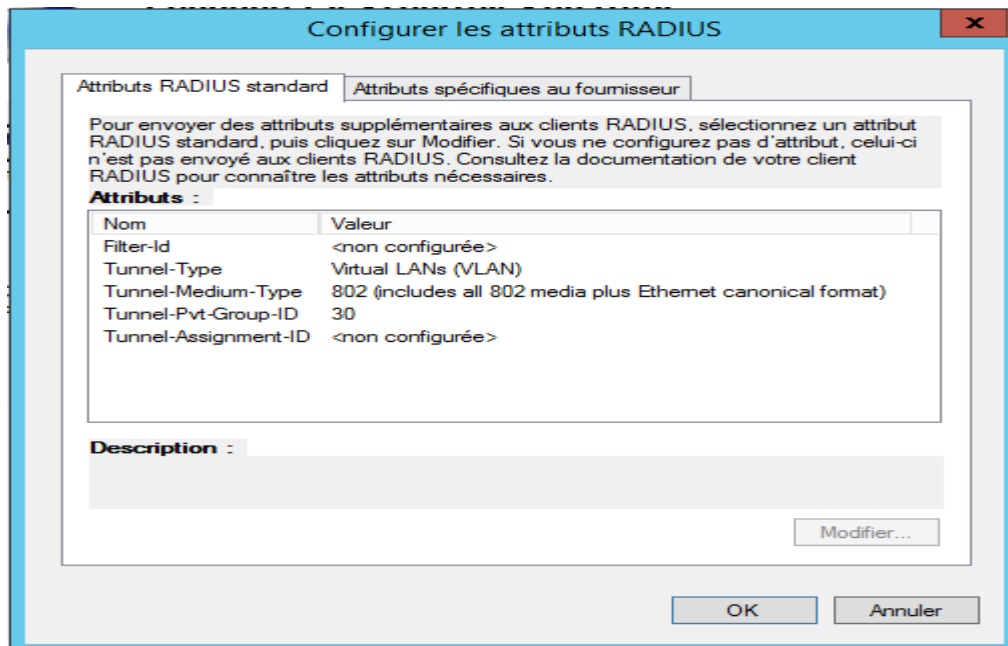


Figure 4.34 : Configuration des attributs RADIUS

La figure (4.35) définit les différentes stratégies créées.

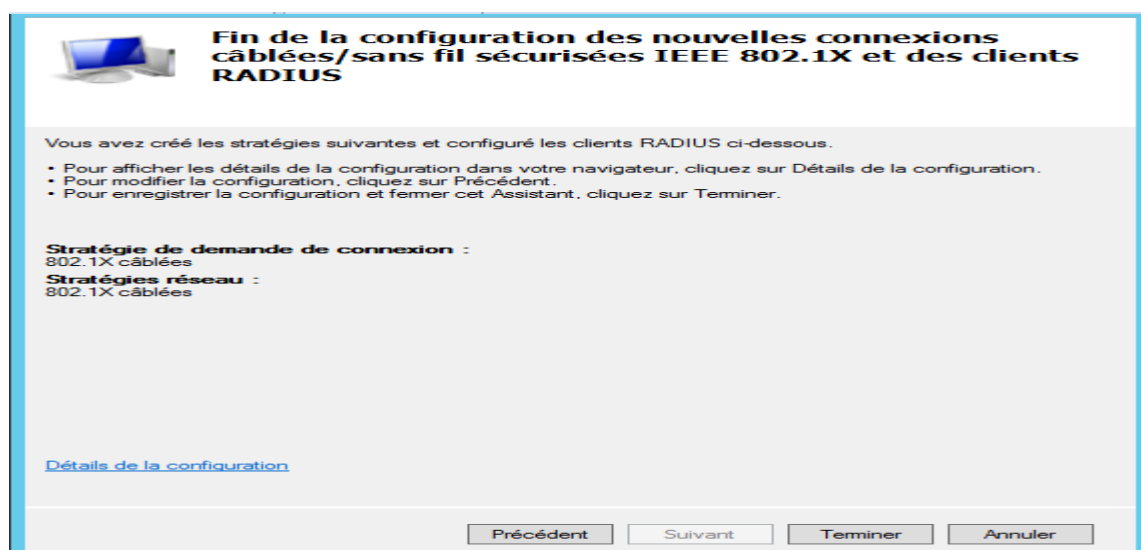


Figure 4.35 : L'affichage des différents stratégie créées

7. Création d'une stratégie

Nous sommes censés de désactiver en premier lieu les deux stratégies par défaut dans la console Serveur NPS dans « Développant stratégies », puis en sélectionnant stratégie Réseau comme illustrée dans la figure (4.36).

Etant donné que nous avons besoin d'appliquer d'autres stratégies pour notre solution. Nous avons créé deux autres qu'on peut voir sur la figure (4.36), Les stratégies s'appliqueront selon l'ordre de leurs apparitions et selon l'état de la machine.

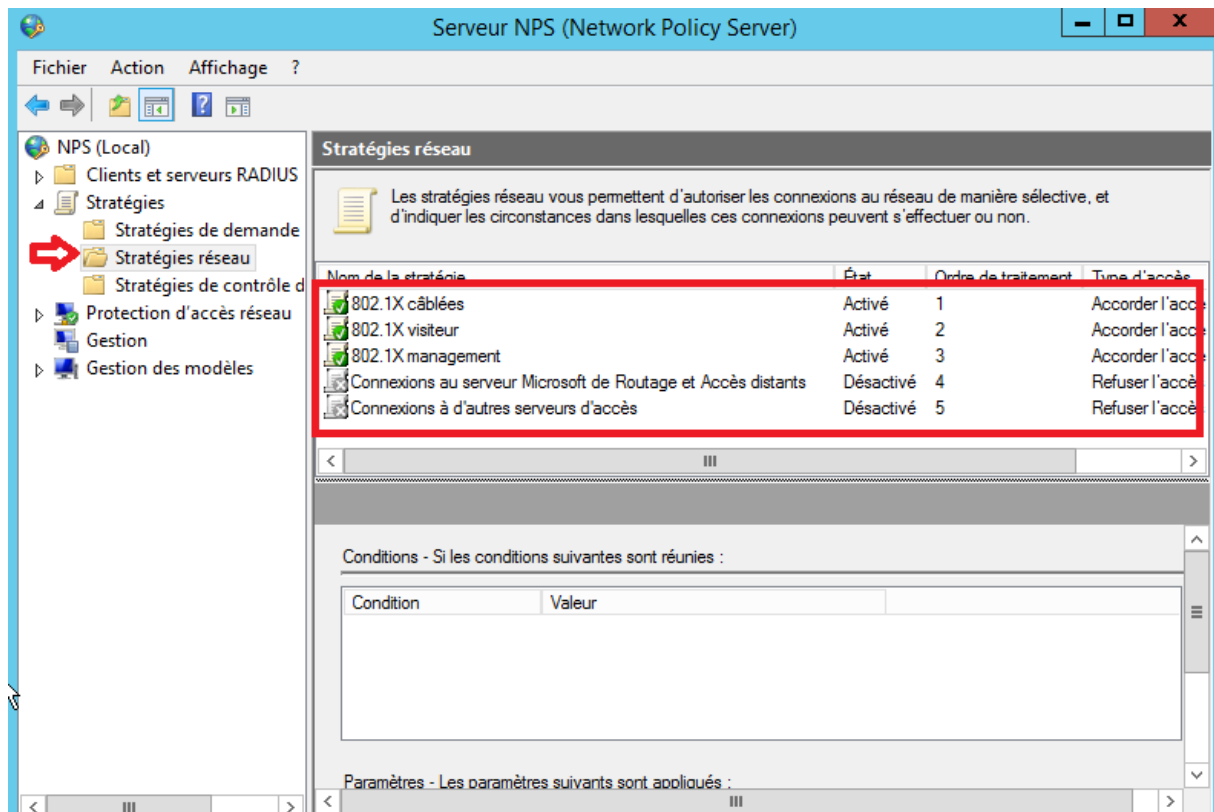


Figure 4.36 : Désactivation et création de stratégies.

Une fois la stratégie créée, nous devons vérifier le contenu d'une stratégie (figure 4.37) :

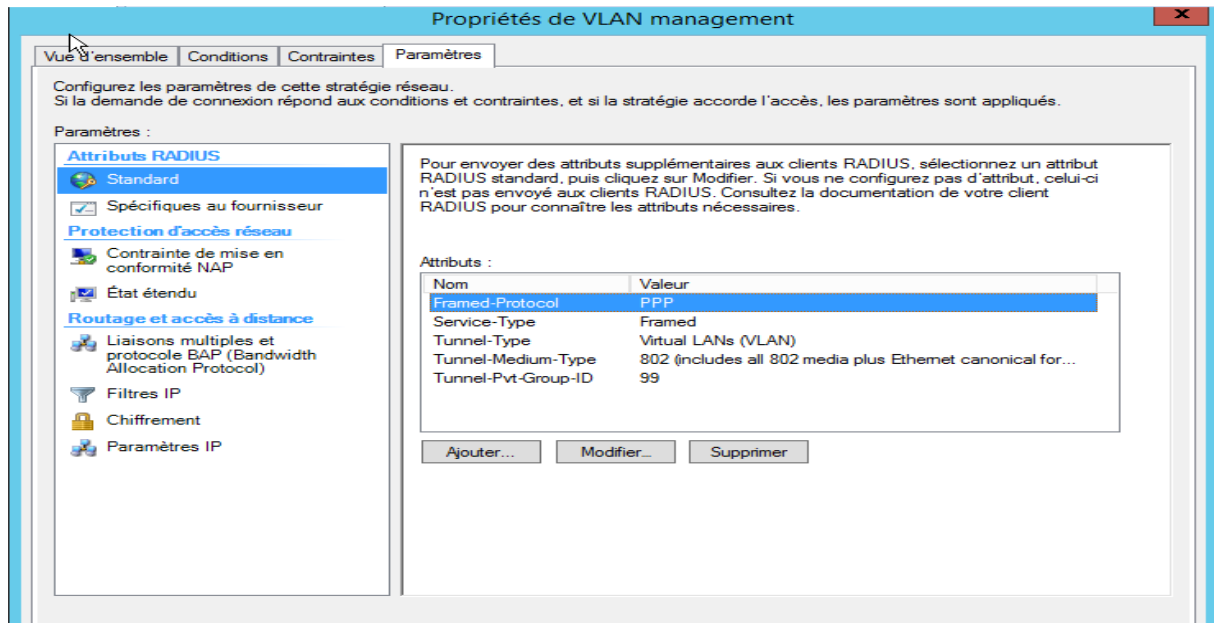


Figure 4.37: Le contenu d'une stratégie.

4.5. Tests de fonctionnement de notre solution

4.5.1. Tests d'attribution des VLANs selon l'état du PC

Vlan 30 : Un Pc conforme et qui appartient au domaine, Une fois l'authentification est bien réussie en remarque que le serveur DHCP lui affecte l'adresse du vlan 30 (figure 4.38).

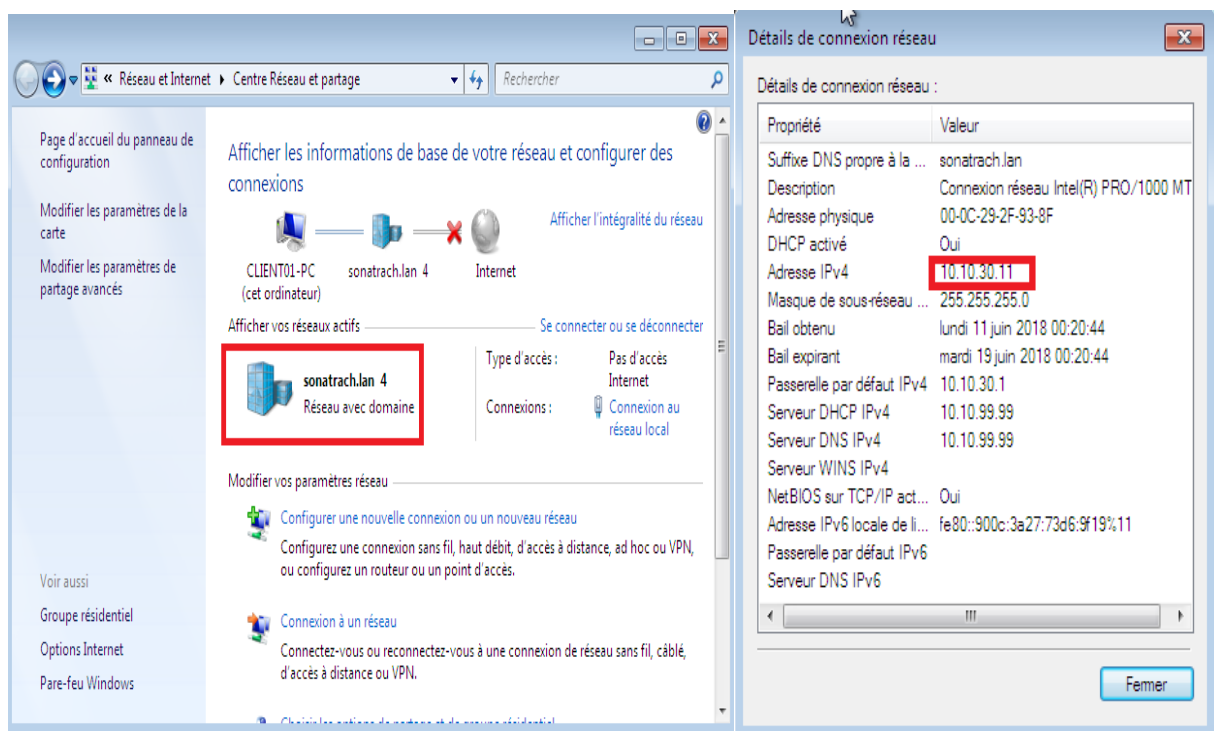
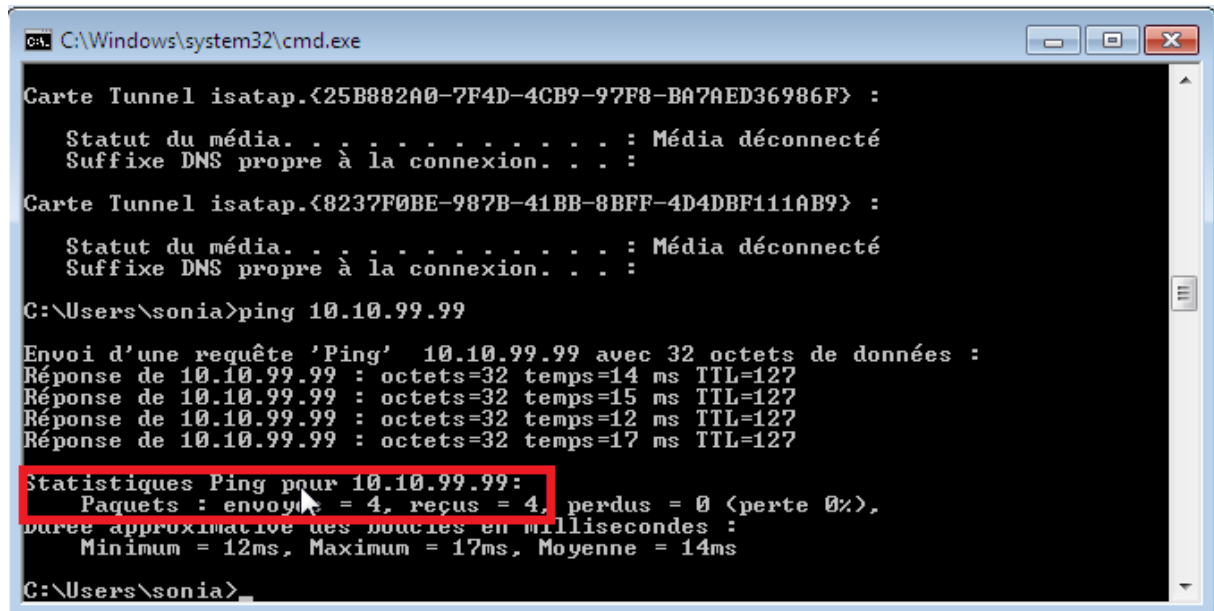


Figure 4.38 : Test de routage inter vlan et DHCP relais

- Dès qu'un PC se connecte au switch, une adresse IP lui y est attribuée. Nous avons pris l'exemple du vlan authenticated-vlan (vlan 30).
- Après avoir configurée le serveur DHCP, on va à présent tester les différents "Ping" entre un PC et le serveur d'authentification (figure 4.39).



```

C:\Windows\system32\cmd.exe

Carte Tunnel isatap.{25B882A0-7F4D-4CB9-97F8-BA7AED36986F} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.{8237F0BE-987B-41BB-8BFF-4D4DBF111AB9} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\sonia>ping 10.10.99.99

Envoi d'une requête 'Ping' 10.10.99.99 avec 32 octets de données :
Réponse de 10.10.99.99 : octets=32 temps=14 ms TTL=127
Réponse de 10.10.99.99 : octets=32 temps=15 ms TTL=127
Réponse de 10.10.99.99 : octets=32 temps=12 ms TTL=127
Réponse de 10.10.99.99 : octets=32 temps=17 ms TTL=127

Statistiques Ping pour 10.10.99.99:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    durée approximative des boucles en millisecondes :
        Minimum = 12ms, Maximum = 17ms, Moyenne = 14ms

C:\Users\sonia>
  
```

Figure 4.39 : Test du routage inter VLAN.

Après l'activation du standards 802.1x un message s'affiche dans la barre de tâche, une fois cliqué dessus l'interface dans la figure (4.40) apparaîtra demandons à l'utilisateur de saisir le couple (login /mot de passe).

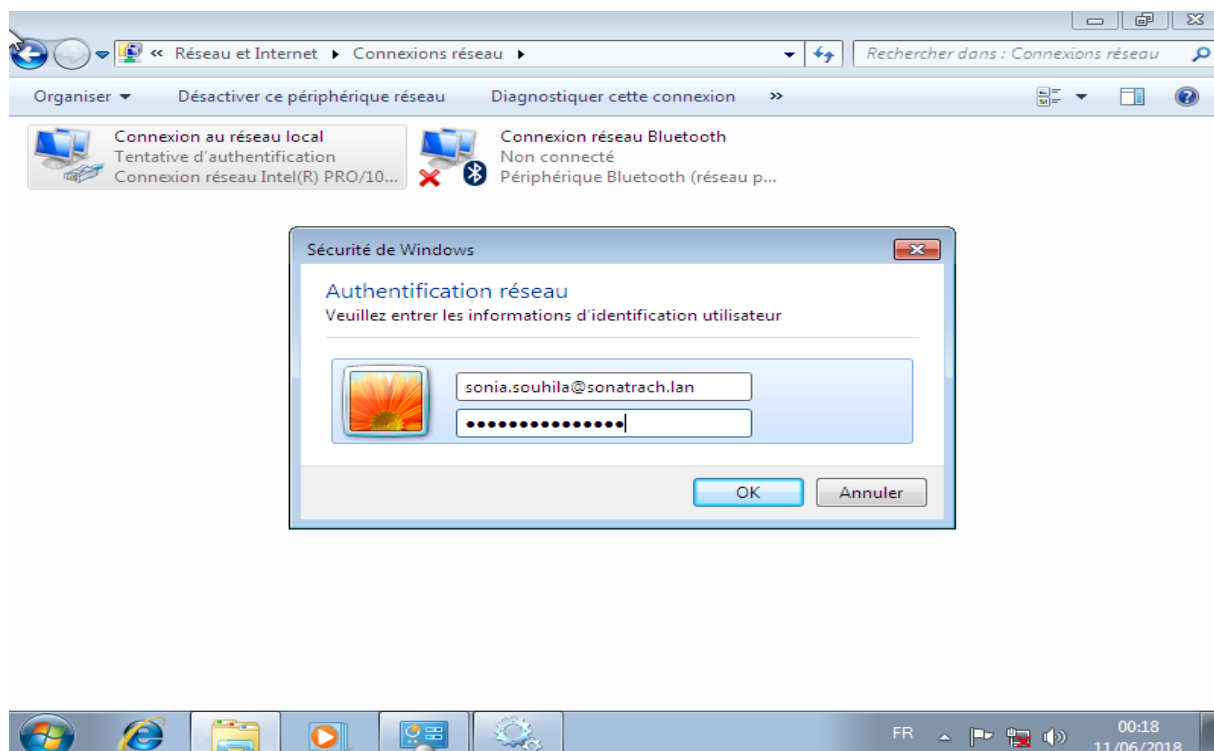


Figure 4.40: Exemple d'authentification d'un utilisateur

- **Teste sur le client :**

Dans la figure (4.41) nous avons pris l'exemple d'une authentification réussie, comme on peut le voir :

- 1) Le client est affecté au vlan 30 qui est le vlan authenticated-vlan dans notre cas.
- 2) On voit également le message « authsuccess » qui signifie authentification réussie.
- 3) Le message « interface 1/1 has changed to up » qui indique l'activation de la 802.1x sur le port.
- 4) Le message « Added MAC » nous permet de récupérer l'adresse MAC via le switch.
- 5) Le message « authzsuccess » signifie qu'après authentification, le client est autorisé à accéder au réseau.

```
*Mar 1 00:35:27.987: EAPOL pak dump rx
*Mar 1 00:35:27.987: EAPOL Version: 0x1 type: 0x0 length: 0x006B
*Mar 1 00:35:27.991: dot1x-packet:Received an EAP packet on the FastEthernet1/1 from mac 000c.292f.938f
*Mar 1 00:35:27.991: dot1x-sm:Posting EAPOL_EAP on Client=66BD8FB4
*Mar 1 00:35:27.995: dot1x_auth_bend Fa1/1: during state auth_bend_request, got event 6(eapolEap)
*Mar 1 00:35:27.995: @@@ dot1x_auth_bend Fa1/1: auth_bend_request -> auth_bend_response
*Mar 1 00:35:27.995: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_response_enter called
*Mar 1 00:35:27.995: dot1x-ev:dot1x_sendRespToServer: Response sent to the server from 000c.292f.938f
*Mar 1 00:35:27.995: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_request_response_action called
*Mar 1 00:35:27.995: AAA/AUTHEN/DOT1X (00000003): Pick method list 'default'
*Mar 1 00:35:28.051: dot1x-packet:Received an EAP Success on the FastEthernet1/1 for mac 000c.292f.938f
*Mar 1 00:35:28.055: dot1x-sm:Posting EAP_SUCCESS on Client=66BD8FB4
*Mar 1 00:35:28.055: dot1x_auth_bend Fa1/1: during state auth_bend_response, got event 11(eapSuccess)
*Mar 1 00:35:28.055: @@@ dot1x_auth_bend Fa1/1: auth_bend_response -> auth_bend_success
*Mar 1 00:35:28.059: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_response_exit called
*Mar 1 00:35:28.059: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_success_enter called
*Mar 1 00:35:28.059: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_response_success_action called
*Mar 1 00:35:28.059: dot1x_auth_bend Fa1/1: idle during state auth_bend_success
*Mar 1 00:35:28.063: @@@ dot1x_auth_bend Fa1/1: auth_bend_success -> auth_bend_idle
*Mar 1 00:35:28.063: dot1x-sm:Fa1/1:000c.292f.938f:auth_bend_idle_enter called
*Mar 1 00:35:28.067: dot1x-sm:Posting AUTH_SUCCESS on Client=66BD8FB4
*Mar 1 00:35:28.067: dot1x_auth Fa1/1: during state auth_authenticating, got event 12(authSuccess_portValid)
*Mar 1 00:35:28.067: @@@ dot1x_auth Fa1/1: auth_authenticating -> auth_authc_result
*Mar 1 00:35:28.067: dot1x-sm:Fa1/1:000c.292f.938f:auth_authenticating_exit called
*Mar 1 00:35:28.067: dot1x-sm:Fa1/1:000c.292f.938f:auth_authc_result_enter called
*Mar 1 00:35:28.071: dot1x-ev:dot1x_vlan_assign_authc_success called on interface FastEthernet1/1
*Mar 1 00:35:28.071: dot1x-ev:RADIUS provided VLAN name 30 to interface FastEthernet1/1
*Mar 1 00:35:28.071: dot1x-ev:dot1x_switch_pm_port_set_vlan: Setting vlan 30 on interface FastEthernet1/1 (1)
*Mar 1 00:35:28.071: dot1x-ev:Assigning dynamic vlan = 30 on port FastEthernet1/1
*Mar 1 00:35:28.071: dot1x-ev:Successfully assigned VLAN 30 to interface FastEthernet1/1
*Mar 1 00:35:28.071: dot1x-sm:Posting AUTHC_SUCCESS on Client=66BD8FB4
*Mar 1 00:35:28.071: dot1x_auth Fa1/1: during state auth_authc_result, got event 22(authcSuccess) (2)
*Mar 1 00:35:28.071: @@@ dot1x_auth Fa1/1: auth_authc_result -> auth_authz_success
*Mar 1 00:35:28.071: dot1x-sm:Fa1/1:000c.292f.938f:auth_authz_success_enter called
*Mar 1 00:35:28.087: dot1x-registry:dot1x_switch_port_linkcominup invoked on interface Fa1/1
*Mar 1 00:35:28.087: dot1x-ev:dot1x_mgr_if_state_change: FastEthernet1/1 has changed to UP (3)
*Mar 1 00:35:28.103: dot1x-registry:** dot1x_switch_vp_statechange:
*Mar 1 00:35:28.103: dot1x-ev:vlan 30 vp is added on the interface FastEthernet1/1
*Mar 1 00:35:28.119: dot1x-ev:dot1x_switch_addr_add: Added MAC 000c.292f.938f to vlan 30 on interface FastEthernet1/1 (4)
*Mar 1 00:35:28.119: dot1x-ev:Received successful Authz complete for 000c.292f.938f
*Mar 1 00:35:28.119: dot1x-sm:Posting AUTHZ_SUCCESS on Client=66BD8FB4
*Mar 1 00:35:28.119: dot1x_auth Fa1/1: during state auth_authz_success, got event 25(authzSuccess) (5)
*Mar 1 00:35:28.119: @@@ dot1x_auth Fa1/1: auth_authz_success -> auth_authenti
```

Figure 4.41: Cas d'une authentification réussie.

- **TEST des paquets échangé entre le client et le serveur Radius**

Dans la figure (4.42) Nous sommes en face d'un échange entre l'Authenticator (point d'accès SWITCH – 10.10.99.1) et le serveur Radius (Authentication Server – 10.10.99.99). Cet échange se fait en 4 trames et utilise le protocole de transport UDP. On constate bien aussi le port de destination « radius 1812 » ainsi que tous les attributs contenus dans le paquet, par exemple le port utilisé par le NAS (est fixe par rapport au port du switch relié) ou encore le login utilisé lors de cet authentification (sonia.souhila).

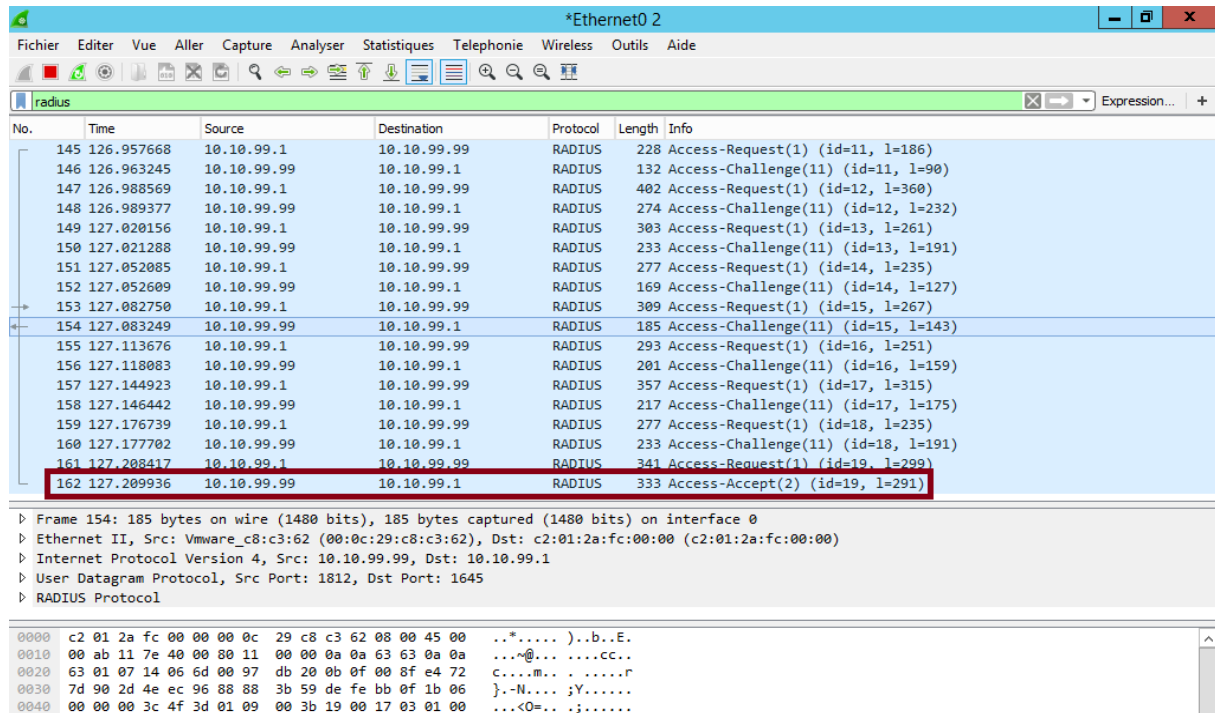


Figure 4.42 : Exemple des messages échangés dans le client RADIUS et le serveur RADIUS.

- a) **Vlan 40** : un Pc dont le standard IEEE 802.1X est activé et non du domaine ni d'un employé qui a un compte utilisateur se voit attribuer au VLAN 40

Dans ce cas l'authentification a échoué et dès que on tape la commande d'activation du 802.1x sur le switch un message s'affiche dans la barre de tâche en demandant à l'utilisateur de s'authentifier.

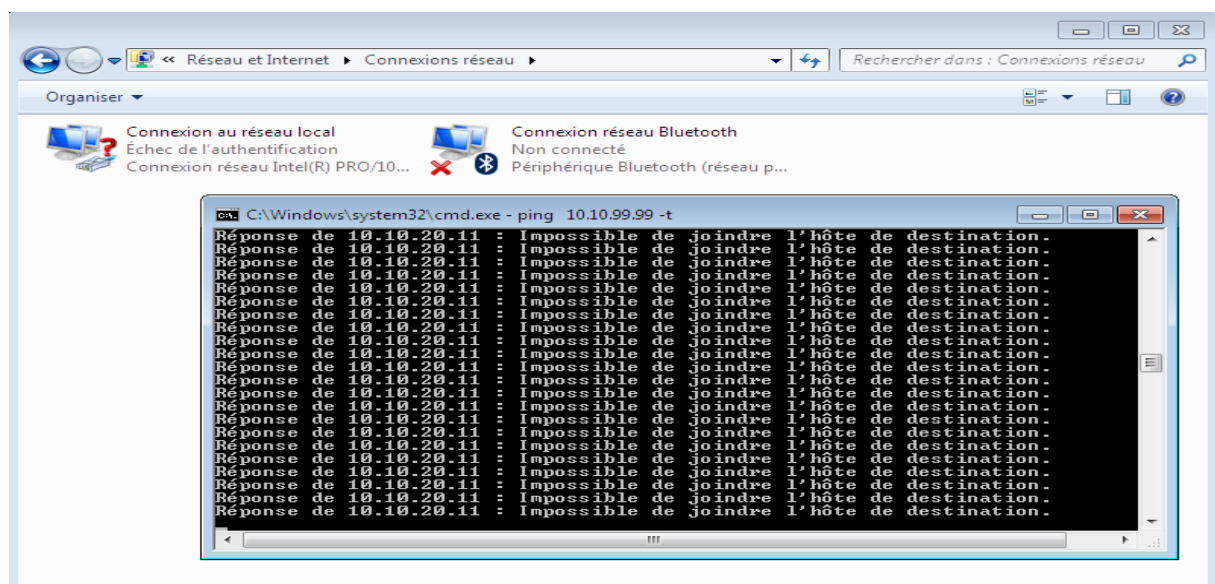


Figure 4.43: Test du vlan 40

Dans le cas où l'utilisateur n'est pas relié au domaine l'authentification n'est pas réussite alors il sera assigné au vlan 40, voir la figure (4.44).

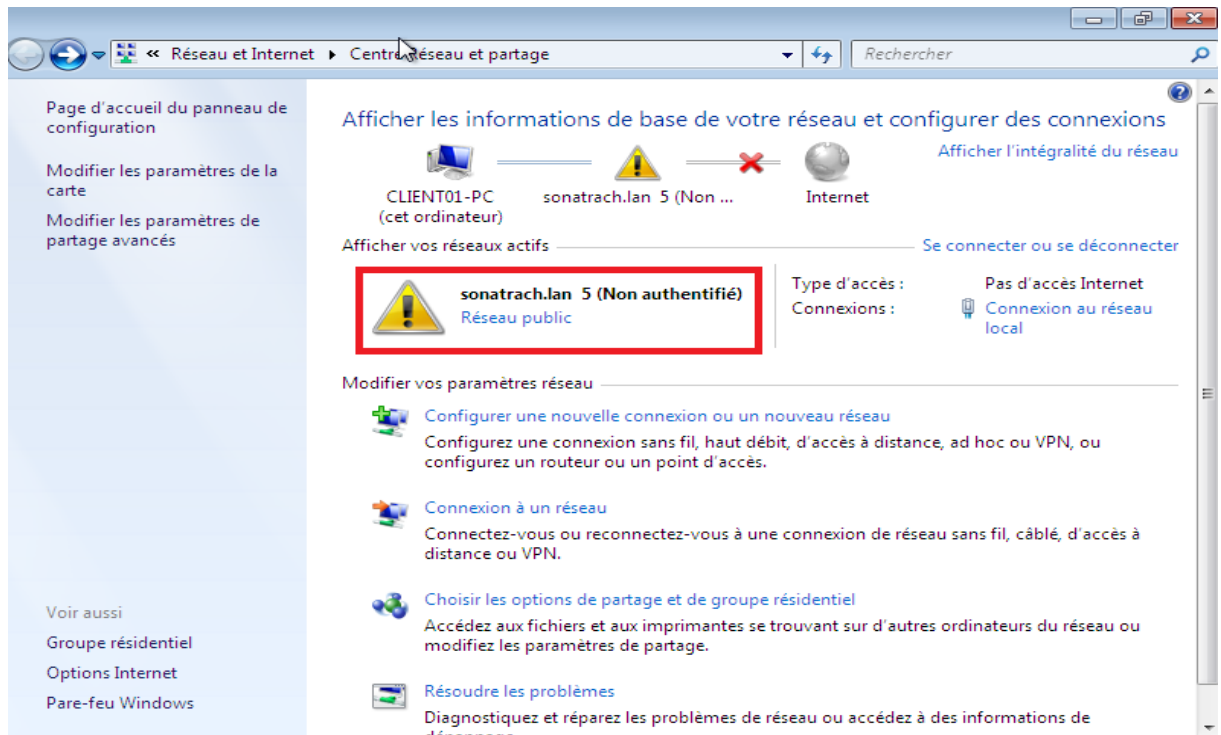


Figure 4.44 : Exemple d'une authentification non réussite.

Les commandes dans la figure (4.45), prend l'exemple d'une authentification non réussite :

- 1) La message « eaptimeout » signifie que le temps d'authentification est expiré.
- 2) Le message « authTimeout » signifie que le temps d'autorisation est expiré.
- 3) Tandis que le message « AUTH_FAIL » signifie que l'authentification a échouée.

```
*Mar 1 01:19:55.819: dot1x-ev:Received an EAP Timeout on FastEthernet1/1 for mac 0000.0000.0000
*Mar 1 01:19:55.823: dot1x-sm:Posting EAP TIMEOUT on Client=650A1E28
*Mar 1 01:19:55.823: dot1x_auth_bend Fa1/1: during state auth_bend request, got event 12(eapTimeout)
*Mar 1 01:19:55.823: @@@ dot1x_auth_bend Fa1/1: auth_bend request -> auth_bend timeout
*Mar 1 01:19:55.823: dot1x-sm:Fa1/1:0000.0000.0000:auth_bend_timeout enter called
*Mar 1 01:19:55.827: dot1x-sm:Fa1/1:0000.0000.0000:auth_bend_request_timeout action called
*Mar 1 01:19:55.827: dot1x_auth_bend Fa1/1: idle during state auth_bend_timeout
*Mar 1 01:19:55.827: @@@ dot1x_auth_bend Fa1/1: auth_bend_timeout -> auth_bend_idle
*Mar 1 01:19:55.827: dot1x-sm:Fa1/1:0000.0000.0000:auth_bend_idle enter called
*Mar 1 01:19:55.831: dot1x-sm:Posting AUTH_TIMEOUT on Client=650A1E28
*Mar 1 01:19:55.831: dot1x_auth Fa1/1: during state auth_authenticating, got event 14(authTimeout)
*Mar 1 01:19:55.831: @@@ dot1x_auth Fa1/1: auth_authenticating -> auth_fallback
*Mar 1 01:19:55.835: dot1x-sm:Fa1/1:0000.0000.0000:auth_authenticating_exit called
*Mar 1 01:19:55.835: dot1x-sm:Fa1/1:0000.0000.0000:auth_fallback enter called
*Mar 1 01:19:55.835: dot1x-sm:Posting AUTH_FAIL on Client=650A1E28
*Mar 1 01:19:55.835: dot1x_auth Fa1/1: during state auth_fallback, got event 15(authFail)
*Mar 1 01:19:55.835: @@@ dot1x_auth Fa1/1: auth_fallback -> auth_authc_result
*Mar 1 01:19:55.839: dot1x-sm:Fa1/1:0000.0000.0000:auth_authc_result enter called
*Mar 1 01:19:55.839: dot1x-sm:Posting AUTHC_FAIL on Client=650A1E28
*Mar 1 01:19:55.839: dot1x_auth Fa1/1: during state auth_authc_result, got event 23(authcFail)
*Mar 1 01:19:55.839: @@@ dot1x_auth Fa1/1: auth_authc_result -> auth_held
*Mar 1 01:19:55.843: dot1x-sm:Posting RESTART on Client=650A1E28
*Mar 1 01:19:55.843: dot1x_auth Fa1/1: during state auth_held, got event 13(restart)
*Mar 1 01:19:55.843: @@@ dot1x_auth Fa1/1: auth_held -> auth_restart
*Mar 1 01:19:55.843: dot1x-sm:Fa1/1:0000.0000.0000:auth_held_exit called
*Mar 1 01:19:55.843: dot1x-sm:Fa1/1:0000.0000.0000:auth_restart enter called
*Mar 1 01:19:55.847: dot1x-ev:Resetting the client 0000.0000.0000
*Mar 1 01:19:55.847: dot1x-sm:Posting EAP_RESTART on Client=650A1E28
*Mar 1 01:19:55.847: dot1x_auth Fa1/1: during state auth_restart, got event 6(no_eapRestart)
*Mar 1 01:19:55.847: @@@ dot1x_auth Fa1/1: auth_restart -> auth_connecting
*Mar 1 01:19:55.851: dot1x-sm:Fa1/1:0000.0000.0000:auth_connecting enter called
```

Figure 4.45 : cas d'une authentification non réussite.

4.6. Conclusion

La réalisation de ce chapitre nous a permis de découvrir l'environnement de Windows Server 2012 R2 et de se familiariser avec ses différents composants et services que nous pouvons décomposer comme suit : Premièrement en termes de fonctionnalités, à savoir l'organisation des ressources de l'entreprise que ce soit humaines ou matérielles en utilisant l'AD. Deuxièmement, en termes de sécurité, que ce soit par la définition des stratégies de groupe ou par l'infrastructure PKI qui offre aux utilisateurs du domaine la possibilité de chiffrement et de signature à l'aide des certificats. Troisièmement, en termes de gestion d'adressage dynamique qui se fait grâce au serveur DHCP.

Conclusion générale

Ce projet a été une occasion pour nous enrichir et perfectionner nos capacités académiques et pédagogiques. Pour munir à bien le travail demandé, nous nous sommes impliquées rigoureusement dans la réalisation de notre projet durant toute la période de stage.

Notre stage pratique nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion de nous familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir, approfondir nos connaissances et de les appliquer aux diverses réalités du terrain.

Dans ce projet nous avons établi un système d'authentification des machines avant tout accès au réseau de l'entreprise SONATRACH brache de transport par canalisation (RTC DE BEJAIA) qui est basée sur la norme 802.1X et le protocole RADIUS.

Pour proposer une solution de sécurité, nous nous sommes basés sur l'analyse du réseau LAN de l'entreprise ainsi que ces besoins attendus.

Pour l'implémentation de la solution, nous avons utilisé les outils suivants :

- L'administration et la sécurité des réseaux locaux dans une entreprise.
- La gestion des différentes machines sous Windows Server 2012 R2.
- La configuration des switches et des routeurs sous GNS3.

Pour terminer, nous tenons à souligner que nous n'avons nullement pas la prétention d'avoir présenté un travail parfait, car aucun travail scientifique ne peut l'être, ainsi diverses perspectives futures pourront être envisagées :

- La gestion de groupe(GPO).
- Configuration du NAP pour analyser l'état de santé de l'ordinateur client.
- Création des des tunelles VPN/RADIUS pour renforcer la sécurité.

Liste des références

- [1] B. Davie, L. Peterson. *Réseaux d'ordinateurs*. Vuibert, 1998.
- [2] N. Benbara, N. Bouchama Nesrine, M.Moketfi. *Administration et Supervision d'un Réseau LAN à l'aide des solutions open source Cas: Entreprise SONATRACH Béjaia. 2017.Memoire de fin cycle M2*. Université A/Mira de Béjaia.2017.
- [3] J-F. Pillou, *Tout sur les réseaux et Internet*, Dunod,Paris 2006.
- [4] R.Myana.*Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP* Cas de Mecelco.Thèse de doctorat. 2011.
- [5] V.Remazeilles. *La sécurité des réseaux avec Cisco*. Editions ENI, 2009.
- [6] D.Bertrand. *Etude et mise en œuvre du protocole 802.1 X dans le cadre de la politique de sécurité de Sphéria Val de France*.Thèse de doctorat.2013.
- [7] P-E. Périllon. *L'authentification avec 802.1X*. Université claude bernard Lyon1.2008.
- [8] J-F.Pillou, J-PH.BAY, *Tout sur la scurité informatique*, 4^{ème} édition .Dunod,Paris 2016.
- [9] H.Olivier. *A strang authentication server for ALCASAR*, *memoire de fin de cycle M2*.Ecole d'ingénieur du monde numérique.2013.
- [10] T.Coeytaux. *La thechnologie de contrôle d'accès réseau, 802.1X et son implémentation pratique*.Mémoire de fin de cycle M2.Haute école de gestion de Genève(HEG-GE)2012.
- [11] R.Vincent. *La sécurité des réseaux avec cisco*.ENI, Février 2009.
- [12] Cisco système, *wired 802.1X deployment guide*, cisco, 2011.
- [13] N. Saadali, K.Ouaret, A.Boukerram. *Installation et configuration des services de Windows server 2012 Cas d'etude: Candia Tchir-Lait*. Mémoire de fin de cycle M2. Université Abderrahmane Mira Béjaia.2017.
- [14] S.Caicoya, J-G Saury. *TCP/IP le guide complet 2^{ème} édition*. MA édition.2012.
- [15] <https://www.e-qual.fr/accueil-2/reseau-informatique-entreprise/>.
- [16]https://www.fibre+optique&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjWpoLipuzbAhXFC8AKHXTA9MQ_AUICigB&biw=1366&bih=613#imgrc=unoPtUa3BSf3XM:
- [17]https://www.google.dz/search?q=paire+torsad%C3%A9&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiZ2tfypzbAhWoQJoKHQeRA0Q_AUICigB&biw=1366&bih=613#imgrc=Pxqau8USp6XGFM:

- [18] <https://www.livescience.com/50399-radio-waves.html>.
- [19] <https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.cidr.html>.
- [20] A.Akilal, Z.Farah. *Cours de la sécurité informatique*. Université de Béjaia.2016/2017.
- [21] A.Boukerram. *Cours de la sécurité informatique*. Université de Béjaia.2017/2018.
- [22] <https://fr.wikipedia.org/wiki/Sonatrach>.
- [23] A.Sider. *Cour de Technologie Internet*. Université de Béjaia. 2017/2018.

A.1. Installation de Windows server 2012

L'installation de Windows server 2012 est très classique et ressemble à celle de Windows 8. Ce système peut être installé en démarrant depuis le DVD, ou depuis une image ISO.

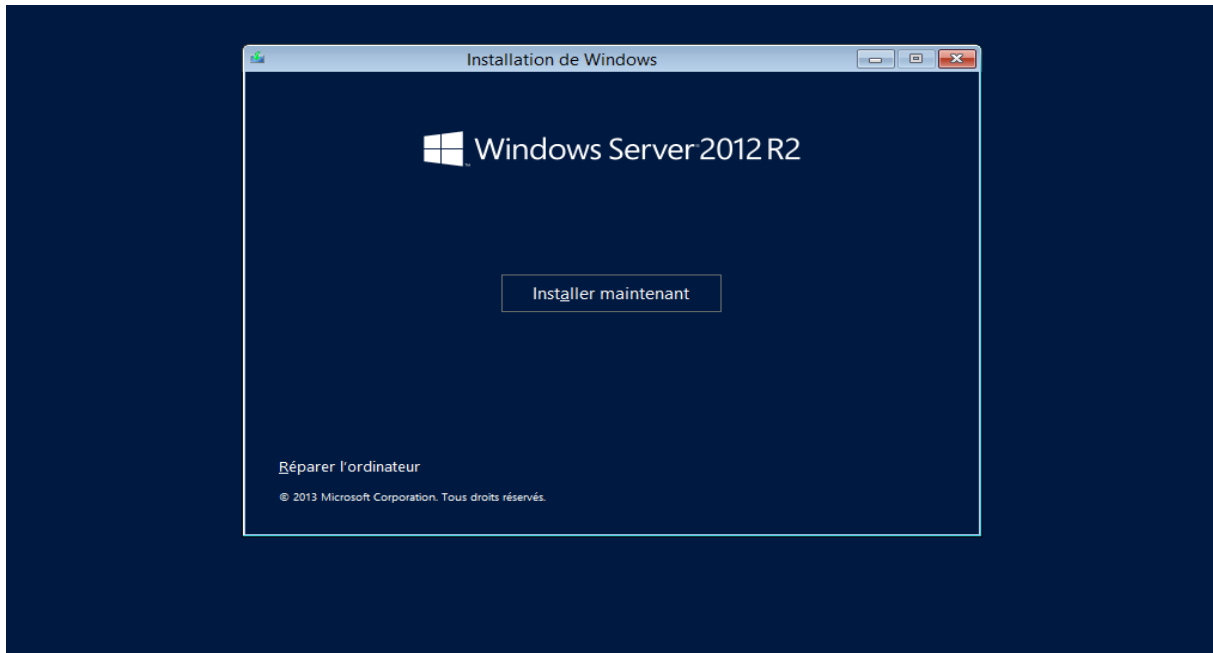


Figure A.1 : Installation de Windows serveur 2012

A.2. Gestionnaire de serveur

Le premier démarrage se fait sur l'écran Gestionnaire de serveur, son design est très différent des anciennes versions de Windows server mais les fonctions sont conservées, voire améliorées. Celui-ci nous donne la possibilité d'ajouter des rôles, surveiller l'état de notre serveur ou encore gérer ses fonctionnalités

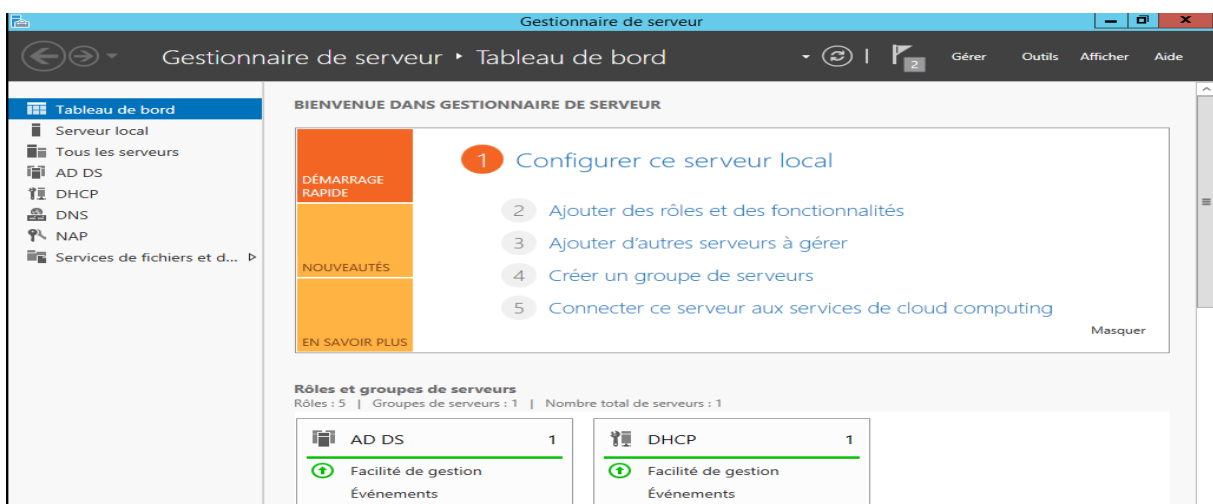


Figure A.2 : Gestionnaire de serveur

A.3. Installation de l'active directory

Avant de promouvoir le serveur en tant que contrôleur de domaine dans notre domaine, il faut installer (le rôle Service de domaine Active Directory).

- Dans le Gestionnaire de serveur, nous avons sélectionné (Ajout des rôles et des fonctionnalités).
- Au niveau des rôles, choisir (Service AD DS) qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour indiquer que d'autres éléments requis AD DS doivent être installés, cliquer sur "Ajouter des fonctionnalités".

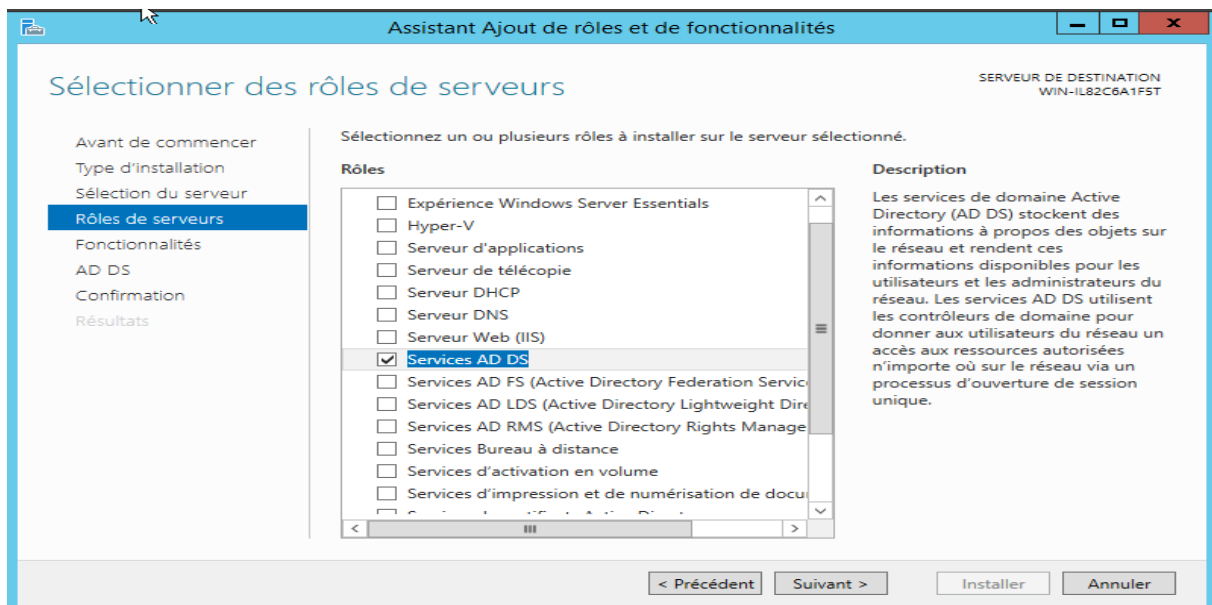


Figure A.3 : Ajout du service AD DS.

Une fois les fonctionnalités d'AD DS installées, le serveur va redémarrer automatiquement. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé.

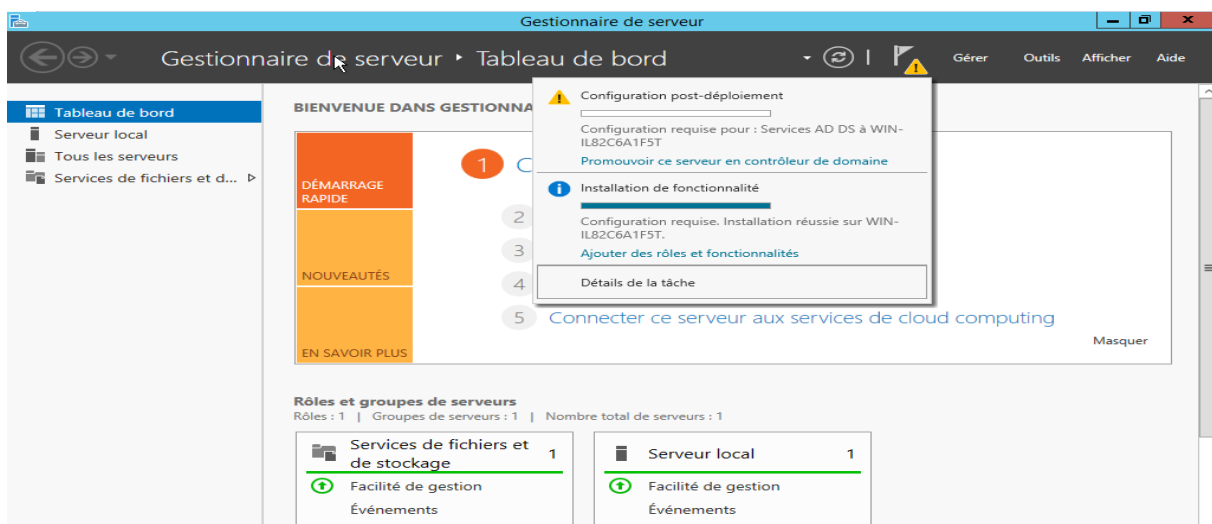


Figure A.4 : Promouvoir du serveur en contrôleur de domaine.

A.4. Installation du service DHCP

Dans l'assistant de gestion des rôles, ajouter le rôle DHCP.

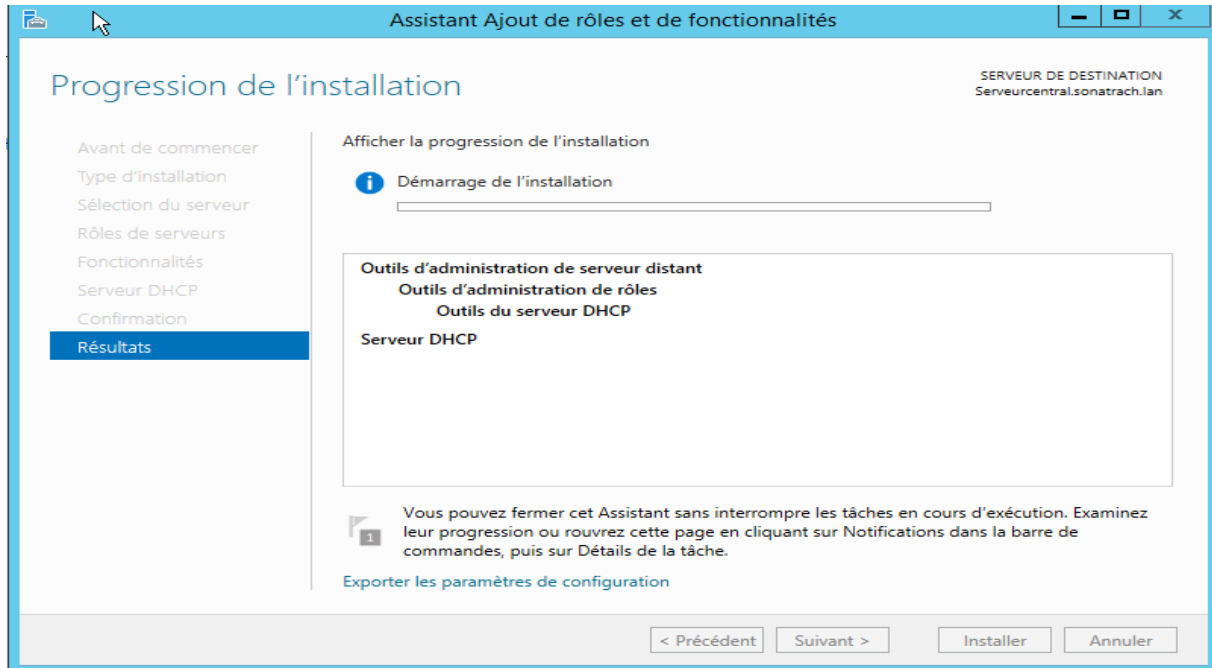


Figure A.5 : Installation du serveur DHCP.

Après quelques minutes le rôle est installé, l'écran final nous invite à commencer la configuration de DHCP.

A.5.1. Ajout du rôle NPS (Network Policy Server)

Dans la console gestionnaire de serveur, cliquer sur Gérer, puis sur ajouter des rôles et fonctionnalités, dans la rubrique de rôle de serveurs sélectionner « Services de stratégies et accès réseau », ajouter les fonctionnalités par défaut, Au niveau de services de rôle, sélectionner uniquement « Serveur NPS » et lancer l'installation.

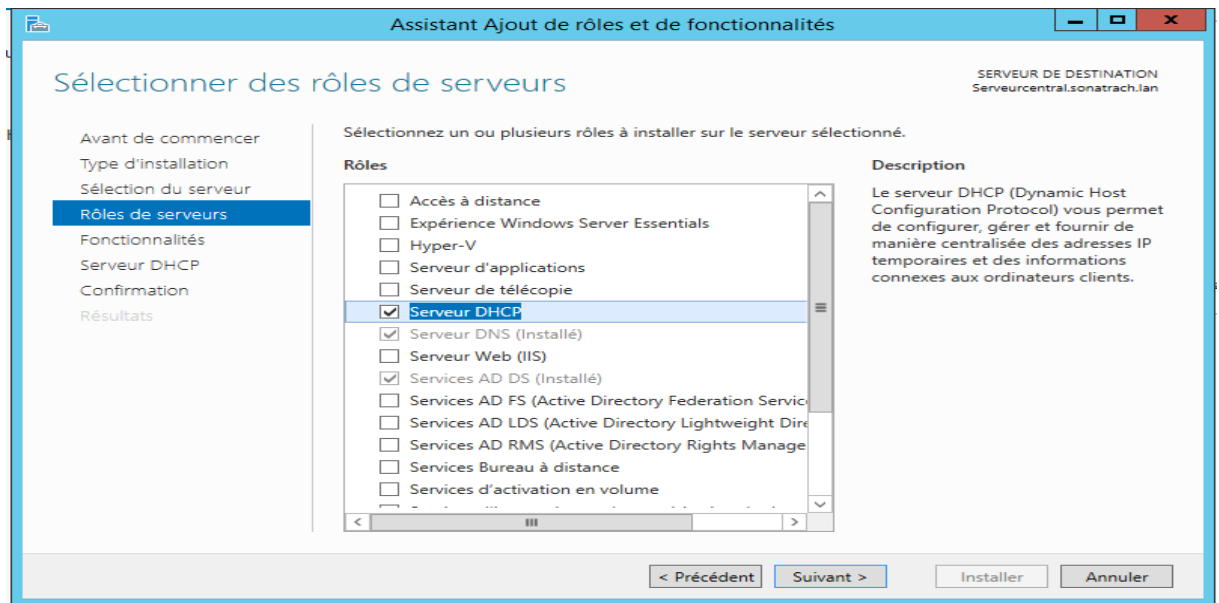
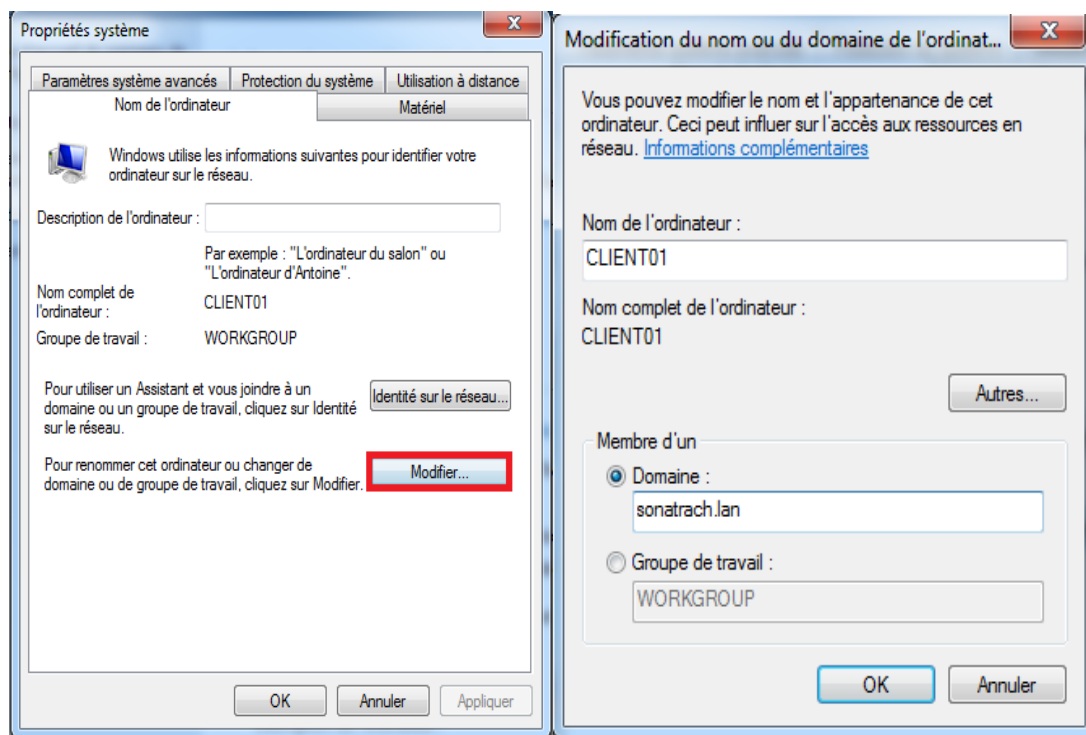


Figure A.6 : ajout du rôle NPS

A.6. Joindre le pc au domaine

Afin qu'en puissent joindre un pc au domaine, Dans système on appui sur modifier les paramètres puis nous allons saisir le nom du domaine auquel il sera joint. Voir la figure (A.7)



Figures A.7 : Modifier le nom du domaine

Une fois que le nom du domaine est saisi, on va introduire le nom et le mot de passe de l'utilisateur (fig A.8).

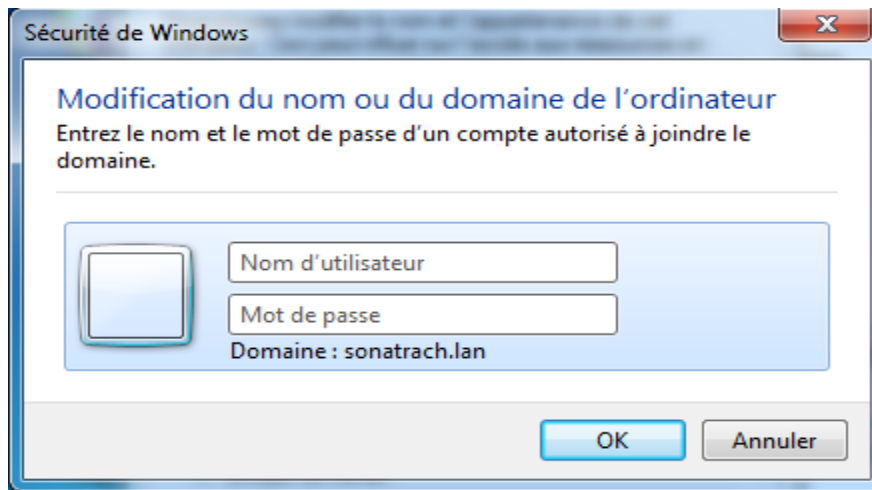


Figure A.8 : Saisie du nom et du mot de passe

Une boîte de dialogue s'affiche pour informer que le PC est bien joint au domaine (fig A.9).

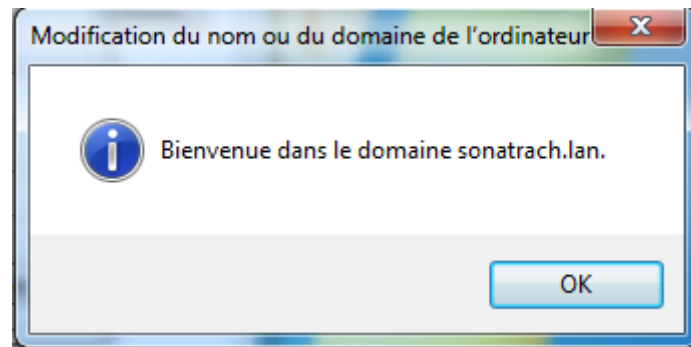


Figure A.9 : boîte de dialogue

Enfin on doit redémarrer le PC. Pour que les modifications s'appliquent sur ce dernier (fig A.10).

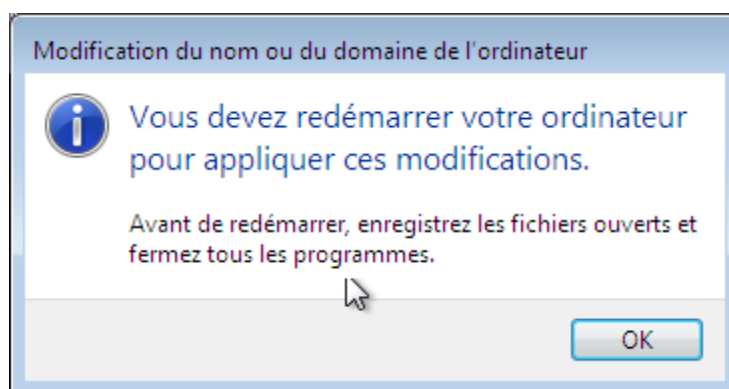


Figure A.10 : Notification pour redémarrer de pc

A.7. Activer l'authentification 802.1x pour PC

- ✓ Pour utiliser 802.1x, le client doit activer 802.1x. S'il n'est pas activé, l'utilisateur ne sera pas authentifié et sera assigné au VLAN 30.

En effet, sur la barre démarrée en tape « service » puis avec le bouton droit « ouvrir » comme illustré sur la figure (A.12) :

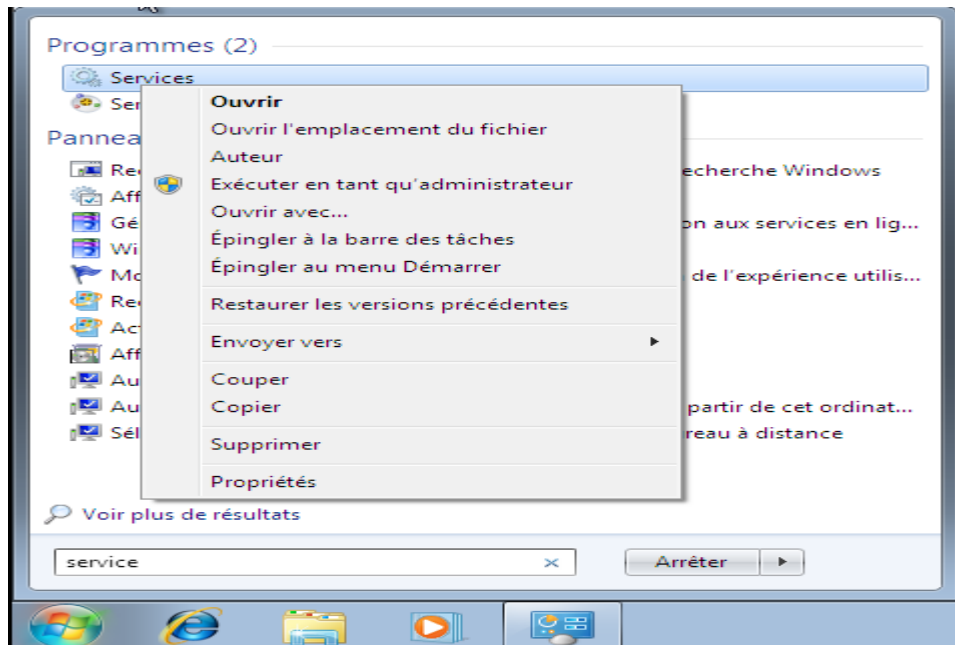


Figure A.11: Démarrage du service

Ensuite y'aura une fenêtre qui va apparaître en demandant d'entrer le nom d'utilisateur et mot de passe dans Active Directory pour l'authentification avec le serveur RADIUS.

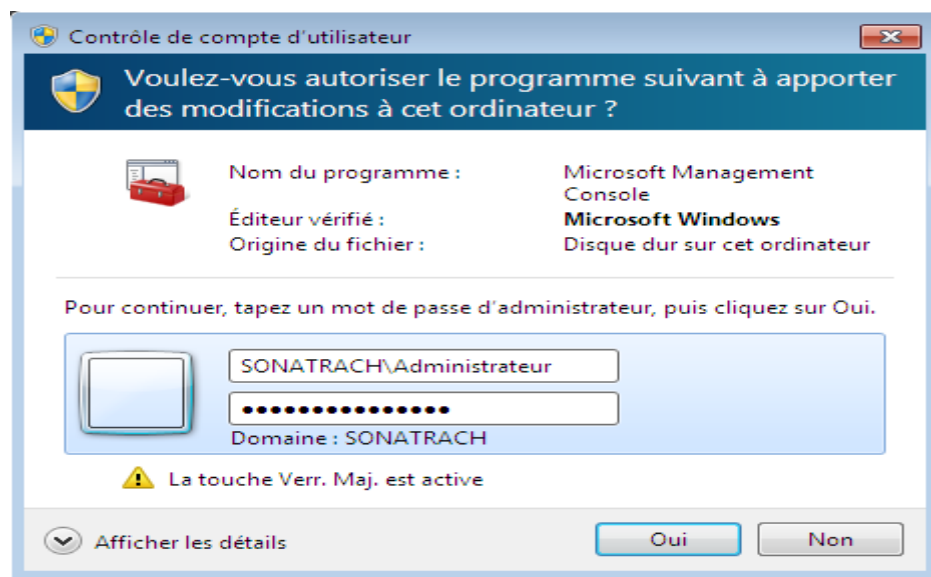


Figure A.12 : authentification au tant qu'administrateur

Si les machines ont rejoint le domaine, nous pouvons créer des stratégies sur Active Directory pour activer 802.1x pour les PC qui ont rejoint le domaine. Ce PC n'a pas rejoint le domaine

donc je vais devoir démarrer le service "configuration automatique de réseau local " pour activer 802.1x.

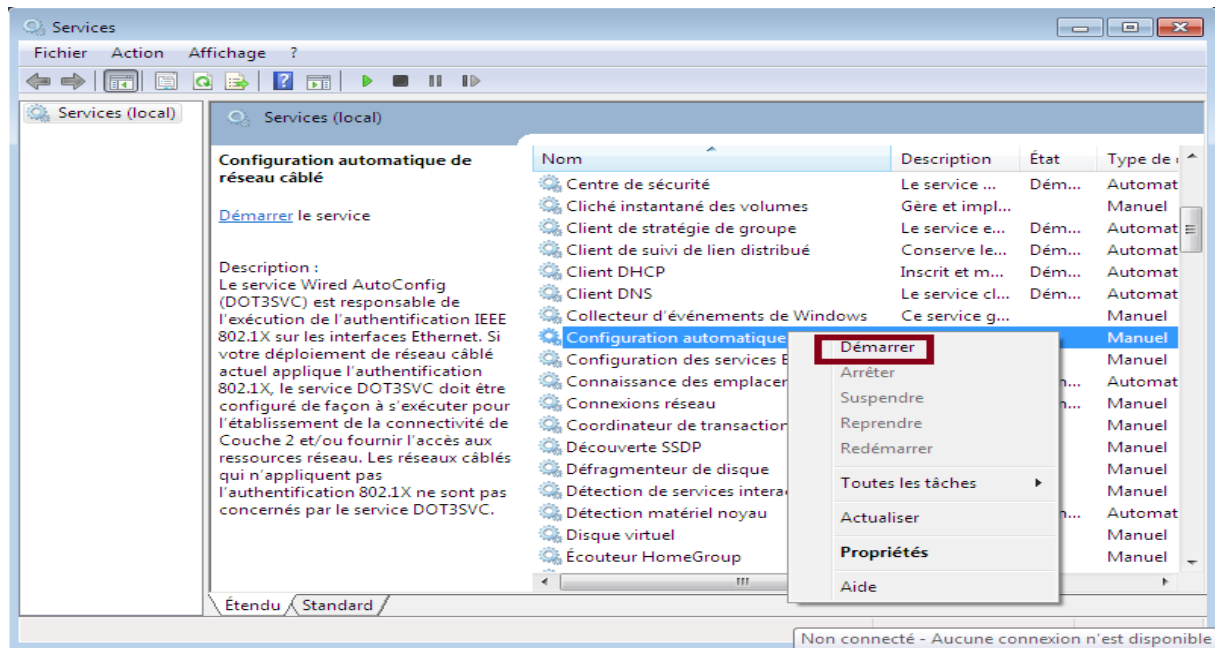


Figure A.13 : démarrage et activation du service 802.1x

Après le démarrage du service 802.1x, "Propriétés Ethernet" aura plus d'onglet "Authentification". Sélectionnez "Activer l'authentification IEEE 802.1X" pour activer et sélectionner la méthode d'authentification avec le serveur RADIUS comme "Microsoft : Protected EAP (PEAP)", voir la figure (A.10).

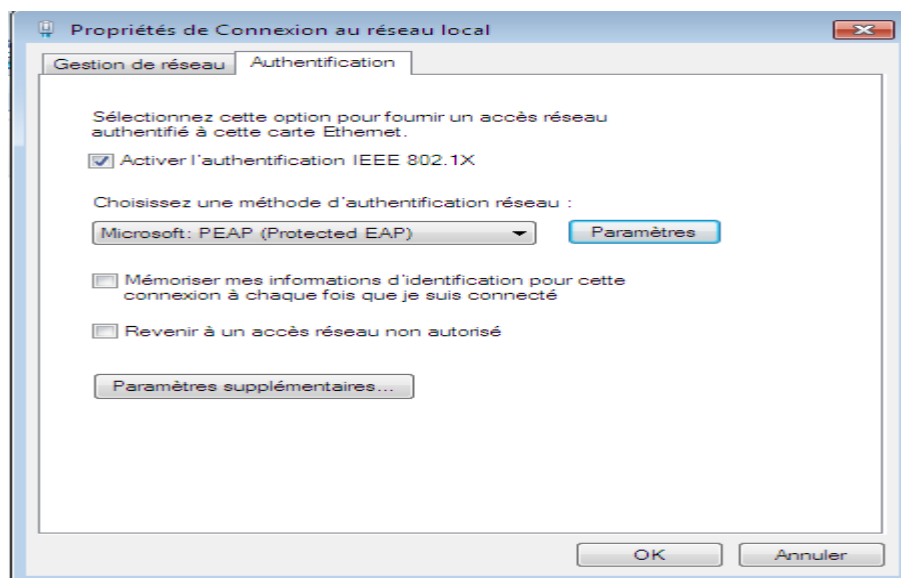


Figure A.14 : Activation du standard IEEE 802.1x.

Une fois l'authentification est bien réussite en remarque que le serveur DHCP lui effectue l'adresse du vlan 30

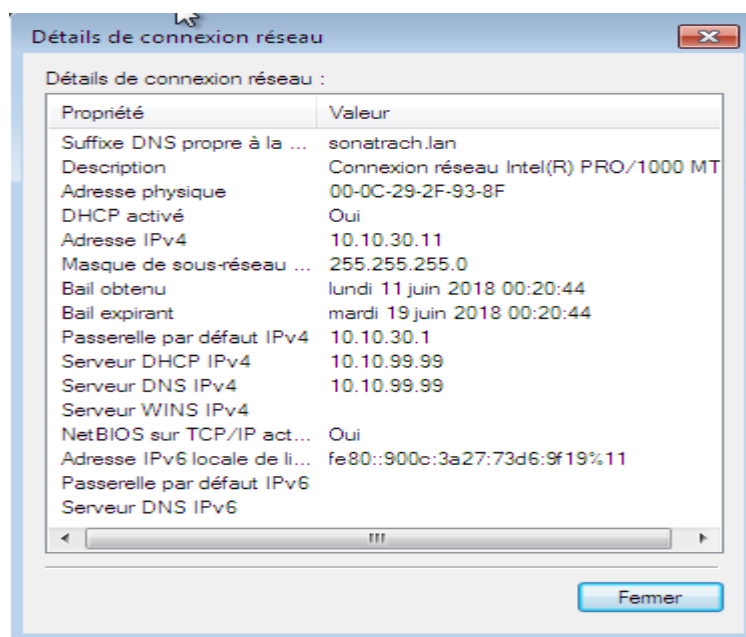


Figure A.12 : Affectation de l'adresse IP après authentification.

B.1. Mode privilégié

Pour entrer en mode privilégié, il suffit de taper la commande suivante (figure B.1) :

```
SW-B > enable
```

Figure B.1 : Mode privilégié.

Une fois dans le mode privilégié, on pourra effectuer plusieurs actions, on cite quelques-unes :

B.1.1. Afficher la configuration de base

Pour afficher une configuration, il suffit de taper la commande suivante (figure B.1.1) :

```
SW-D1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
10	isolation	active	
20	no-authenticated-vlan	active	
30	authenticated-vlan	active	
40	guest	active	
99	management	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

Figure B.1.1 : Afficher la configuration de base dans un switch.

B.1.2. Supprimer une configuration

La commande dans la figure (B.1.1) permet de supprimer la configuration dans un switch

```
SW-D1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
```

Figure B.1.2 : Supprimer une configuration dans un switch

B.1.3. Sauvegarder une configuration

La commande dans La figure (B.1.3) permet de sauvegarder la configuration dans un switch.

```
SW-D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure B.1.3. : Sauvegarder une configuration dans un switch.

B.2. Mode d'exécution globale

Pour entrer dans le mode d'exécution globale, il suffit de taper la commande dans la figure (B.2).

```
IOU1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU1(config)#
```

Figure B.2 : Mode d'exécution globale.

Une fois dans ce mode, nous pouvons effectuer diverses opérations, on citera quelques-unes.

B.2.1. Configuration de hostname

Pour changer le nom d'un switch, il suffit de taper la commande dans la figure (B.1.2).

```
IOU1(config)#hostname S-COEUR
```

Figure B.2.1 : Configuration de hostname.

B.2.2. Configuration des VTP

Pour la configuration des vtp (on a pris l'exemple du vtp serveur qui sera configuré dans le switch cœur), il suffit de taper les commandes dans la figure (B.2.2).

```
SW-D1(config)#vtp domain sonatrach.lan
Domain name already set to sonatrach.lan.
SW-D1(config)#vtp mode server
Device mode already VTP Server for VLANs.
SW-D1(config)#vtp version 2
VTP version is already 2
SW-D1(config)#
*Jun 23 13:08:54.279: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not half duplex), with
SW-COEUR Ethernet0/0 (half duplex).
SW-D1(config)#vtp password sonatrach2018!@
Password already set to sonatrach2018!@
```

Figure B.2.2 : Configuration de vtp.

B.2.3. Configuration de l'étherchanelle

Etherchanelle c'est le rassemblement de plusieurs liens physiques dans un seul lien logique afin d'améliorer la bande passante.

Pour effectuer cette configuration dans un switch, il suffit de taper les commandes dans la figure (B.2.3).

```
sw-coeur(config)#interface range ethernet 0/0-3
sw-coeur(config-if-range)#channel-protocol lacp
sw-coeur(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

sw-coeur(config-if-range)#exit
sw-coeur(config)#in
*Jun 3 09:47:11.339: %EC-5-L3DONTBNDL2: Et0/1 suspended: LACP currently not enabled on the remote port.
*Jun 3 09:47:11.700: %EC-5-L3DONTBNDL2: Et0/0 suspended: LACP currently not enabled on the remote port.
*Jun 3 09:47:11.874: %EC-5-L3DONTBNDL2: Et0/3 suspended: LACP currently not enabled on the remote port.
*Jun 3 09:47:11.894: %EC-5-L3DONTBNDL2: Et0/2 suspended: LACP currently not enabled on the remote port.
sw-coeur(config)#interface port-channel 1
sw-coeur(config-if)#switchport trunk encapsulation dot1q
sw-coeur(config-if)#switchport mode trunk
sw-coeur(config-if)#exit
```

Figure B.2.3 : Configuration d'étherchanelle.

B.2.4. Configuration du SSH

Configuration d'un compte utilisateur avec un mot de passe en utilisant la syntaxe *user Name(nom-utilisateur) password(mot de passe)*, par la suite on définit un nom de domaine pour que le routeur puisse générer les clés de chiffrement en utilisant la Commande *ip domain-name*. La figure (B.2.4) illustre la suite des commandes à entrer dans le switch :

```
SW-D1(config)#
*Jun 23 13:19:35.924: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-D1(config)#ip ssh version 2
SW-D1(config)#ip ssh time ou 120
^
% Invalid input detected at '^' marker.

SW-D1(config)#ip ssh time
SW-D1(config)#ip ssh time-out
*Jun 23 13:20:21.780: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/1 (not half duplex)
h SW-COEUR Ethernet0/1 (half duplex).
*Jun 23 13:20:22.112: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not half duplex)
h SW-COEUR Ethernet0/0 (half duplex).
SW-D1(config)#ip ssh time-out 120
SW-D1(config)#ip ssh authentication-retries 3
^
% Invalid input detected at '^' marker.

SW-D1(config)#ip ssh authentication-
SW-D1(config)#ip ssh authentication-retries 3
SW-D1(config)#
```

Figure B.2.4 : Configuration du ssh.

B.2.5. Configuration lignes VTY

Les commandes dans la figure (B.2.5) permettent de configurer les lignes vty dans un switch.

```
SW-D1(config)#line vty 0 4
SW-D1(config-line)#password sonatrach2018!@
SW-D1(config-line)#login
SW-D1(config-line)#end
```

Figure B.2.5 : Configuration des lignes vty dans un switch.

B.2.6. Configuration des lignes consoles

Les commandes dans la figure (B.2.6) permettent de configurer les lignes console dans un switch.

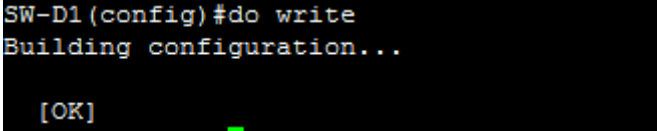
```
SW-D1(config)#line console 0
SW-D1(config-line)#password sonatrach2018!@
SW-D1(config-line)#login
SW-D1(config-line)#end
```

Figure B.2.6 : Configuration des lignes consoles.

B.2.7. Utilisation de la commande « do »

Pour effectuer l'opération de sauvegarde ou d'affichage dans le mode de configuration globale, on tape la commande « do » suivit de l'une des commandes citées précédemment.

Dans la figure (B.2.7), nous avons pris l'exemple de la sauvegarde.



```
SW-D1(config)#do write
Building configuration...

[OK]
```

Figure B.2.7 : Sauvegarder la configuration dans un switch.

Résumé

L'objectif de ce projet est de prévoir un mécanisme d'authentification basé à la fois sur la norme IEEE 802.1X et le protocole RADIUS. La réalisation de ce travail a commencé par une étude approfondie du réseau local de la BRANCHE DE TRANSPORT PAR CANALISATION de SONATRACH (RTC DE BEJAIA), pour ensuite mettre en œuvre une solution d'authentification répondant à leur exigence de sécurités. Pour la réalisation de cette solution, nous avons tout d'abord installé la machine virtuelle « VMware Workstation 2012 », par la suite nous avons importé les logiciels nécessaires pour sa mise en œuvre : GNS3 pour la simulation, PUTTY pour la configuration des switchs et des routeurs, Windows Server 2012 pour l'administration et la gestion, WireShark pour analyser les différents messages qui interagissent entre les entités.

Mots clés: IEEE 802.1x, RADIUS, VMware workstation 2012, GNS3, windows server 2012, Wireshark., Authentication

Abstract

The goal of this project is to provide an authentication mechanism based on both the IEEE 802.1X standard and the RADIUS protocol. The realization of this work began with an in-depth study of the SONATRACH (RTC DE BEJAIA) local network of the SONATRACH PIPING BRANCH, in order to then implement an authentication solution that meets their security requirements. For the realization of this solution, we first installed the virtual machine "VMware workstation 2012, for the continuation we imported the necessary software for its implementation: GnS3 for the simulation, putty for the configuration of the switches and routers, windows server 2012 for administration and management, Wireshark to analyze the different messages that interact between entities.

Keywords: IEEE 802.1x, RADIUS, VMware workstation 2012, GNS3, windows server 2012, Wireshark., Authentication