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

Mémoire de fin de cycle

En vue de l'obtention du

Diplôme de Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Mise en place d'une solution D'authentification réseau Pour l'APC de Béjaia

Présenté par :

- M. BOUSSEBISSI Toufik
- Mme. BOUSSOUFA Souhila

Encadreur :

- M. FARAH Zoubeyr

Devant le jury composé de :

Présidente : - Mme. GADOUCHE Hania

Examinateur : - M. KHANOUCHE Mohamed Essaid

Année universitaire 2021-2022

Remerciements

Avant tout développement sur cette expérience, il apparaît opportun de commencer ce mémoire par des remerciements.

D'abord au bon dieu de nous avoir accordé la force et le courage de mener à terme ce modeste travail.

Nos premières pensées se tournent vers notre maîtresse de stage Mme. Megdouda MESSAOUDI, ingénieur d'état en informatique responsable de bases de données, M. Zinedine YAHIA CHERIF, ingénieur en informatique à la direction des transmissions de la wilaya de Bejaia, M. Riad ADJIRI, premier responsable du service d'Etat Civil de l'APC de Bejaia, pour leur aimable disponibilité, pour avoir tout mis en œuvre afin que notre stage de fin d'études se passe dans les meilleures conditions.

Un grand merci à l'équipe de l'APC de Bejaïa qui nous a accompagnés tout au long de cette expérience et qui a eu la gentillesse de faire de ce stage, un moment très profitable.

On souhaiterait aussi remercier M. Zoubeyr FARAH, notre tuteur pédagogique avec qui on a entretenu de bons rapports, ainsi que pour ses judicieux conseils formulés avec beaucoup de pédagogie tout au long du stage. Il a été à l'écoute et nous a appris à adopter une bonne approche professionnelle au sein du service d'Etat Civil de l'APC de Bejaïa.

On tient à exprimer nos remerciements aux membres de jury, qui ont accepté d'évaluer notre travail.

Merci à vous.

Dédicaces

Je dédie ce modeste travail :

À la prunelle de mes yeux, mes précieux enfants, Yasmine et Yacine pour leur patience et leur soutien.

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse et leurs prières tout au long de mes études.

À mon mari Mouhamed.

À mes chères sœurs, Lamia, Aicha, Meriem et Farah pour leurs encouragements permanents, et leur soutien moral.

À mes chers frères, Abd Elhalim et Mouhamed Amine, pour leur appui et leur encouragement.

À mes adorables neveux.

À toute ma famille pour leur soutien tout au long de mon parcours.

À mon beau père Abd elmadjid CHEURFA, pour son appui et soutien.

À mes belles sœurs Lynda et Chafia qui m'ont toujours soutenues.

À mon binôme Toufik, je lui souhaite une réussite dans sa vie.

À tous mes amis.

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible.

Merci d'être toujours là pour moi.

Soussou.

Je dédie ce modeste travail :

À la mémoire de mes chers parents ellah yerhamhom.

À ma plus belle étoile qui puisse exister dans l'univers, ma très chère femme Nahla, pour sa patience et son soutien pour moi, Celle a qui je souhaite une longue vie et bonne santé.

À mon petit ange mon fils Fares, Que le dieu me le garde en très bonne santé.

À mes sœurs Farida, Ouahiba et Rafika pour leurs encouragements permanents, et leur soutien moral.

À mon frère Smail, pour son appui et son encouragement.

À mes neveux, Yacine, Mohamed, Amina et Fatima.

À mes chers, beau père Khlifa MOUHOUB et belle mère Malika MAAZIZ, pour leur appui et leur encouragement.

À mes belles sœurs, Abla, Loubna, Hafidha, Assia et Nour El Houda qui m'ont toujours soutenues.

À mes enseignants et tous les étudiants de 2ème année informatique.

À ma binôme Souhila, je lui souhaite une réussite dans sa vie.

À tous mes amis.

Et enfin à tous ceux qui m'aiment et tous ceux que j'aime.

Toufik.

SOMMAIRE

Chapitre II : Présentation de l'organisme d'accueil et problématique

Chapitre III : Installation du serveur RADIUS

Chapitre IV : Déploiement de la solution RADIUS

LISTE DES FIGURES

LISTE DES TABLEAUX

Introduction générale

Avec le développement des technologies informatiques, les réseaux locaux des entreprises présentent des infrastructures complexes qui doivent répondre à un certain nombre de normes spécifiques aux équipements à interconnecter et aux applications à supporter. C'est pourquoi la technologie de l'implémentation du réseau local offre plusieurs solutions qui doivent être adaptées tout particulièrement à l'architecture de l'organisme concerné et d'accompagner sa croissance tout en sécurisant ses services des attaques qui proviennent de l'intérieure ou de l'extérieure de l'entreprise.

L'APC de Béjaia, comme toute administration algérienne, connait une large opération d'informatisation de ses structures. Ceci a engendré le besoin d'adopter des solutions de sécurité réseau, notamment des solutions de contrôle d'accès qui sécurise le réseau de toute intrusion éventuelle, et qui permet de reconnaitre les utilisateurs et définir les droits qui leurs sont accordés.

L'objectif de notre travail est de mettre en place un système d'authentification des utilisateurs par un login et un mot de passe, il s'agit exactement de configurer un point d'accès au réseau de tel manière à ce que tout utilisateur doit s'authentifier par un nom d'utilisateur et un mot de passe à chaque tentative d'accès. Afin de répondre à cet objectif, nous avons optés pour une solution d'authentification basée sur le serveur RADIUS (client/ serveur).

Radius avait tout d'abord pour objet de répondre aux problèmes d'authentification pour des accès distants, par liaison téléphonique, vers les réseaux des fournisseurs d'accès ou des entreprises. C'est de la qu'il tien son nom qui signifie Remote Access Dial In User Service. Au fil du temps, il a été enrichi et on peut envisager aujourd'hui de l'utiliser pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil.

Le présent rapport est composé de quatre chapitres : Le premier chapitre est une introduction aux réseaux informatiques, nous allons exposer brièvement quelques notions théoriques utiles pour une compréhension des éléments servant à résoudre notre problématique, le deuxième chapitre donne une idée générale de l'environnement dans lequel notre stage s'est déroulé (APC BEJAIA, service d'Etat Civil) et cerner les problèmes rencontrés au niveau du réseau local, le troisième chapitre est consacré à l'installation du serveur RADIUS, alors que le quatrième est le Déploiement de la solution d'authentification RADIUS simulée avec Packet Tracert, ainsi qu'un test pour validation de la configuration globale utilisé pour une optimisation des processus de sécurisation de l'ensemble des réseaux locaux.

Chapitre I :
Introduction à la sécurité des réseaux informatiques

1 Introduction

Les réseaux informatiques sont nés d'un besoin d'échanger des informations de manière simple, sécurisée et rapide entre les machines.

Au cours de ce chapitre, nous abordons principalement les différentes caractéristiques liées à la sécurité des réseaux informatiques. Nous allons définir en premier temps les notions de bases sur les réseaux informatiques tels que leurs types, leurs architectures, les différentes topologies, ensuite nous donnons un aperçu sur les différentes couches du modèle OSI et TCP/IP, nous citons aussi les protocoles de communication amenés à faire le routage des données entre les réseaux. Puis nous passons à la sécurité informatique où nous allons définir les différentes attaques et les moyens mis à la disposition pour sécuriser les données informatiques.

2 Généralité sur les réseaux informatiques

2.1 Définition

Un **réseau informatique** est un ensemble d'ordinateurs reliés entre eux qui échangent des informations et des services. Un réseau peut aussi contenir des équipements spécialisés (Hubs, routeurs, et bien d'autres équipements) interconnectés entre eux.

Un réseau informatique peut servir [W1] :

- **Pour les entreprises et organisations :**
  - Partage des ressources (programmes, matériels, données)
  - Fiabilité/résistance aux pannes (duplication des données, cloud)
  - Outil de communication (messagerie électronique, travail collaboratif)
  - Commandes de fournitures en temps réel...
- **Pour les particuliers :**
  - Accès à l'information partagée (www)
  - Communication (email, messagerie instantanée, forums, blogs, etc.)
  - Jeux en réseau
  - Commerce en ligne...

2.2 Principe de fonctionnement

Dans la pratique, les ordinateurs ne sont pas directement reliés entre eux. Ils sont d'abord interconnectés au sein d'une entreprise, d'un lycée, d'un hôpital, d'un appartement formant ainsi une multitude de réseaux. Puis une machine par réseau (bien souvent un

routeur) est chargée de s'interconnecter aux autres sous réseaux. Enfin, on obtient une interconnexion complète de tous les réseaux et sous réseaux.

Il existe plusieurs types de réseaux qui peuvent être classés selon plusieurs critères.

2.3 Classification des réseaux

Les réseaux informatiques peuvent être divisés en plusieurs types : selon leurs étendues, leurs architectures et leurs topologies [W1].

2.3.1 Classification selon l'étendue géographique

a) WAN (Wide Area Network) :

Les réseaux étendus appelés WAN (Wide Area Network) sont destinés, comme le nom l'indique, à transporter des données numériques sur des distances à l'échelle d'un pays, d'un continent. Ce sont, par exemple, les réseaux des fournisseurs d'accès internet (Free, Orange, SFR...), de grandes sociétés...

Le réseau WAN est soit terrestre en utilisant des infrastructures au niveau du sol, soit par liaison satellite [W1].

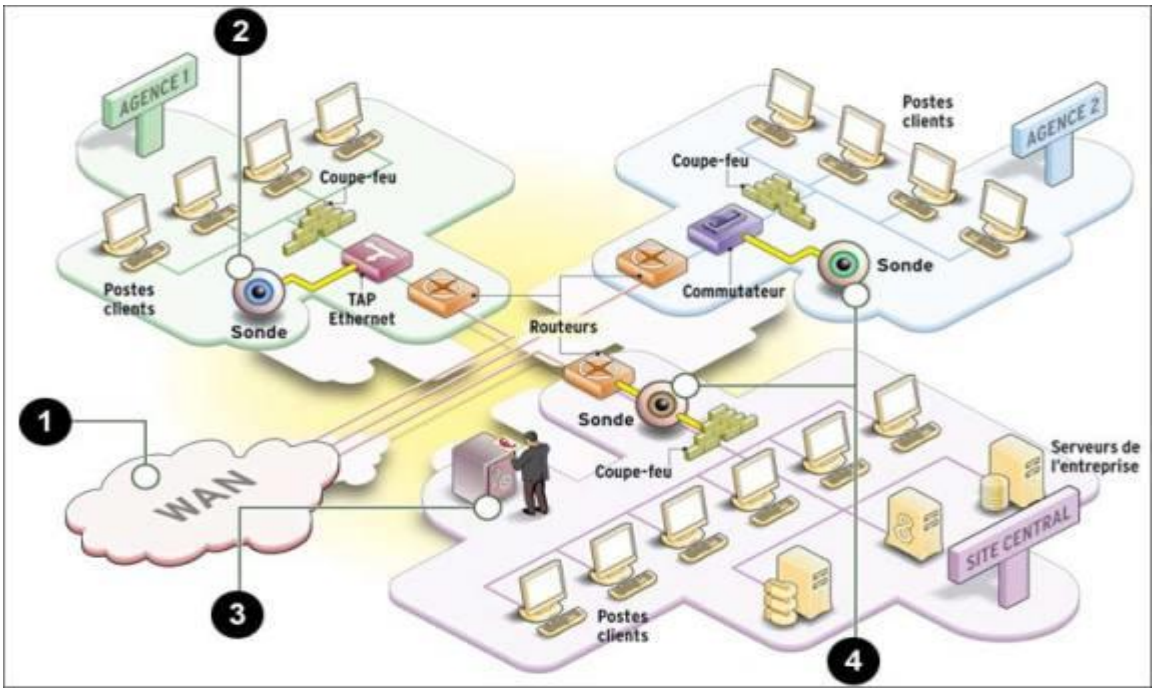

Figure I. 1: WAN

b) MAN (Metropolitan Area Network) :

Les MAN (réseaux métropolitains) interconnectent plusieurs réseaux locaux LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Ainsi, un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Ces réseaux MAN peuvent être publics ou privés. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [W1].

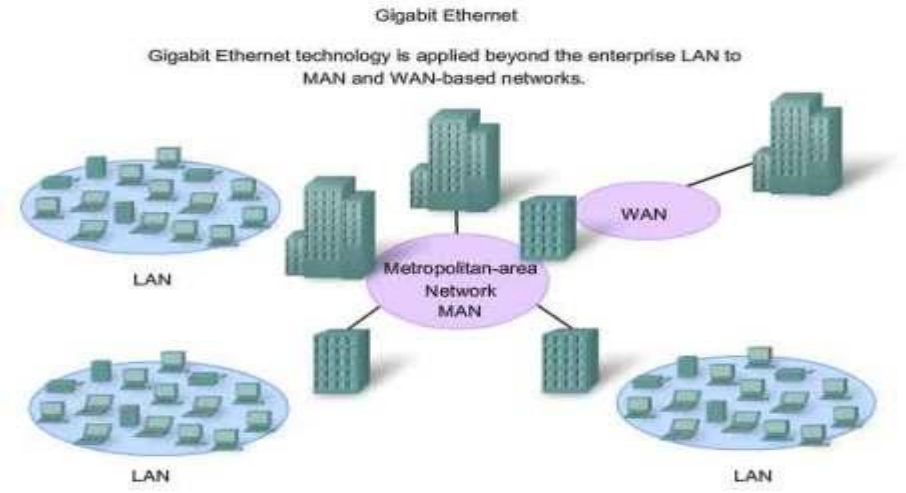

Figure I. 2: MAN

c) LAN (Local Area Network) :

Les réseaux locaux, appelés LAN (Local Area Network) sont constitués des moyens de communication internes à un établissement, une entreprise, donc entièrement maîtrisés et privés. La zone servie peut être un simple bâtiment, un complexe de bâtiments ou un campus.

C'est un système de communication de données limité à une zone géographique restreinte et utilisant des débits de l'ordre de quelques Mbits/s jusqu'au Gigabits/s.

Le réseau n'emploie pas les circuits des opérateurs publics, mais peut contenir des passerelles ou des ponts vers d'autres réseaux comme Internet par exemple [W1].

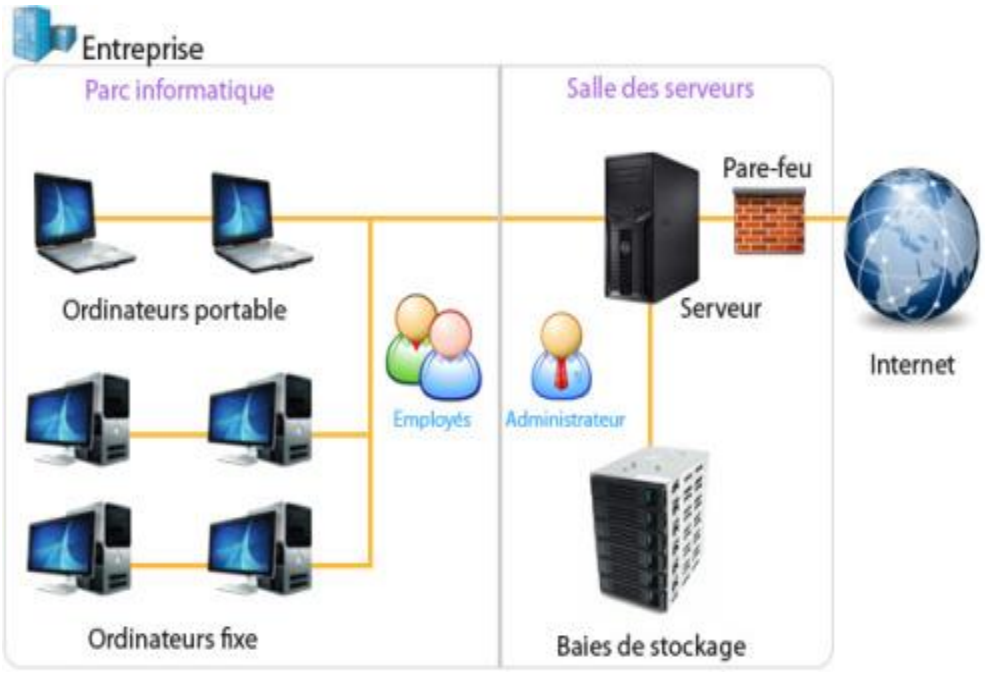

Figure I. 3: LAN

d) PAN (Personal Area Network)

Un **réseau personnel** ou (*Personal Area Network*, **PAN**) désigne un type de réseau informatique restreint en matière d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour ce type de réseau sont : réseau domestique ou réseau individuel [W1].

2.3.2 Classification selon l'architecture

On distingue deux catégories de réseaux LAN [W1] :

- Réseaux poste à poste
- Réseaux avec serveur dédié

a) Réseaux LAN poste à poste ou égal à égal (peer to peer)

Chaque poste ou station fait office de client et de serveur. Les données ne sont pas centralisées.

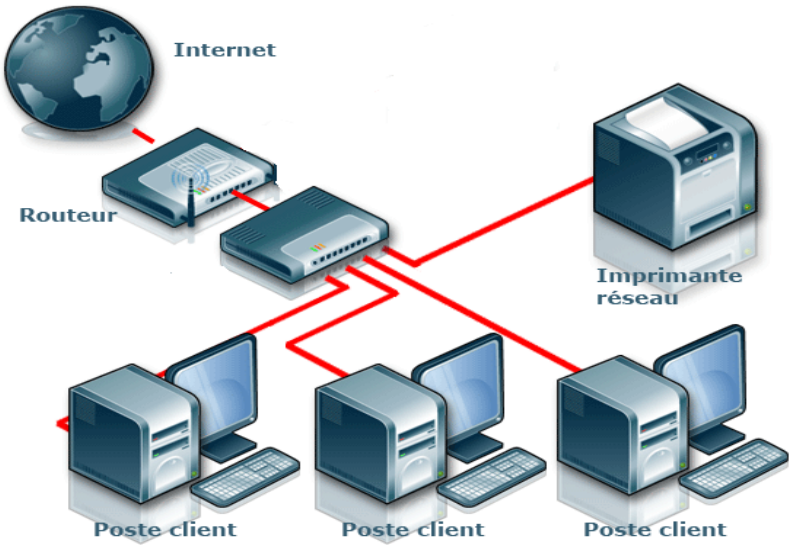

Figure I. 4: LAN Peer to Peer

L'avantage majeur d'une telle installation est son faible coût en matériel (postes de travail, cartes réseau, Switch, câbles).

En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer.

b) Réseaux LAN avec serveur dédié (client/serveur)

Il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises : le **serveur**.

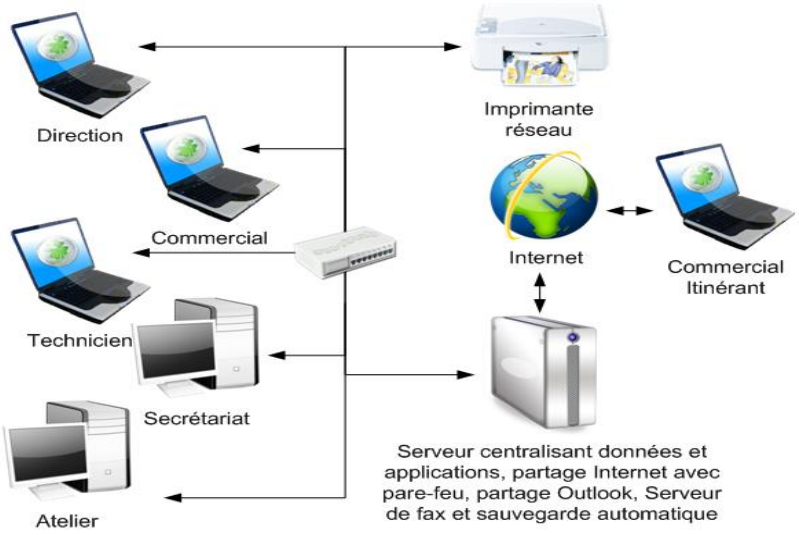

Figure I. 5: LAN Client/ Serveur

Le serveur centralise les données relatives au bon fonctionnement du réseau. Dans l'exemple précédant, c'est lui qui contient tous les mots de passe. Ainsi les comptes utilisateurs et mots de passe ne se trouvent plus qu'à un seul endroit, et il est donc plus facile pour l'administrateur du réseau de les modifier ou d'en créer d'autres.

L'avantage de ce type de réseau est la facilité de gestion d'un nombre important de postes.

Dans le jargon-réseau, un ensemble de ressources informatiques (matérielles ou logicielles) contrôlées par un serveur s'appelle un **domaine**.

2.3.3 Classification selon la topologie

La topologie du réseau et les emplacements relatifs de source et de destination des flux de trafic sur le réseau déterminent le chemin optimal pour chaque flux et la mesure dans laquelle des options redondantes de routage existent en cas de défaillance. Il existe deux manières pour définir un réseau : la topologie physique et la topologie logique (ou signal) [W2].

- **Topologie physique:** La topologie physique d'un réseau est la disposition des nœuds et des connexions physiques, y compris les câbles (Ethernet, DSL), les fibres optiques, etc. Il existe plusieurs topologies physiques, décrites ci-dessous [W2].

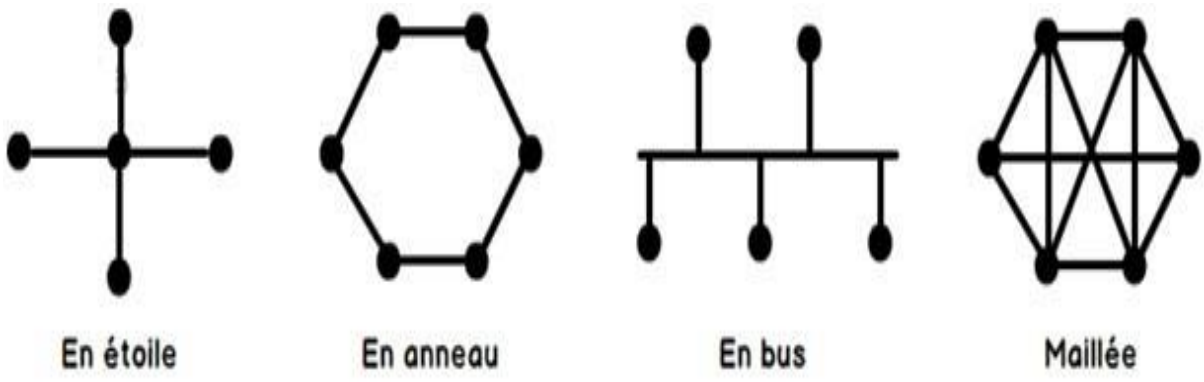

Figure I. 6: Topologies Physiques

- **Topologie logique:** Une topologie logique est un concept de réseau qui définit l'architecture de communication pour tous les nœuds d'un réseau. À l'aide d'équipements réseau tels que des routeurs et des commutateurs, la topologie logique d'un réseau peut être maintenue et reconfigurée de manière dynamique [W2].

- **Réseaux à transmission par diffusion:** Un seul canal est partagé par tous, et chaque message envoyé sur le réseau est reçu par toutes les stations. Le message possède un champ adresse de destination, et la station possédant cette adresse accepte le message [W1].
- **Réseaux à transmission point à point :** Ce mode de transmission réseau est constitué de lignes de transfert et de nœuds. Chaque ligne connecte deux nœuds. Dans ce mode de transmission, le support physique ne relie qu'une paire de stations seulement. Pour que deux stations communiquent, elles passent obligatoirement par un intermédiaire (le nœud)[W1].

La topologie logique définit le mode de transfert des données. Tandis que la topologie physique consiste à définir des périphériques réseau et du câblage [W2].

2.4 Modèle de référence OSI

Open Systems Interconnection (OSI) est un modèle de référence sur la façon de communiquer sur un réseau. Un modèle de référence est un modèle conceptuel pour comprendre les relations. Son objectif est l'interopérabilité de divers systèmes de communication avec des protocoles standards.

Le modèle (OSI) permettant d'implémenter des protocoles en sept couches. En fait, ce n'est même pas réel. Le modèle OSI n'effectue aucune fonction dans le processus de mise en réseau. C'est un modèle conceptuel qui nous permet de mieux comprendre les interactions complexes qui se produisent [W2].

International Standards Organization (ISO) a crée le modèle OSI. Il décrit sept couches portant les noms de couche physique, liaison, réseau, transport, session, présentation et application. Les divers protocoles qui définissent le réseau et les communications sont donc répartis dans chaque couche, selon leur utilité. Il est d'usage de diviser ces sept couches en deux : les couches basses, qui se limitent à gérer des fonctionnalités de base, et les couches hautes, qui contiennent les protocoles plus élaborés.

Les *couches basses*, aussi appelées *couches matérielles*, s'occupent de tout ce qui a trait au bas-niveau, au matériel. Elles permettent d'envoyer un paquet de données sur un réseau et garantir que celui-ci arrive à destination. Elle est généralement prise en charge par le matériel et le système d'exploitation, mais pas du tout par les logiciels réseaux. Les couches basses sont donc des couches assez bas-niveau, peu abstraites. Les couches basses sont au nombre de trois. Pour résumer, ces trois couches s'occupent respectivement des liaisons « point à point » (entre deux ordinateurs/équipements réseaux), des réseaux locaux, et des réseaux Internet [W3].

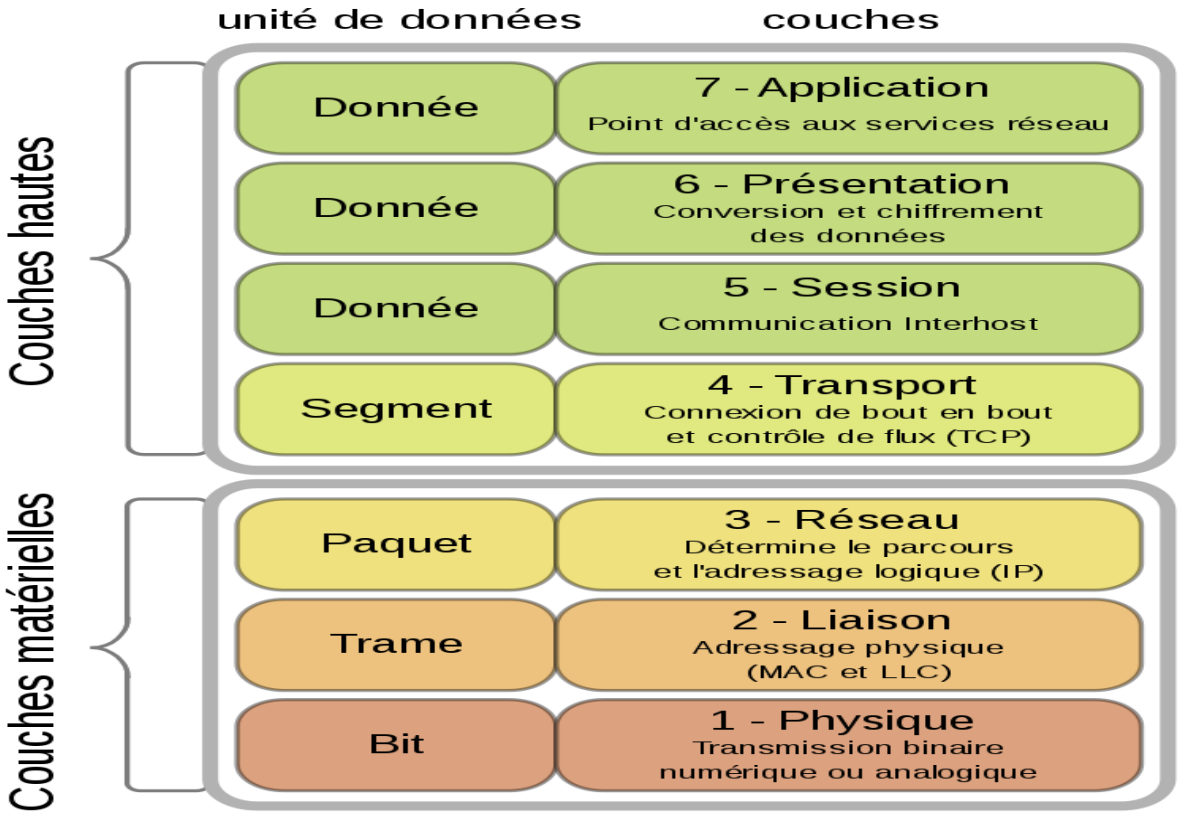

Figure I. 7: Modèle OSI

- La **couche physique** s'occupe de la transmission physique des bits entre deux équipements réseaux. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.
- La **couche liaison** s'occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend notamment en charge les protocoles MAC, ARP, et quelques autres.
- La **couche réseau** s'occupe de tout ce qui a trait à internet : l'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C'est notamment cette couche qui s'occupe du routage, à savoir la découverte d'un chemin de transmission entre récepteur et émetteur, chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche. Le protocole principal de cette couche est le protocole IP.

Les *couches hautes*, aussi appelées *couches logicielles*, contiennent des protocoles pour simplifier la programmation logicielle. Elles requièrent généralement que deux programmes

communiquent entre eux sur le réseau. Elles sont implémentées par des bibliothèques logicielles ou directement dans divers logiciels. Le système d'exploitation ne doit pas, en général, implémenter les protocoles des couches hautes. Elles sont au nombre de quatre :

- La **couche transport** permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP.
- La **couche session**, comme son nom l'indique, permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.
- La **couche présentation** se charge du codage des données à transmettre. Elle s'occupe notamment des conversions de boutisme ou d'alignement, mais aussi du chiffrement ou de la compression des données transmises.
- La **couche application** prend en charge tout le reste.

2.5 Modèle de protocole TCP/IP

Le modèle TCP/IP est plus simple qu'OSI, avec seulement quatre couches : liaison, Internet, transport et application. La différence avec OSI est simplement que certaines couches ont été fusionnées. La couche liaison de TCP/IP regroupe notamment les couches physiques et liaison d'OSI. De même, la couche application de TCP/IP regroupe les couches session, présentation et application d'OSI [W3].

- **La couche hôte réseau :** Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches : physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau [W4].

- **La couche internet :** Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI [W4].

- **La couche transport** : Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant [W4].

- La couche application : Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces deux couches, et finalement, le modèle OSI dépouillé de ces deux couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs [W4].

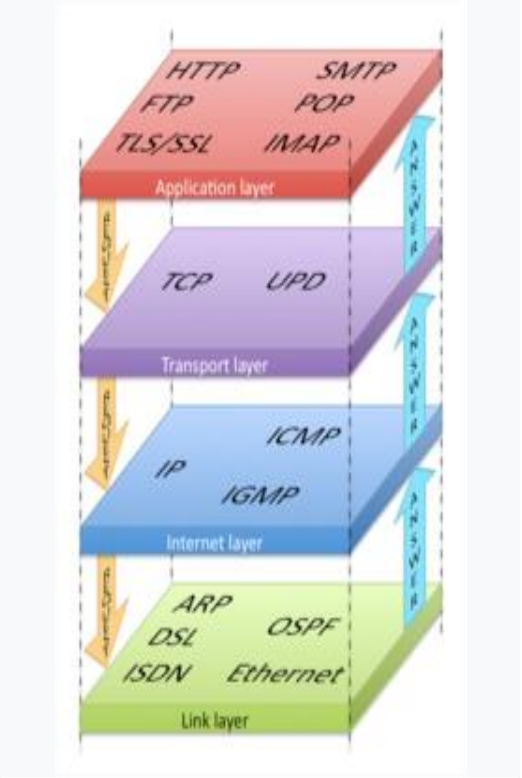

Figure I. 8: Internet Protocol Stack

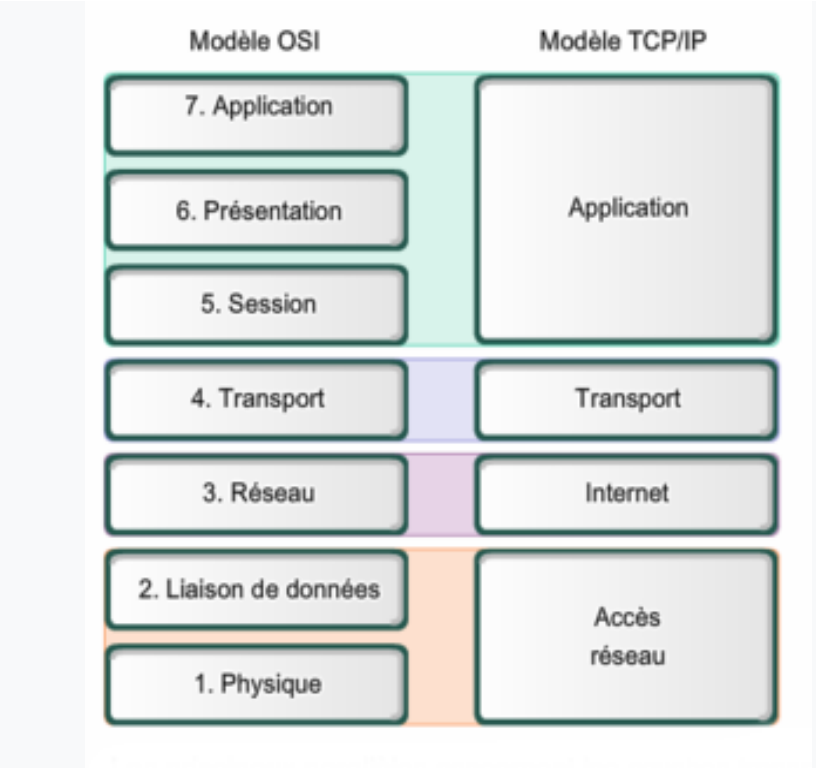

Figure I. 9: Comparaison des modèles OSI et TCP IP

2.6 Encapsulation des données

Les données ne sont pas transmises telles quelles sur le réseau, car chaque protocole a besoin d'informations bien précises pour faire son travail. Par exemple, les protocoles de couche liaison ont besoin d'informations particulières, non présentes dans la donnée transmise, pour détecter les erreurs ou indiquer le récepteur. Même chose pour les protocoles TCP et UDP de la couche transport, qui ont besoin d'informations sur le processus émetteur et récepteur, qui ne sont pas dans la donnée transmise. Et ce problème nous amène à parler de l'**encapsulation** [W3].

- **Les en-têtes des paquets**

Pour résoudre le problème précédent, chaque protocole ajoute les informations dont il a besoin à la donnée transmise. Ces informations sont regroupées dans un **en-tête**, placé au début des données à transmettre. Plus rarement, certains protocoles ajoutent leurs informations devant, mais aussi derrière la donnée à transmettre : l'en-tête est complété par un *pied* (le terme anglais est : *footer*). Lorsqu'un protocole prend en charge un paquet de données, il lui ajoute un en-tête à son début. Avec cette méthode, les en-têtes de chaque couche sont séparés, placés les uns à côté des autres. Lors de la réception, cet en-tête sera enlevé : les couches supérieures n'ont pas besoin des en-têtes des couches inférieures [W4].

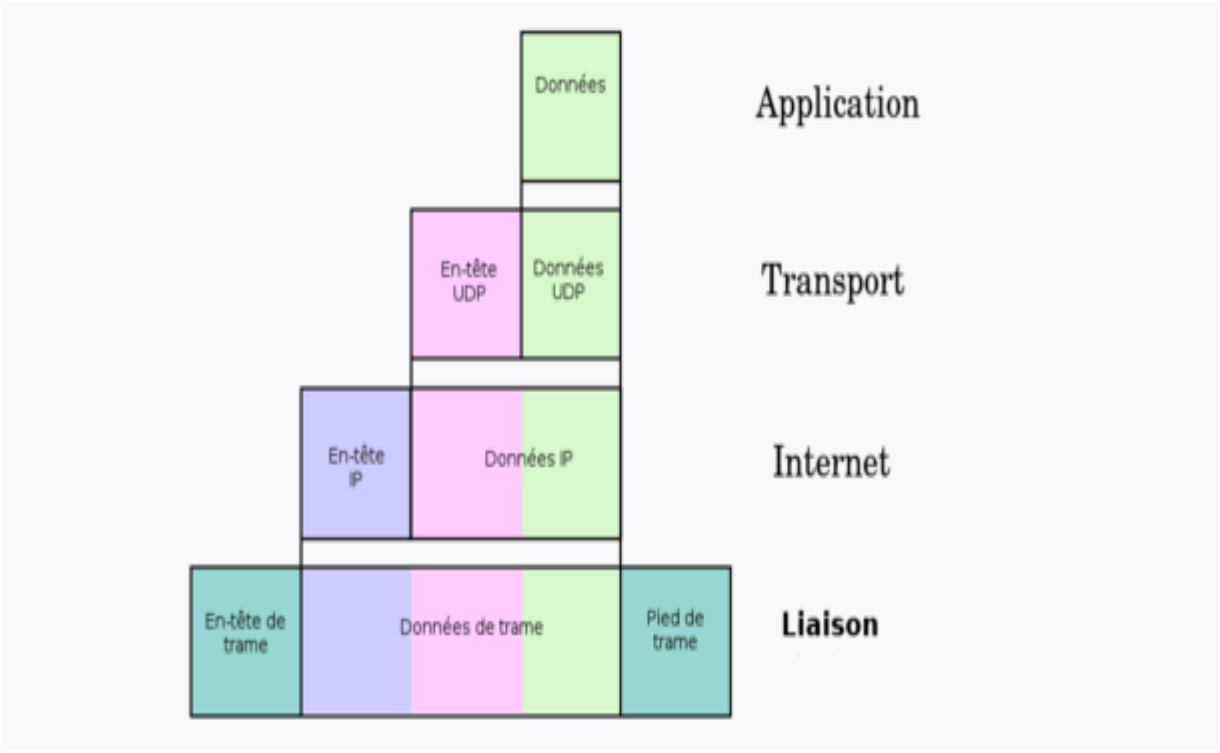

Figure I. 10: Illustration de l'encapsulation en fonction des couches TCP/IP

2.7 Routage IP

Parmi les fonctionnalités principales de la couche IP, on trouve le routage IP qui consiste à déterminer la manière d'acheminer les datagrammes IP à travers les différents réseaux d'un internet.
Chaque réseau se compose d'un ou de plusieurs machines, et est relié aux autres réseaux par des routeurs. La fonction du routeur est de transmettre les paquets IP d`un réseau à un autre selon un algorithme de routage prédéfini.
On peut distinguer deux types de routage [W5]:

- **Le routage direct :** Permet de transférer directement un datagramme d'une machine à une autre, et peut être utilisé par deux machines si elles sont reliées directement au même système de transmission physique (Ethernet).
- **Le routage indirect :** Permet de transmettre les datagrammes d'un réseau à un autre, ainsi il est nécessaire de déterminer vers quel routeur envoyer un datagramme IP en fonction de sa destination finale.

Dans le cas du routage indirect le choix du routeur vers lequel va être envoyé le datagramme IP se fait à l'aide des tables de routages. Ces tables contiennent les informations

relatives aux différentes destinations possibles et à la façon de les atteindre. Machines et routeurs possèdent tous des tables de routage.

D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (D, R) où D est l'adresse IP d'un réseau destination et R l'adresse IP du routeur suivant sur le chemin menant à cette destination. Tous les routeurs mentionnés dans une table de routage doivent bien sûr être directement accessibles à partir du routeur considéré. Cette technique, dans laquelle un routeur ne connaît pas le chemin complet menant à une destination, mais simplement la première étape de ce chemin, est appelée routage par sauts successifs (next-hop routing).

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du **routage statique** et du **routage dynamique** [W6].

a) **Routage statique :** Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau. Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux.
b) **Routage dynamique :** Le routage dynamique permet quant à lui de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre au routeur de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter.

	Routage statique	Routage dynamique
Mis en œuvre dans des	Petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les Routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonction du changement de topologie.
La construction de la table de routage	Les routes sont remplis à la main	Les routes sont remplies dynamiquement dans la table.
Algorithmes de routage	N'utilise pas d'algorithmes de routage complexes.	Utilise des algorithmes de routage complexes pour effectuer des opérations de routage.
Sécurité	Fournit une haute sécurité.	Moins sécurisé en raison de l'envoi de diffusions et de multidiffusions.
Échec du lien	L'échec de liaison bloque le routage.	L'échec de liaison n'affecte pas le routage.

Tableau I. 1: Table de comparaison entre le routage statique et le routage dynamique

2.8 Protocoles réseaux

Un **protocole réseau** est un protocole de communication mis en œuvre sur un réseau informatique ou un réseau de télécommunications.

Les protocoles réseau sont un ensemble de règles, de conventions et de structures de données qui dictent la manière dont les appareils échangent des données sur les réseaux. En d'autres termes, les protocoles réseau peuvent être assimilés à des langages que deux appareils doivent comprendre pour une communication transparente des informations, indépendamment de leur infrastructure et des disparités de conception.

Liste de quelques protocoles réseau	
Nom	**Fonction**
FTP	**FTP** (File Transfer Protocol) s'occupe des transferts de fichiers.
TELNET	**TELNET** Permet d'établir une connexion à un hôte distant et de gérer les données locales.
TCP	**TCP** (Transmission Control Protocole) s'assure que les connexions entre deux ordinateurs sont établies et maintenues.
IP	**IP** (Internet Protocol) gère les adresses logiques des nœuds (stations,…).
ARP	**ARP** (Adress Resolution Control) fait correspondre les adresses logiques (IP) avec les adresses physiques (MAC).
RIP	**RIP** (Routing Information Protocol) trouve la route la plus rapide entre deux ordinateurs.
OSPF	**OSPF** (Open Shortest Path First) est une amélioration de RIP, plus rapide et plus fiable.
ICMP	**ICMP** (Internet Control Message Protocol) gère les erreurs et envoie des messages d'erreurs.
BGP/EGP	**BGP/EGP** (Border Gateway Protocol / Exterior Gateway Protocol) gère la transmission des données entre les réseaux.
SNMP	**SNMP** (Simple Network Management Protocol) permet aux administrateurs réseaux de gérer les équipements de leur réseau.
PPP	**PPP** (Point to Point Protocol) permet d'établir une connexion distante par téléphone. PPP (après **SLIP**) est utilisé par les fournisseurs d'accès à Internet.
SMTP	**SMTP** (Simple Mail Transport Protocol) permet d'envoyer des courriers électroniques.
POP 3 & IMAP 4	**POP 3** (Post Office Protocol version 3) et **IMAP 4** (Internet Message Advertising Protocol version 4) permettent de se connecter à un serveur de messagerie et de récupérer son courrier électronique.
DNS	Domain Name System (ou système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine
HTTP	L'HyperText Transfer Protocol, est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, il permet l'échange de données de différents types
DHCP	Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau

Tableau I. 2: Liste de quelques protocoles réseau

3 Sécurité informatique

Parmi les informations qui circulent sur les réseaux, on trouve des informations qui ont un caractère confidentiel, ce qui fait que la sécurité des communications et des données est une préoccupation primordiale des utilisateurs et des entreprises, pour se protéger contre des utilisation frauduleuse de leurs données ou encore des intrusions malveillantes dans les systèmes informatiques. Par ailleurs, une multitude de virus se propagent à l'insu des utilisateurs dans les fichiers téléchargés. Les virus sont susceptibles de détruire des documents ou même de provoquer la perte totale des informations stockées dans les machines. La solution est de mettre en place des mécanismes de contrôle d'accès et des protocoles sécurisés qui apportent plusieurs services : l'authentification, la confidentialité, l'intégrité, la non-répudiation [W6].

3.1 Définition

La sécurité informatique recouvre l'ensemble de techniques informatiques permet tant de réduire au maximum les chances de fuites d'informations, de modification de données ou de détérioration des services. Elle consiste à un très grand nombre de méthodes, de technologies, d'architectures permettant d'atteindre un certain niveau de protection.

- C’est l’ensemble des moyens mis en œuvre pour réduire la vulnérabilité d’un système contre les menaces accidentelles ou intentionnelles.
- C’est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient [B1].

3.2 Objectifs et fonctions de la sécurité informatique

La notion de sécurité fait référence à la propriété d’un système, d’un service ou d’une entité. Elle s’exprime le plu souvent par les objectifs de sécurité suivants [B1]:

- **La disponibilité :** l’information sur le système doit être toujours disponible aux personnes autorisées.
  - Une ressource doit être accessible, avec un temps de réponse acceptable.
  - Un service doit aussi être assuré avec le minimum d'interruption en respect avec l'engagement établi.

Des pertes de données sont possibles si l'enregistrement et le stockage ne sont pas gérés correctement, d’où l’importance d’une haute disponibilité d’un système et de la mise en place d'une politique de sauvegarde.

- **L'intégrité :** permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.
    - L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.
- **La confidentialité :** est le maintien du secret des informations. Dans le cadre d'un système d'information, cela peut être vu comme une protection des données contre une divulgation non autorisée.
- **L'Authentification:** permet de vérifier l'identité d'un utilisateur sur une des bases suivantes:

    - Un élément d'information que l'utilisateur connaît (mot de passe, etc.)
    - Un élément que l'utilisateur possède (carte à puce, clé de stockage,certificat, etc.).
    - Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (empreinte digitale, ADN, etc.).

- **La non répudiation:** C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

3.3 Terminologie de la sécurité

La sécurité informatique utilise un ensemble de termes bien spécifique, que nous énumérons comme suit [B2] :

a) Sûreté : protection contre les actions non intentionnelles.

b) Sécurité : protection contre les actions intentionnelles malveillantes.

c) Menace : Événement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage à un système donné.

d) Vulnérabilité : Une vulnérabilité est une faiblesse dans le système qui peut être exploitée par une menace.

e) Risque : Association d'une menace aux vulnérabilités qui permettent sa réalisation.

f) Attaques : elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité.

g) Politiques de sécurité

- Définition des autorités et des ressources,
- Organisation, règles d'usage,
- Spécification des droits.

h) Mécanismes de sécurité : Moyens pour la mise en œuvre d'une politique. Parmi les moyens, on cite la protection physique, l'authentification par mot de passe, le chiffrement et les listes d'accès.

3.4 Anatomie d'une attaque

En général, chaque attaque obéit à un canevas constitué de 5 éléments « les 5 P » : Probe, Penetrate, Persist, Propagate, Paralyse [W8].

- **Probe :** C'est l'opération de la collecte d'information sur le système cible. Cette collecte peut se faire à l'aide d'outils déjà disponibles (ou gardés secrets).
- **Penetrate :** Une fois les informations collectées vient la phase de la pénétration du réseau. Nous détaillerons dans les prochains paragraphes les différents types d'attaques.
- **Persist :** Il s'agit de la création à l'intérieur du système pénétré d'un compte super utilisateur pour pouvoir s'y introduire une prochaine fois. Ou bien l'installation d'une application permettant le contrôle à distance. L'application installée devra être capable de subsister même après un redémarrage.
- **Propagate :** Il s'agit de l'étape d'observation du réseau pour déceler ce qui est accessible et ce qui est disponible.
- **Paralyse :** Il s'agit du coup de grâce qui peut s'exprimer, par exemple, par l'usage du serveur pénétré pour attaquer d'autres serveurs, ou tout simplement par la destruction de ses données et de son système d'exploitation.

Après ces cinq étapes, le pirate peut tenter d'effacer ses traces même si cela n'est pas complètement possible.

3.5 Types d'attaques

3.5.1 Attaques réseaux

Les attaques des réseaux informatiques se basent sur les failles liées aux protocoles ou à leurs implémentations. Ce qui suit, décrit les plus connues [W8].

- **Techniques de scan :** Le scan de port, comme vu de l'étape « probe » n'est pas vraiment une attaque. Mais, c'est plutôt un moyen pour déceler les ports ouverts et les services actifs. C'est la première étape d'une attaque et la meilleure technique de scan est celle qui est la plus furtive que possible afin de ne pas alerter les soupçons de la future victime.
- **IP Spoofing :** L'objectif de l'IP spoofing est l'usurpation de l'adresse IP d'une autre machine. Elle est utile dans le cas d'authentification par adresse IP. Elle se base sur le truquage des paquets IP. Cependant, en changeant son adresse IP, le pirate ne recevra pas de réponse de la machine distante puisque cette dernière sera envoyée au propriétaire réelle l'adresse IP usurpée. A moins de faire :
  - Une source routing : en plaçant à l'intérieur du paquet IP le chemin de routage. Cependant, les routeurs de nos jours n'acceptent plus cette option.
  - Un Reroutage : en envoyant au routeur des paquets de modification des tables de routage et ainsi les paquets de l'adresse usurpée seront envoyées vers un autre routeur. qui est contrôlé par le pirate et ainsi pouvant être reçus par ce dernier.
- **ARP Spoofing :** ARP Spoofing (ou ARP Redirect) consiste en la redirection du trafic d'une machine vers une autre. C'est la même finalité que l'IP spoofing mais on est actuellement au niveau de la couche de liaison. Elle se base sur la corruption du cache ARP. L'Address resolution protocol (ARP, protocole de résolution d'adresse) est un protocole effectuant l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI). Ainsi, la nouvelle trame ARP doit indiquer à la victime que l'adresse IP d'une autre machine est la sienne. Cependant, les caches ARP sont régulièrement vidés, donc il faut songer à maintenir l'usurpation.
- **DNS Spoofing :** L'objectif d'un DNS Spoofing est de fournir de fausses réponses aux requêtes DNS en indiquant une fausse adresse IP pour un nom de domaine. Les ordinateurs connectés à un réseau IP, comme Internet, possèdent une adresse IP qui, pour être plus facilement traitées par une machine, est représenté sous une forme numérique. Cependant, il n'est pas pratique d'apprendre toute une suite de chiffres numérique pour accéder à site web d'où le mécanisme DNS permettant l'association d'un nom (nom de domaine) à une adresse IP. Ainsi, l'opérateur au lieu de se connecter à l'adresse voulue, il se retrouve redirigé vers un site pirate (qui peut être l'image du site réel) où le pirate peut, par exemple, récupérer les identifiants de l'opérateur.

  Cette opération se déroule soit par :
  - DNS Cache Poisonning : les serveurs DNS dispose d'un cache qui permet de garder un certain temps la correspondance entre un nom de domaine et son adresse IP. L'objectif étant de corrompre ce cache.

- DNS ID Spoofing : lorsque nous introduisons un nom de domaine dans un navigateur, une requête est envoyée pour obtenir son adresse IP. Dans la trame de cette requête subsiste un numéro d'identification qui permet au client et au serveur de l'identifier. En récupérant cet identifiant (par un sniffer par exemple que nous verrons dans le quatrième chapitre), nous pouvons envoyer au client des réponses falsifiées avant que le serveur DNS ne lui réponde.

- **Fragments attacks :** L'objectif de cette attaque est de passer outre les protections des équipements de filtrage IP. Ainsi, une fois infiltré, le pirate peut effectuer d'autres attaques. Cela peut se faire par :
  - Fragments Overlapping : pour être transmis sur un réseau, le message est fragmenté en paquets. Chaque paquet dispose d'un offset permettant l'identification de sa position par rapport aux autres paquets de départ et permettant ainsi la reconstruction du message. Le but de l'attaque et de chevaucher les paquets en spécifiant des offsets incorrects. La plupart des filtres analysent les paquets d'une manière indépendante donc il ne détecte pas l'attaque. Ainsi, lors de la défragmentation, la demande de connexion est valide et l'attaque a lieu.
  - Tiny fragments : la demande de connexion est divisée en deux paquets. Le premier de taille minimum ne comprenant que l'adresse IP et le port de destination donc il outrepasse le filtre car il ne contient rien de suspect. Le deuxième paquet, quant à lui, contient la demande effective de connexion et du moment que la première partie est inoffensive alors certains filtres ne contrôlent pas la deuxième partie en jugeant qu'elle aussi va être inoffensive.

De nos jours, une grande partie des firewalls détectent et arrêtent ces attaques.

- **TCP Session Hijacking :** Le but de cette attaque est d'exploiter une session déjà ouverte par l'utilisateur. L'authentification ne se fait qu'à l'ouverture de la session. Ainsi, le pirate reste à l'écoute du réseau et une fois que l'utilisateur est authentifié, il désynchronise la session entre ce dernier et le serveur en construisant un paquet avec l'adresse IP source de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. De plus, ce paquet construit permet aussi d'injecter d'autres commandes dans cette session déjà ouverte.

3.5.2 Attaques applicatives

Les attaques informatiques applicatives peuvent être classifiées selon leur provenance. Leur origine peut être une faille dans un programme ou une erreur de configuration [W8].

- **Problèmes de configuration :**La majorité des utilisateurs se contentent des configurations par défaut de leurs programmes. Alors que ce n'est pas forcément la configuration la plus sécurisée. Ainsi, il faut toujours avoir le réflexe de bien lire la documentation des développeurs et consacrer le temps nécessaire dans la configuration.
- **Bugs :**Il s'agit de problèmes de programmation et de code source des logiciels. Ces derniers, peuvent être exploités pour une attaque. Le seul moyen pour y remédier et d'attendre le correctif du développeur ou de ne pas utiliser ce logiciel.
- **Buffers overflows :** Il s'agit d'un cas particulier des bugs où le développeur n'a pas instauré un système de contrôle de la taille des variables avant affectation. Ainsi, le pirate exploite cette faille pour copier dans une pile des données dont la taille est supérieure. Ce qui engendre un débordement et donc un dépassement de la pile (buffer overflows) qui peut causer la destruction du système cible.
- **Scripts :**Ils sont principalement web qui s'exécutent sur un serveur et renvoient le résultat au client. Des failles peuvent apparaitre si les entrées ne sont pas correctement contrôlées lors de leur saisie par un utilisateur.
- **Injections SQL :**Idem que les scripts, ils exploitent des paramètres d'entrée non vérifiés. La différence réside dans le fait qu'il s'agit d'un code SQL dans une requête de base de données.
- **Man in the middle :**C'est une attaque efficace qui consiste à placer la machine pirate au milieu (rôle de proxy) entre le client et le serveur. De ce fait, le pirate a accès à toutes les communications sans que le client ne s'en rende compte.

3.6 Logiciels malveillants

Un **logiciel malveillant** (en anglais, ***malware***) est un logiciel développé dans le but de nuire à un système informatique. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus. En revanche il en existe beaucoup d'autres [W9].

- **Virus :** Est Un virus est un programme capable de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». En plus de se reproduire, un virus peut effectuer d'autres actions qui peuvent être nuisibles à l'utilisateur de l'ordinateur infecté ou à d'autres utilisateurs reliés par réseau à l'ordinateur infecté. Les virus ne doivent pas être confondus avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer de programme hôte.
- **Ver (*worms*) :** Le ver est un programme qui se répand par courrier électronique en profitant des failles des logiciels de messagerie. Dès qu'un ver a infecté un ordinateur, il tente d'infecter d'autres ordinateurs en s'envoyant lui-même à des adresses contenues dans le carnet d'adresses de l'ordinateur infecté. Le plus souvent, le destinataire ne se

méfie pas du message, car il provient d'une personne connue. Certains vers, comme le I Love You, ont connu une expansion fulgurante.

- **Les chevaux de Troie (*Trojan horses*) :** Un cheval de Troie est un programme d'apparence légitime (souvent un petit jeu ou un utilitaire) qui comporte une routine nuisible exécutée sans l'autorisation de l'utilisateur. On confond souvent le cheval de Troie et la porte dérobée. Une porte dérobée se retrouve souvent dans certains chevaux de Troie, mais il existe des chevaux de Troie qui n'en contiennent pas. Un cheval de Troie n'est pas un virus, car il ne peut se reproduire et la capacité de reproduction est une caractéristique essentielle des virus.
- **Les portes dérobées (*backdoors*) :** Une porte dérobée est un accès secret à un logiciel qui permet à un pirate informatique de prendre le contrôle d'un logiciel à l'insu de l'utilisateur légitime du logiciel.
- **Les logiciels-espions (*spywares*) :** Un logiciel espion est un programme inclus dans un autre programme (le plus souvent un graticiel, un partagiciel ou un pilote de périphérique) qui s'installe discrètement sur l'ordinateur sans prévenir l'utilisateur, collecte des informations sur l'utilisation de l'ordinateur et envoie ces informations à un organisme tiers. Un logiciel qui collecte des informations sur l'utilisation d'un ordinateur n'est pas malveillant s'il informe l'utilisateur lors de son installation et s'il ne collecte aucune information dans le but de nuire à l'utilisateur.
- **Cookies :** Un cookie est en réalité un fichier stocké sur le disque dur de l'utilisateur, afin de permettre au serveur web de le reconnaître d'une page web à l'autre. Les cookies sont notamment utilisés par les sites de commerce électronique afin de conserver les préférences de l'utilisateur (par exemple les options qu'il a coché) afin de lui éviter de les ressaisir. Mais certain cookies sont utilisés par des personnes malintentionnées à des fins malicieuses.

4 Sécurité des réseaux

Les réseaux sont basés sur le principe de l'autoroute, tout le monde y a accès et c'est à chacun de se protéger. Pour que tout soit clair, l'administrateur doit prévoir une politique de sécurité précisant les droits d'accès, les services réseau disponibles, les précautions à prendre, les procédures à suivre lorsqu'une faille a été décelée dans la protection du réseau et des méthodes de restauration de données.

La protection des données et des applications dépend de leur niveau de confidentialité. La protection la plus sûr est l'isolation physique du réseau.

4.1 Quelques méthodes de protection

- **Antivirus :** logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire [B3].
- **Le pare-feu :** un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas) [B3].
- **Détection d'intrusion :** repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime.

Mauvaise détection : taux de faux positifs, faux négatifs [B3].

- **Contrôle d'accès :** l'objectif de cette stratégie est qu'aucune porte dérobée interne ne permet d'accéder au cœur du réseau. Pour contourner ce risque, il faut créer un contrôle d'accès à toutes les portes d'entrée du périmètre de sécurité. Ce contrôle sera sous la responsabilité du périmètre de sécurité qui déterminera la politique d'accès à mettre en œuvre. Pour y parvenir, il faut que tous les premiers éléments intelligents d'accès au réseau (commutateurs ou routeurs) fasse un contrôle d'accès. La politique AAA (*Authentication Authorization Accounting*) est particulièrement adaptée.

4.2 Principe de l'authentification

Un service d'authentification repose sur deux composantes :

➢ L'identification dont le rôle est de définir les identités des utilisateurs.

➢ L'authentification permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle d'authentification simple. Lorsque l'authentification nécessite plusieurs facteurs, on parle alors d'authentification forte.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

➢ Un élément d'information que l'utilisateur connaît (mot de passe, « passphrase », etc.) ;

➢ Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat) ;

➢ Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (fond de rétine, empreinte digitale, ADN, etc.).

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle Internet :

➢ Au niveau applicatif : HTTP, FTP

➢ Au niveau transport : SSL, SSH

➢ Au niveau réseau : IPSEC

➢ Au niveau transmission : PAP, CHAP

4.3 Protocoles d'authentification

a) Protocole PAP : Le protocole PAP (*Password Authentication Protocol*) est, comme son nom l'indique, un protocole d'authentification par mot de passe. Le protocole PAP a été originalement utilisé dans le cadre du protocole PPP.

Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé.

Ainsi, le protocole PAP n'est utilisé en pratique qu'à travers un réseau sécurisé.

b) Protocole CHAP : Le protocole CHAP (*Challenge Handshake Authentication Protocol*), défini par la RFC 1994 est un protocole d'authentification basé sur la résolution d'un défi (*challenge*), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée.

Les étapes du défi sont les suivantes :

➢ Un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi ;

➢ La machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau ;

➢ le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;

➢ Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

c) **Protocole MS-CHAP :** Microsoft a mis au point une version spécifique de CHAP, baptisée MS-CHAP (*Microsoft Challenge Handshake Authentication Protocol* version 1, noté parfois MS-CHAP-v1), améliorant globalement la sécurité.

En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle.

Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un *hash* intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.

Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire.

❑ **MS-CHAP-v2** : La version 2 du protocole MS-CHAP a été définie en janvier 2000 dans la RFC 2759. Cette nouvelle version du protocole définit une méthode dite « d'authentification mutuelle », permettant au serveur d'authentification et à la machine distante de vérifier leurs identités respectives. Le processus d'authentification mutuelle de MS-CHAP-v2 fonctionne de la manière suivante :

➢ Le serveur d'authentification envoie à l'utilisateur distant une demande de vérification composée d'un identifiant de session ainsi que d'une chaîne aléatoire.

➢ Le client distant répond avec :

• son nom d'utilisateur,

• un haché contenant la chaîne arbitraire fournie par le serveur d'authentification, l'identifiant de session ainsi que son mot de passe,

• une chaîne aléatoire.

➢ Le serveur d'authentification vérifie la réponse de l'utilisateur distant et renvoie à son tour les éléments suivants :

• la notification de succès ou d'échec de l'authentification,

• une réponse chiffrée sur la base de la chaîne aléatoire fournie par le client distant, la réponse chiffrée fournie et le mot de passe de l'utilisateur distant.

➢ Le client distant vérifie enfin à son tour la réponse et, en cas de réussite, établit la connexion.

Le protocole MS-CHAP-v2 a été cassé et des outils (*chapcrack*) de déchiffrement du mot de passe à partir d'écoute du réseau ont été rendus publics en 2012.

d) Protocole EAP : Le protocole EAP est une extension du protocole PPP, un protocole utilisé pour les connexions à Internet à distance (généralement via un modem RTC classique) et permettant notamment l'identification des utilisateurs sur le réseau. Contrairement à PPP, le protocole EAP permet d'utiliser différentes méthodes d'identification et son principe de fonctionnement rend très souple l'utilisation de différents systèmes d'authentification.

EAP possède plusieurs méthodes d'authentification, dont les plus connues sont : EAP-MD5 (*Message Digest 5*) ; EAP-PEAP ; EAP-TLS ; EAP-TTLS.

e) Protocole RADIUS : Le protocole RADIUS (*Remote Authentication Dial-In User Service*), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

5 Conclusion

Ce chapitre a été consacré à définir des notions de bases liées aux réseaux informatiques et leur sécurité, en particulier l'authentification (son principe, ses méthodes, et ses protocoles), le chapitre suivant va porter sur la présentation de l'organisme d'accueil et son infrastructure informatique.

Chapitre II :
Présentation de l'organisme d'accueil et problématique

1 Introduction

Dans ce chapitre, nous donnons un aperçu de la commune de Béjaia pour mieux comprendre sa structure et ses objectifs, nous étudions son système informatique (réseaux et applications existants). Ensuite, nous détaillant le réseau de l'Etat Civil.

2 Présentation de l'APC de Béjaia

La commune est la plus petite division organique du pays d'après la loi N°90/08 du 07 avril 1990 relative au code communal qui donne une très large définition à la commune dans son premier article « elle est la collectivité territoriale politique, administrative, économique, sociale et culturelle de base dotée de la personnalité morale et de l'autonomie financier, elle est orée par la loi », elle a un territoire, un nom et chef-lieu qui localité principale de la commune qui lui donne son nom.

La commune est administrée par une assemblée élue qui est l'assemblée populaire communale et un exécutif.

Elle est proche de la vie des citoyens, elle est ainsi le cadre naturel de leurs vie sociale et de leurs activités. C'est pourquoi elle doit satisfaire les besoins essentiels de ses habitants, comme elle doit notamment gérer les services obligatoires qui lui incombent : Etat Civil, sécurité, santé, enseignement, sport, etc.

Elle est associée très étroitement à la vie de l'état et au développement de la nation, dans ses domaines elle exerce un rôle très vaste de création de coordination d'orientation et de contrôle des activités économique implantées sur son territoire, elle est l'élément de base des unités administrative de la république.

3 Système informatique de l'APC de Béjaia

a) **Réseau WAN** : il s'agit d'un réseau haut débit de MICLAT (Ministère de l'intérieur, des collectivités locales et de l'aménagement du territoire).

- **Applications utilisées :**

Toutes les bases de données des applications utilisées par ce réseau sont centralisées au niveau du MICLAT.

Parmi les applications installées au sein de la commune de Béjaia pour le suivi et l'exploitation des données des différents programmes dédiés par les services centraux du ministre de l'intérieur et des collectivités locales et de l'aménagement du territoire, on trouve :

Description sur le logiciel / Application	Fonctionnalités
Solidarité Ramadan	Suivi l'opération de solidarité ramadan pour l'année en cours et la saisie des bénéficiaires
PARC AUTO	Recensement du Parc Automobile et Suivi de l'opération de la conversion au Gaz de pétrole liquéfié carburant (GPLc)
Evaluation-Projet-ZO	Système d'information de suivi de l'évolution des indicateurs socio économiques et des réalisations au niveau des zones d'ombre
Gestion EP	Gestion et réalisation de l'éclairage public
Primes Scolarité	Gestion de la distribution de la prime scolaire spéciale et la saisie des bénéficiaires
www.si-psase.dz	Système d'Information national relatif à la Préparation et le Suivi des Activités de la Saison Estivale
www.si-sbfcl.dz	Système d'Information de Suivi Budgétaire et Financier des Collectivités Locales
www.si-ssec.dz	Système d'Information national de Suivi de la situation Socio-Economiques des Collectivités Locales
www.si-ssep.dz	Système d'Information national du Suivi des Ecoles Primaires

Tableau II. 1: Applications MICLAT

b) Réseau MAN : il s'agit d'un réseau reliant les différentes quatorze annexes d'Etat Civil (Boukhiama, Tobal, Aissat Idir, Sidi Ouali, Sidi Ali Lebhar1, Sidi Ali Lebhar2, Sidi Ahmed,

Houm Rih, Taghzout, Ihaddaden 1000 logts, Ihaddaden 600 logts, Tizi, Tala Ouriane et Amtik N'tafath) par la fibre optique (quelques kilomètres).

c) Réseau local : il s'agit d'un réseau interne relié aux différents guichets et bureau par un ou plusieurs Switch.
Exemple : Réseau local de l'Etat Civil, Réseau local de la comptabilité.

4 Infrastructure informatique de l'Etat Civil

4.1 Architecture réseau

La figure 11 montre l'architecture réseau existante dans le service d'Etat Civil :

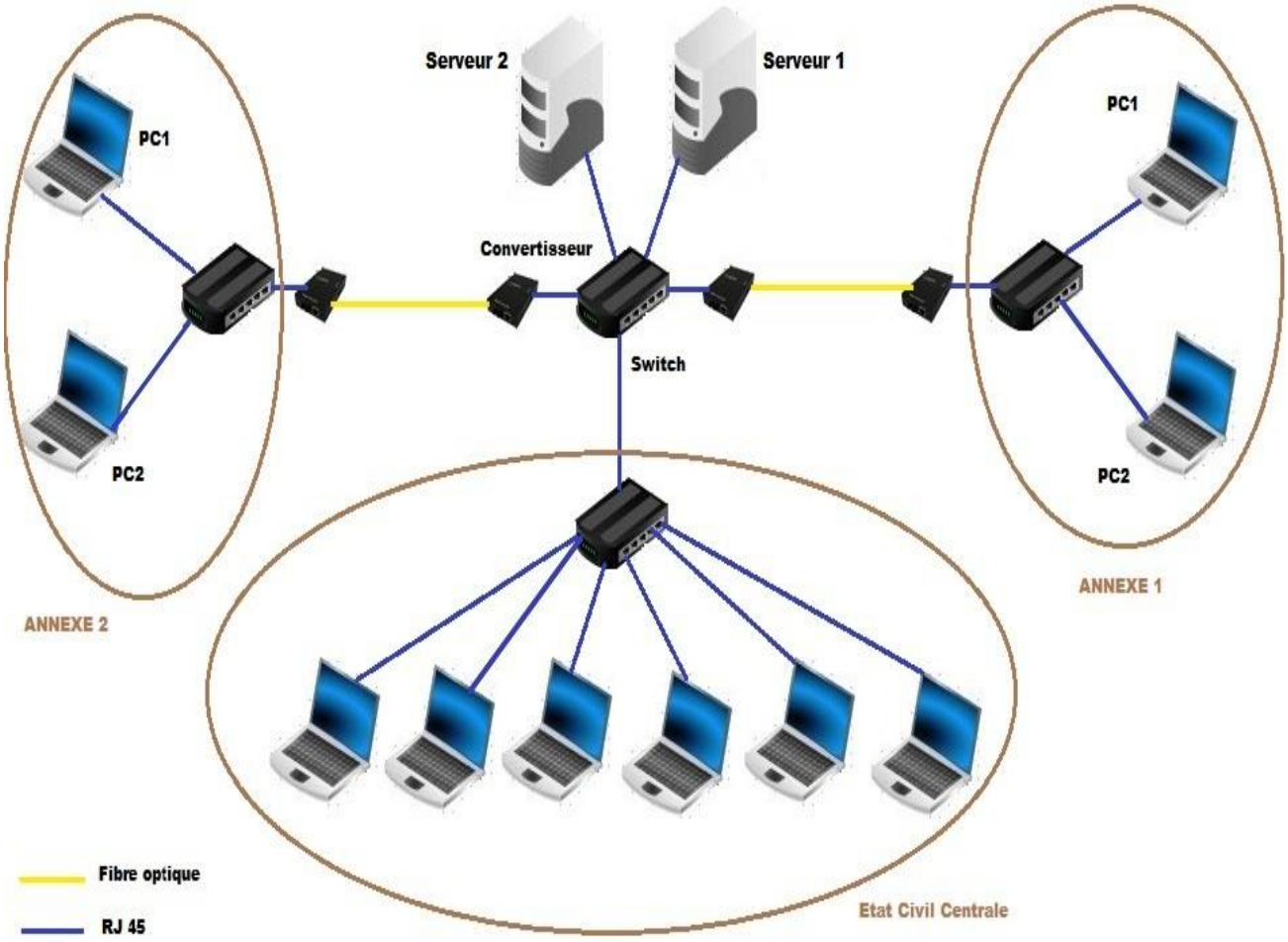

Figure II. 1: Architecture réseau de l'Etat Civil

4.2 Applications utilisées

Parmi les solutions existantes au niveau d'Etat Civil, nous citons quelques une (Tableau II.2) qui sont utilisées pour assurer le fonctionnement interne de l'administration locale.

Description sur le logiciel / Application	Fonctionnalités
Pool Naissance	Saisie des actes de naissance
Pool Mariage	Saisie des actes de mariage
Pool Décès	Saisie des actes de décès
Guichet Unique	Etablissement des actes (Naissance, Mariage, Décès, Jugement collectif, matrice)
Fiche Familiale	Etablissement des fiches familiales
Mariage Divorce	Etablissement des avis de mention (mariage, divorce)
Impression12S	Etablissement des actes de naissance 12 spéciale pour le passeport
GEC (gestion d'Etat Civil)	Saisie et établissement des actes (Naissance, Mariage, Décès) en langue étrangère (Français)
Fiche Familiale	Saisie et Etablissement des fiches familiales en langue française
Attestation d'Hébergement	Etablissement des attestations d'hébergement
Célibat	Etablissement des attestations (Non Mariage, Non Divorce, Non Remariage) en langue française

Tableau II. 2: Application d'Etat Civil

4.3 Equipements réseaux utilisés

Pour rappel, le réseau est un ensemble de machines interconnectées entre elles de pouvoir échanger des données.

Le réseau possède trois types de composants physiques :

- **les périphériques de terminaison :** qui sont les machines en bout de chaîne comme les ordinateurs, les imprimantes, les scanneurs ou les serveurs
- **les équipements intermédiaires :** dont le rôle est interconnecté les périphériques de terminaison entre eux sur le réseau, on parle par exemple des switchs ou des routeurs

- **le support :** qui transporte les données sur le réseau, il s'agit des câbles qui vont transmettre les signaux électriques (paire torsadé) ou la fibre optique qui va propager des ondes lumineuses.

- pour qu'il y est une bonne gestion de câblage, les éléments de réseaux informatique sont centralisés dans une armoire technique appelée une **baie de brassage** ou **armoire de brassage** ou **armoire réseau**.

- Les câbles de fibre optique sortant reliée à une armoire appelée **armoire optique**.

5 Problématique

Dans une grande commune, telle que Béjaia qui dispose d'un réseau commuté de taille importante composé d'une plateforme reliant les différentes annexes (précédemment citées) au serveur de l'état civil centralisé à l'unité principale sise à L'EKHMIS.

En effet l'administrateur réseau trouve beaucoup de difficultés dans la gestion du réseau, notamment la gestion des postes de travail ainsi que le temps considérable passé durant les déplacements quotidiens pour régler manuellement des problèmes qui peuvent êtres gérés à distance. Ajouter à ça la vulnérabilité du système qui ne dispose pas d'un mécanisme d'authentification interne convenable, ce qui le rend accessible sans aucun contrôle

Cet état de fait est du a la méthode de travail adoptée, pour mener à bien cette mission et qui se base principalement sur un mode de gestion entièrement manuelle.

6 Solutions proposées

Notre objectif est de mettre en place un système d'authentification permettant de résoudre les problèmes constatés à l'Etat Civil, tels que :

- La gestion des postes des utilisateurs
- La gestion des données et des périphériques du réseau
- La gestion des droits d'accès

Pour répondre aux besoins cités ci-dessus nous avons optés pour une technique d'authentification RADIUS, qui associés un compte pour chaque utilisateur du réseau. Cette solution permet aux utilisateurs de se connecter au serveur avec des droits d'accès différents.

La figure ci-dessous représente le schéma fonctionnel de notre solution d'authentification.

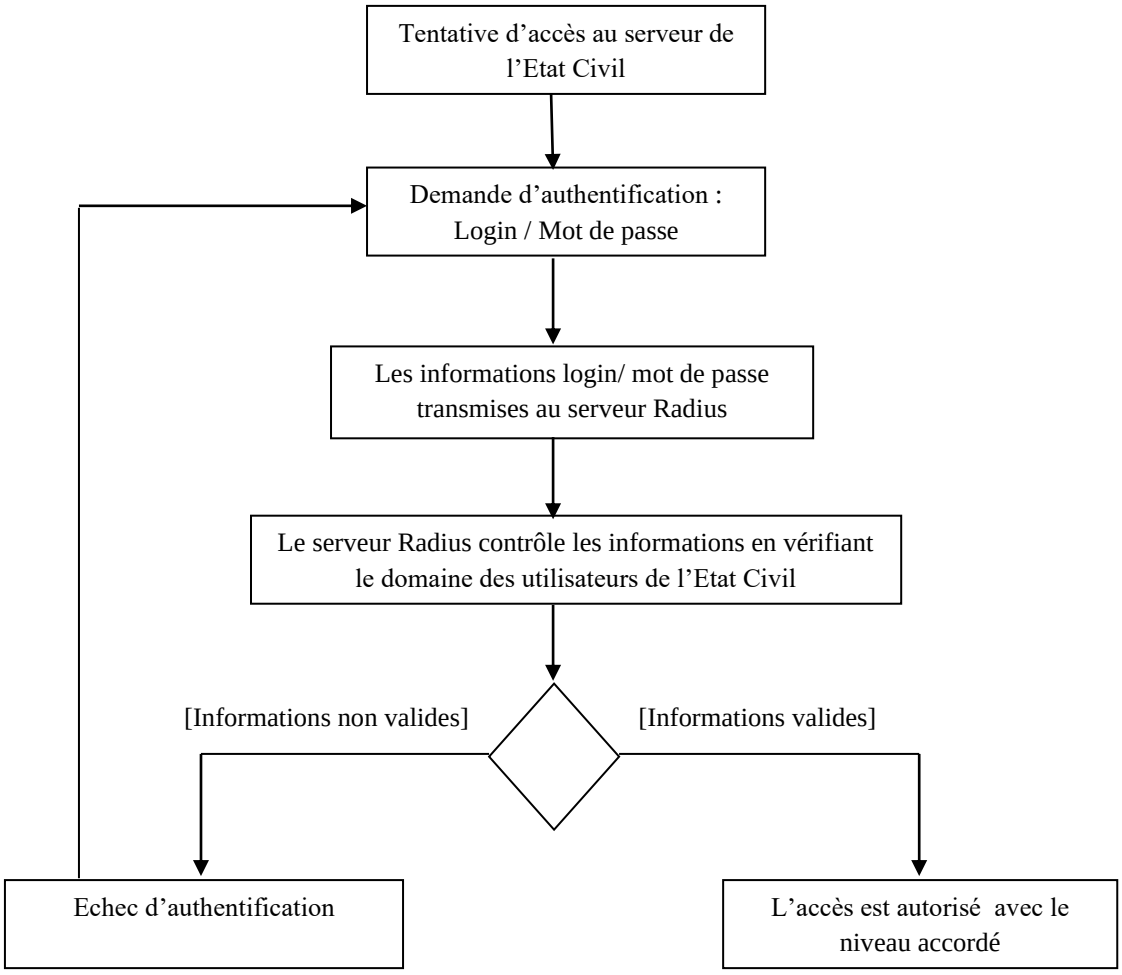

Figure II. 2: Schéma fonctionnel de la solution proposée

7 Conclusion

Ce chapitre nous a permis d'étudier l'architecture réseau de l'organisme d'accueil et les équipements existants. Apres avoir fait l'analyse du réseau de l'APC (réseau d'Etat Civil), nous avons soulevé plusieurs faiblesses réseaux existantes, ce qui nous a permis de cerner la problématique de notre projet et proposer une solution que nous allons mettre en œuvre dans le chapitre suivant.

Chapitre III :
Installation du serveur RADIUS

1 Introduction

Dans ce chapitre, nous allons présenter la mise en place notre solution réseau, qui consiste à la configuration d'un serveur RADIUS sous Windows server 2012 R2. Cette solution nécessite d'avoir la configuration d'un annuaire Active Directory et un serveur de stratégie réseau NPS **(**Network Policy server).

Dans un premier lieu, nous allons présenter les services nécessaires pour la mise en place de la solution d'authentification AAA, en suite, dans un deuxième lieu, les étapes d'installation de cette solution.

2 Services de base de la solution AAA

2.1 Windows server 2012 R2

Windows server est un logiciel proposé par Microsoft pour résoudre les problèmes des entreprises, il permet de créer des solutions plus simples à planifier afin d'enrichir l'expérience utilisateur et l'administration des serveurs composant l'infrastructure de l'entreprise.

2.2 Active Directory

Est un service d'annuaire créé par Microsoft en 1996 et destiné à être installé sur les Windows Server 2000, 2003, 2008, 2012 et 2016. En stockant dans une base de données les renseignements relatifs aux ressources réseau d'un domaine, **Active Directory** a pour objectif premier de centraliser l'identification et l'authentification d'un réseau de postes Windows. Ses fonctions additionnelles permettent aux administrateurs de gérer efficacement une stratégie de groupe, ainsi que l'installation des logiciels et des mises à jour sur les stations du réseau.

2.3 Network Policy server

NPS est l'implémentation Microsoft de la norme RADIUS spécifiée par internet Engineering Task Force (IETF) dans les RFCs 2865 et 2866. En tant que serveur RADIUS, NPS effectue l'authentification, l'autorisation et la comptabilité centralisées pour de nombreux types d'accès réseau, notamment le commutateur sans fil, l'authentification, l'accès à distance de réseau privé virtuel et les connexions de routeur à routeur.

2.4 Fonctionnement d'un RADIUS

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.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire AD DS, etc.) et un client RADIUS, appelé NAS (*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré et authentifié grâce à un secret partagé.

Le fonctionnement de RADIUS suit le scénario ci-après :

➢ 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 scénario 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 quatre réponses suivantes :

• ACCEPT : l'identification est réussi ;

• REJECT : l'identification a échoué ;

• CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un défi (*challenge*) ;

• CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

À la suite de cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Ces étapes sont décrites dans la Figure III.1.

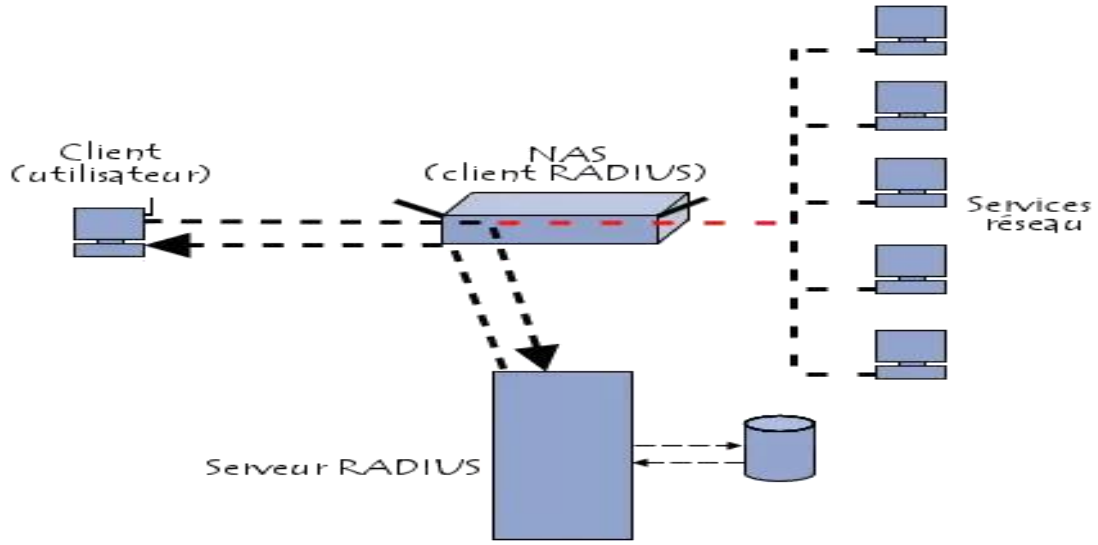

Figure III. 1: Fonctionnement RADIUS

3 Etapes d'installation du serveur RADIUS (Windows server 2012 R2)

Etape 1 : Installation de l'Active Directory

Le service de domaine ***Active Directory*** est un annuaire qui va centraliser des informations du réseau comme par exemple les comptes utilisateurs. Il permet aux administrateurs de gérer ces informations de manière sécurisée. De par sa centralisation, ***Active Directory*** est également un outil d'administration puissant et flexible [W10].

- Avant tout, on doit attribuer une configuration IP fixe sur le serveur. Nous allons commencer par installer le rôle qui va nous permettre d'avoir un domaine ***Active Directory.*** Pour cela, allons dans le gestionnaire de serveur et en haut à droite cliquons sur « ***Gérer*** » et cliquons sur ***« Ajouter des rôles et fonctionnalités ».***
- Sur la première fenêtre laisser coché « ***Installation basée sur un rôle ou une fonctionnalité*** » et cliquer sur ***« Suivant »***.
- Sur la fenêtre suivante ***« Sélection du serveur »***, laisser par défaut et cliquer à nouveau sur ***« Suivant »***. Nous allons arriver sur la fenêtre ci-dessous, sélectionner le rôle ***« Service AD DS ».***
- La fenêtre suivante va s'afficher, cliquer sur ***« Ajouter des fonctionnalités »***. Puis sur ***« Suivant »***.
- Sur la page des fonctionnalités ne rien cocher et cliquer à nouveau sur ***« Suivant »***. Nous allons ensuite arriver sur la page de présentation de l'***Active Directory***, cliquer encore sur ***« Suivant »***. La fenêtre ci-dessous va s'afficher. Cocher la case

« ***Redémarrer automatiquement le serveur de destination, si nécessaire*** » et cliquer sur ***« Installer »***.

L'installation se lance, une fois terminée nous allons pouvoir effectuer la configuration.

Toutes ces étapes sont illustrées dans la figure III.2.

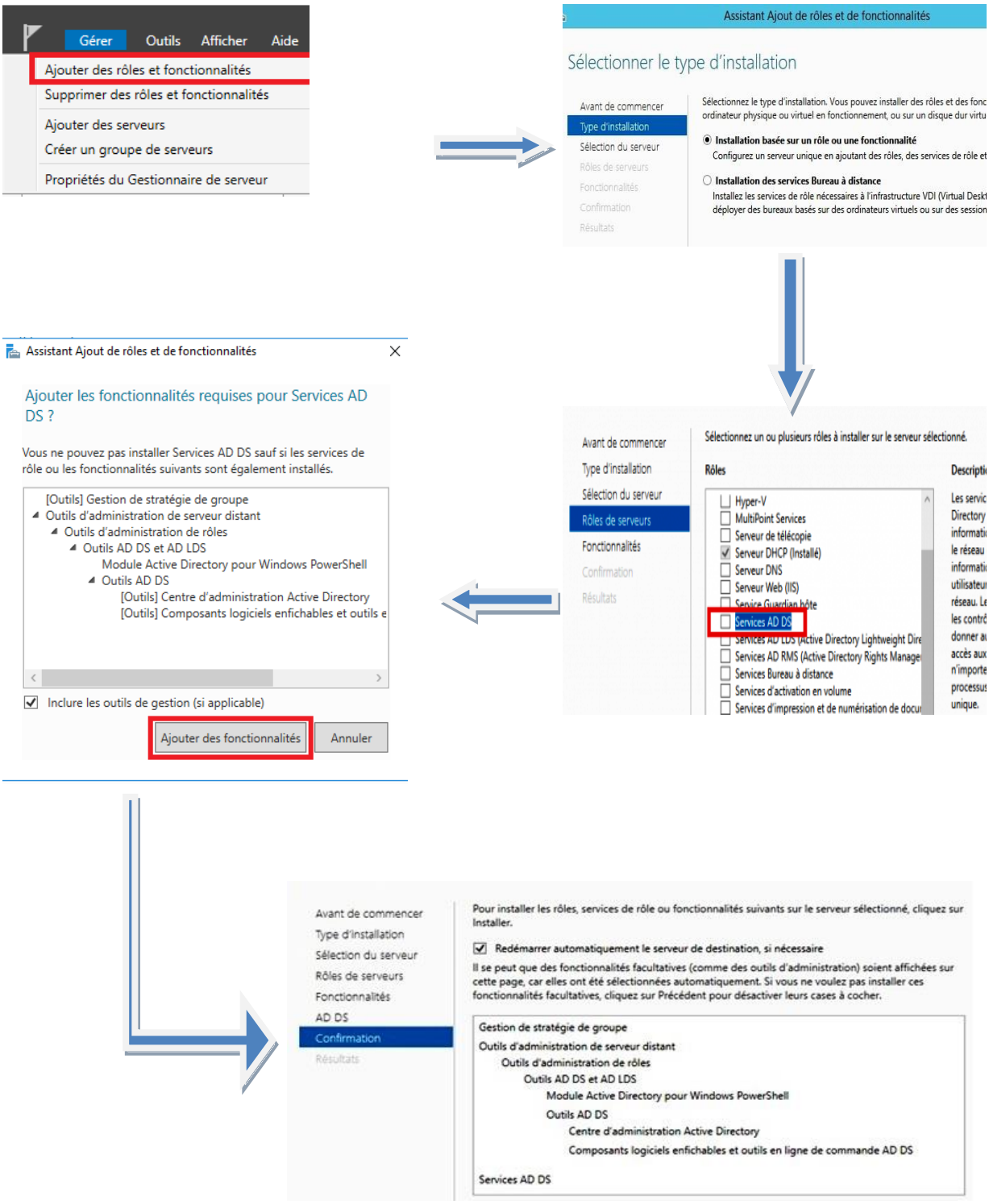

Figure III. 2: Installation de l'Active Directory

- Nous allons commencer la configuration de l'***Active Directory***. On remarque une alerte à coté du drapeau en haut à droite dans le gestionnaire du serveur. On Clique dessus et on sélectionne ***« Promouvoir ce serveur en contrôleur de domaine ».***

- Sur la fenêtre d'après, sélectionner « ***Ajouter une nouvelle forêt*** » et renseigner le nom du domaine. Cliquer sur ***« Suivant »***.

- Sur la fenêtre suivante, pour le niveau fonctionnel de la forêt et du domaine on laisse ***Windows Server 2012.*** Laisser ***« Serveur DNS »*** et ***« Catalogue global »*** cochés, ils sont nécessaires au fonctionnement de l'***Active Directory***. Enfin, on saisit le mot de passe du mode de restauration des services d'annuaire. On garde bien celui-ci en tête il pourra nous être utile en cas de dysfonctionnement sur notre domaine. Cliquer sur ***« Suivant »***.

- Sur la fenêtre suivante ***« Options DNS »***, on peut avoir une alerte mais c'est normal étant donné que c'est le premier serveur ***DNS***, cliquer sur ***« Suivant »***.

  Pour le nom ***NetBios***, on laisse par défaut et cliquer à nouveau sur ***« Suivant »***.

  Pour les chemins d'accès laisser aussi par défaut et cliquer sur ***« Suivant »***.

  On arrive ensuite sur la fenêtre récapitulative des options. Là encore on clique sur ***« Suivant »***.

  La fenêtre de vérification de la configuration apparaît. Cliquer sur ***« Installer »***, le serveur va redémarrer à la suite de l'installation.

  L'ensemble de ces étapes sont résumées dans la figure III.3.

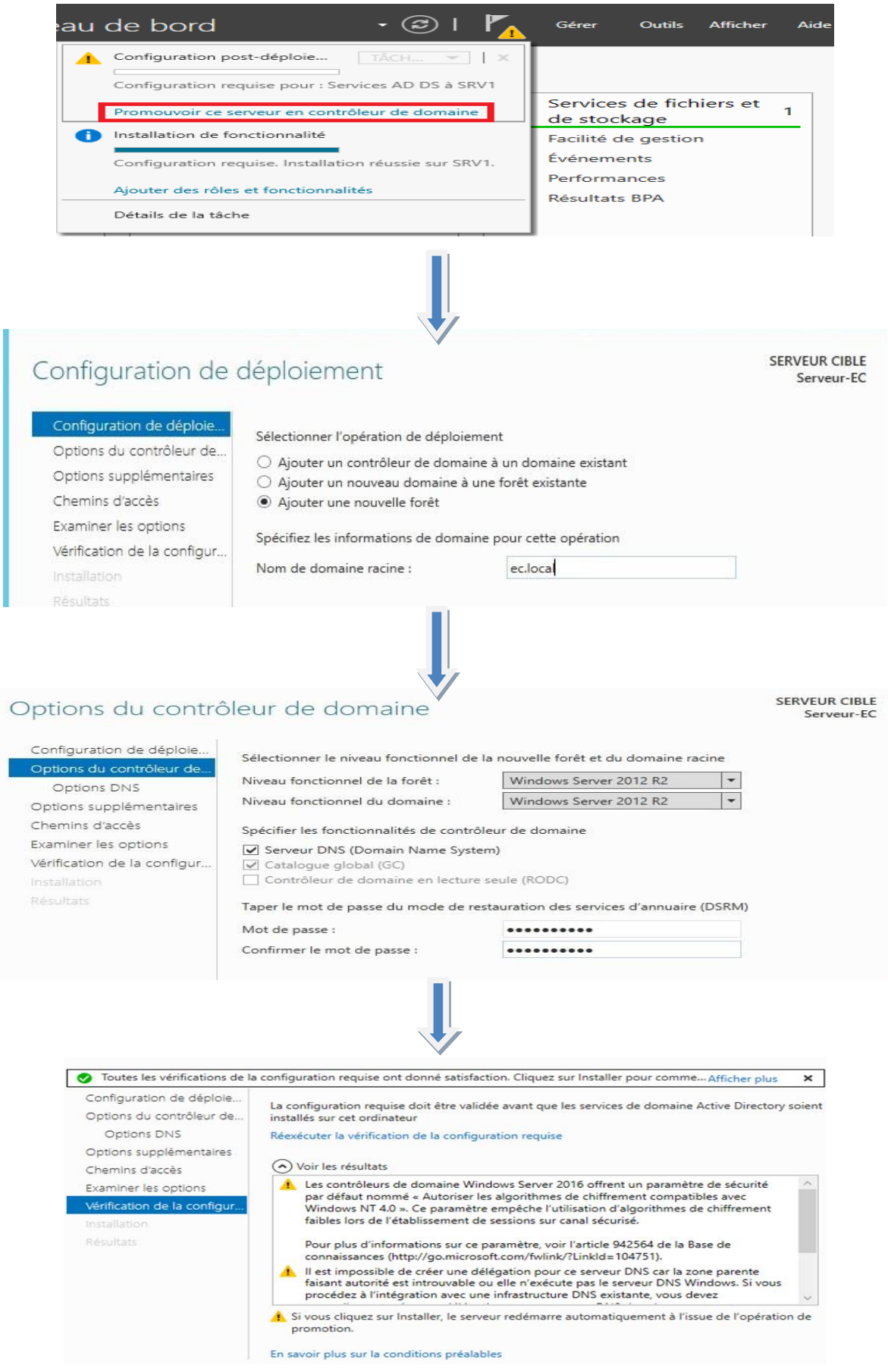

Figure III. 3: Configuration de l'Active Directory

Une fois redémarré, on a désormais notre domaine ***Active directory***. Le contenu avant le \ est notre domaine. Si on souhaite se connecter localement on l'utilise:

```
.\votre nom d'utilisateur local
```

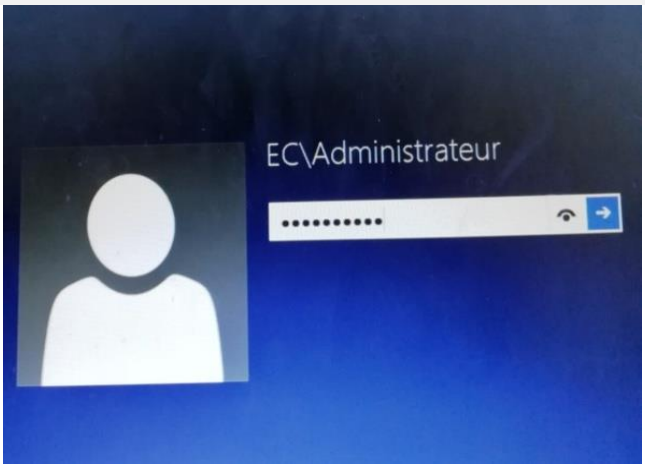

Figure III. 4: Connexion locale au domaine AD

Etape 2 : Installation du serveur RADIUS

Nous allons implémenter l'architecture ci-dessous. Lorsque l'administrateur va se connecter sur le switch, celui-ci va transmettre la requête au serveur ***RADIUS***. Le serveur va ensuite vérifier si les identifiants de session de la personne sont bien présents sur l'Active Directory, si c'est le cas l'accès est autorisé sinon l'accès est refusé.

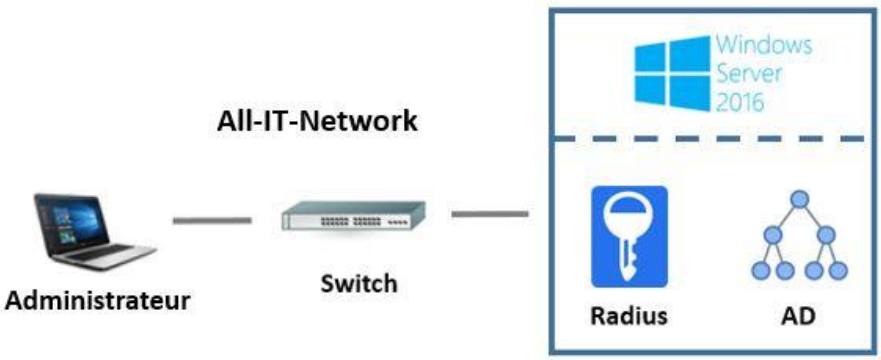

Figure III. 5: Architecture RADIUS à implémenter

- Pour installer le NPS, on refait exactement les mêmes étapes que celles de l'installation de l'Active Directory sauf que sur la fenêtre de **« sélection des rôles »,** cocher **« Services de stratégie et d'accès réseau »**, attendre quelques minutes jusqu'à l'installation du rôle.

Etape 3 : Configuration Groupe Active Directory

On doit créer un groupe ainsi qu'un utilisateur qui fera parti de celui-ci. Nous allons autoriser par la suite tous les utilisateurs présents dans ce groupe à se connecter sur les Switchs Cisco.

- Pour créer le groupe, aller sur la console d'administration AD DS, dans le menu à gauche avec un clic droit sur Users, sélectionner **« Nouveau »** puis **« Groupe ».**
- Nommer le groupe puis cliquer sur **« OK »** pour le créer.

La création d'un groupe AD illustrée dans la figure III.6.

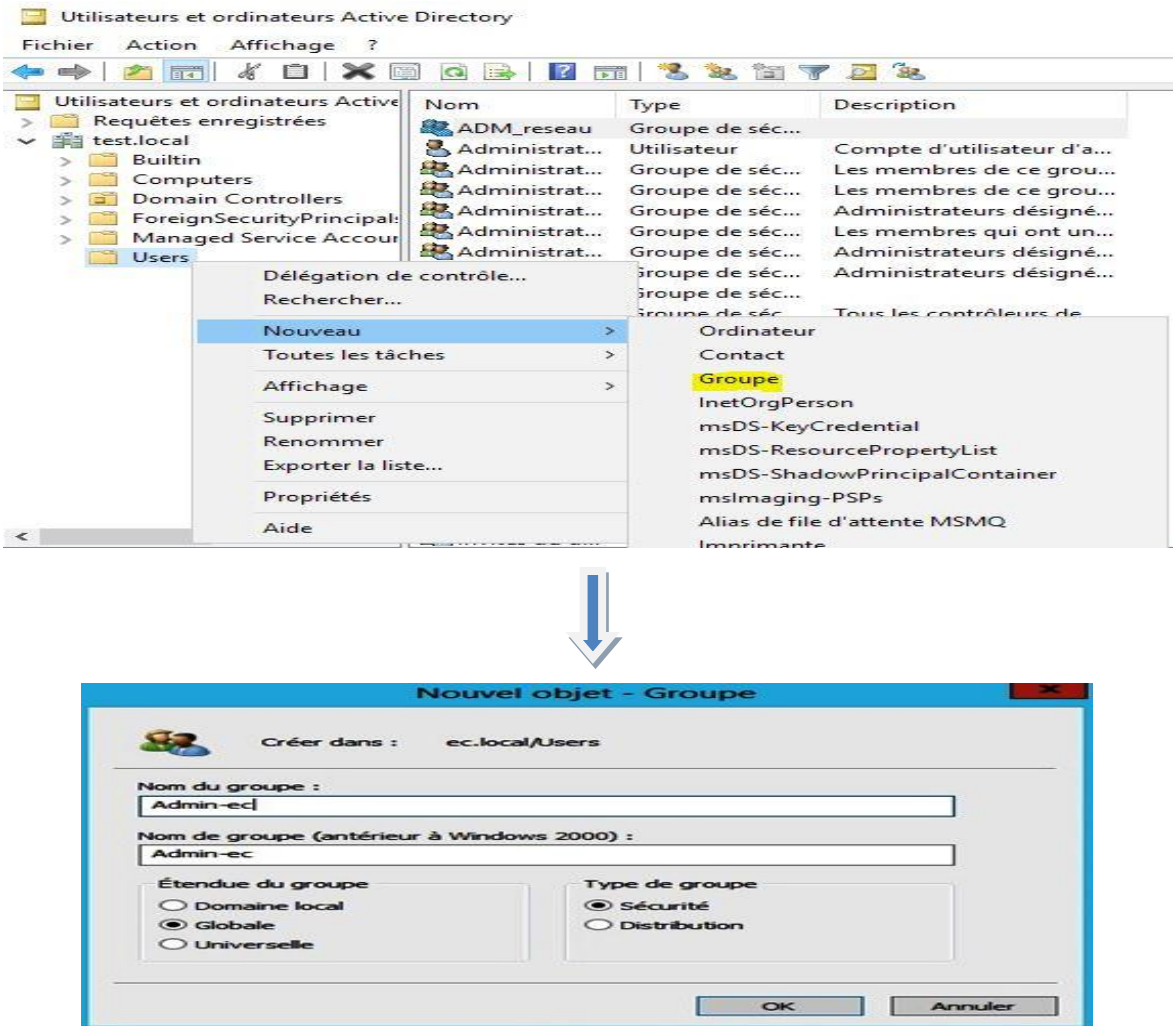

Figure III. 6: Création d'un groupe AD

Après la création du groupe AD, Admin-ec, nous allons devoir créer les utilisateurs qui feront partie de ce groupe.

- A nouveau un clic droit sur « **Users** », choisir « **Nouveau** » puis « **Utilisateur** ».
- Remplir les champs avec les informations de l'administrateur.
- L'utilisateur étant créé, nous allons intégrer l'utilisateur au groupe Admin-ec. Faire un clic droit sur le groupe créé puis sélectionner « **Propriétés** ».
- Sous l'onglet membre, cliquer sur « **Ajouter…** » .
- Renseigner le début du nom de l'utilisateur et cliquer sur « **Vérifier les noms** ».

Valider, notre utilisateur est à présent intégré au groupe.

La création et l'ajout d'un utilisateur au groupe Admin-ec, illustrée dans la figure III.7.

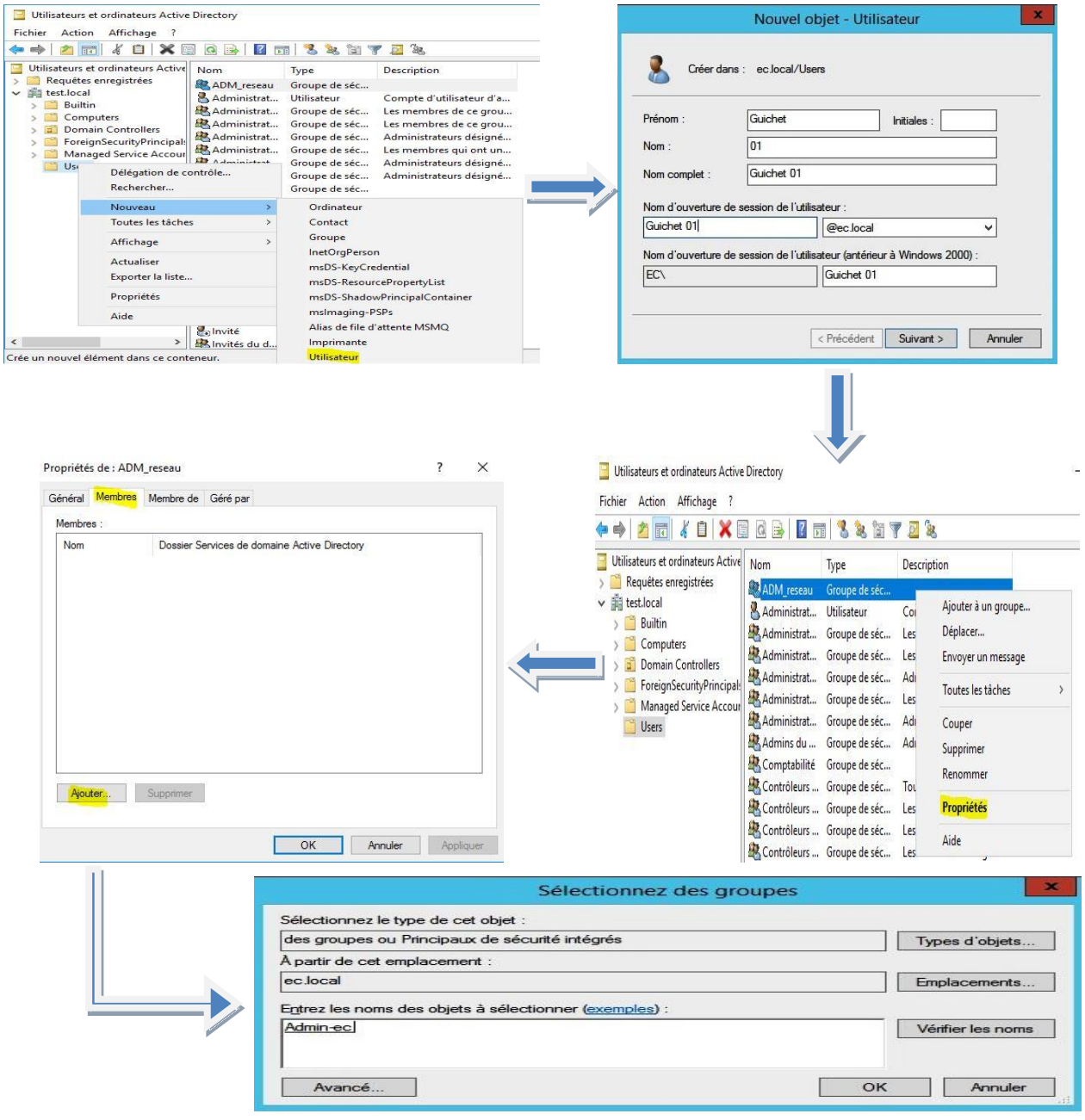

Figure III. 7: Création et l'ajout d'un utilisateur au groupe Admin-ec

Etape 4 : Ajouter des périphériques clients

Pour cette étape, on a besoin de l'adresse IP du switch.

- Aller sur la console NPS sous **« Clients et serveurs RADIUS »** faire un clic droit sur **« Clients RADIUS »** puis sélectionner **« Nouveau ».**
- Renseigner l'adresse IP de l'équipement et le secret, gardez le de coté nous allons nous en servir plus tard.

L'ajout de périphérique client se fait comme suit :

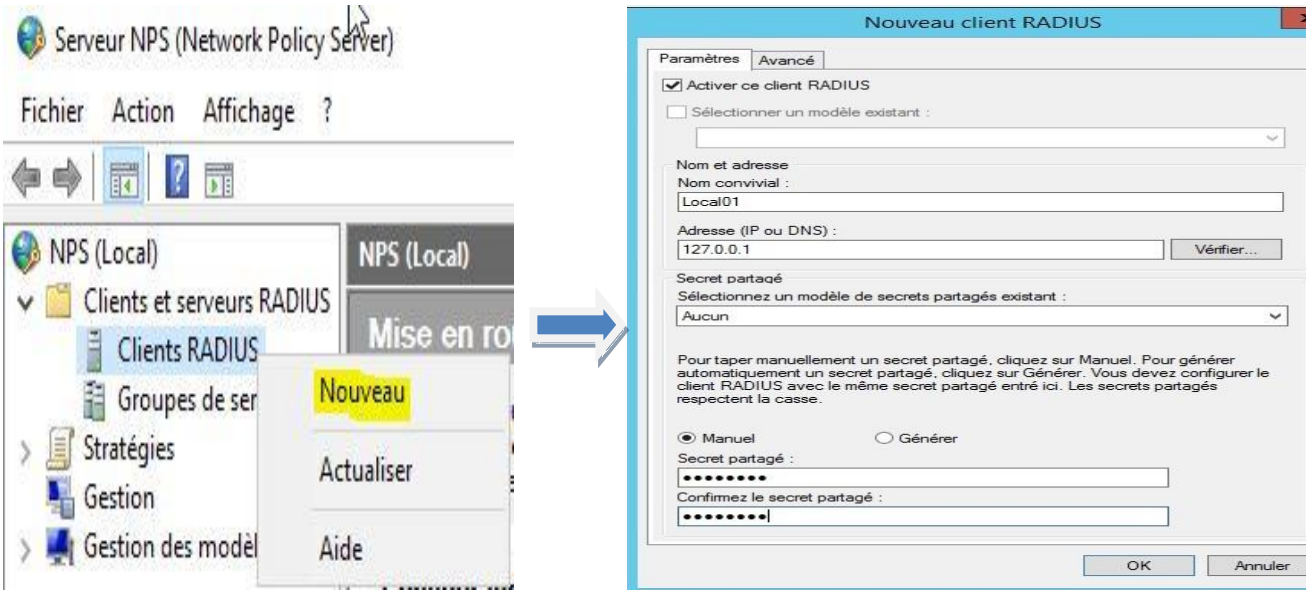

Figure III. 8: Ajout d'un Client RADIUS

Etape 5 : Configurer une stratégie réseau

Nous allons devoir définir la politique d'accès.

- Faire un clic droit sur **« Stratégies réseau »** et sélectionner **« Nouveau »**.
- Nommer la stratégie et cliquer sur **« Suivant »**.
- Sur la fenêtre suivante, spécifier les conditions d'accès, indiquer que seuls les utilisateurs faisant partie du groupe créé auparavant peuvent s'authentifier. Cliquez sur **« Ajouter… »**.
- Sélectionner « **Groupes Windows ».**
- Cliquer sur **« Ajouter des groupes… ».**:
- Indiquer le groupe créé au début de l'article.
- Notre groupe étant ajouté, cliquez sur « **Suivant ».**
- Laisser coché **« Accès accordé »** et cliquez sur **« Suivant »**.

- Cocher uniquement la case « **Authentification non chiffrée (PAP, SPAP)** », une pop-up apparaitra, cliquez sur « **Non** ».
- Pour les contraintes, elles servent à forcer la déconnexion des utilisateurs au bout d'un certain délai. On n'en positionne pas, cliquer sur « **Suivant** ».
- Dans cette fenêtre, nous allons avoir plusieurs paramètres à positionner. Dans la partie « Standard », supprimer les deux éléments déjà présents puis cliquer sur « **Ajouter…** ».
- Dans la liste, sélectionner « **Service-Type** » puis cliquer sur « **Ajouter…** ».
- Cocher la case « **Autres** », sélectionner « **Login** » puis valider.
- Ensuite cliquer sur « **Spécifiques au fournisseur** », puis sur « **Ajouter…** ».
- Sélectionnez « **Cisco-AV-Pair** ».
- Dans le champ « **Fournisseur** », saisir la variable « **shell:priv-lvl=15** ». Les niveaux d'administration fonctionnent exactement comme sur le switch. Le niveau 15 donne tous les droits.
- Cliquez ensuite sur « **Suivant** ».
- On a le récapitulatif de la stratégie réseau, cliquez sur « **Terminer** ».

La Configuration de la stratégie réseau, illustrée dans les figures ci-dessous (Figure III.9, Figure III.10, Figure III.11, Figure III.12, et Figure III.13)

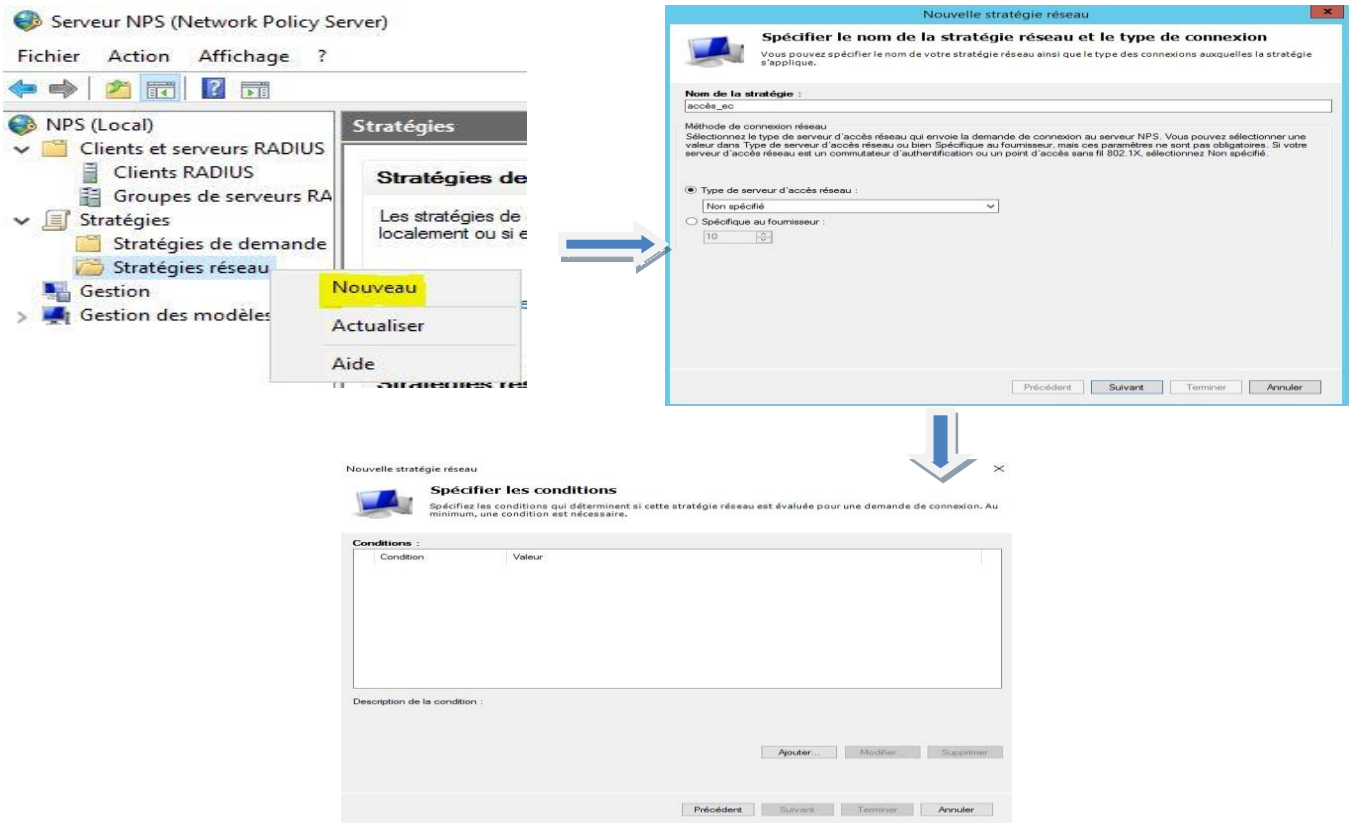

Figure III. 9: Configuration de la stratégie réseau 1

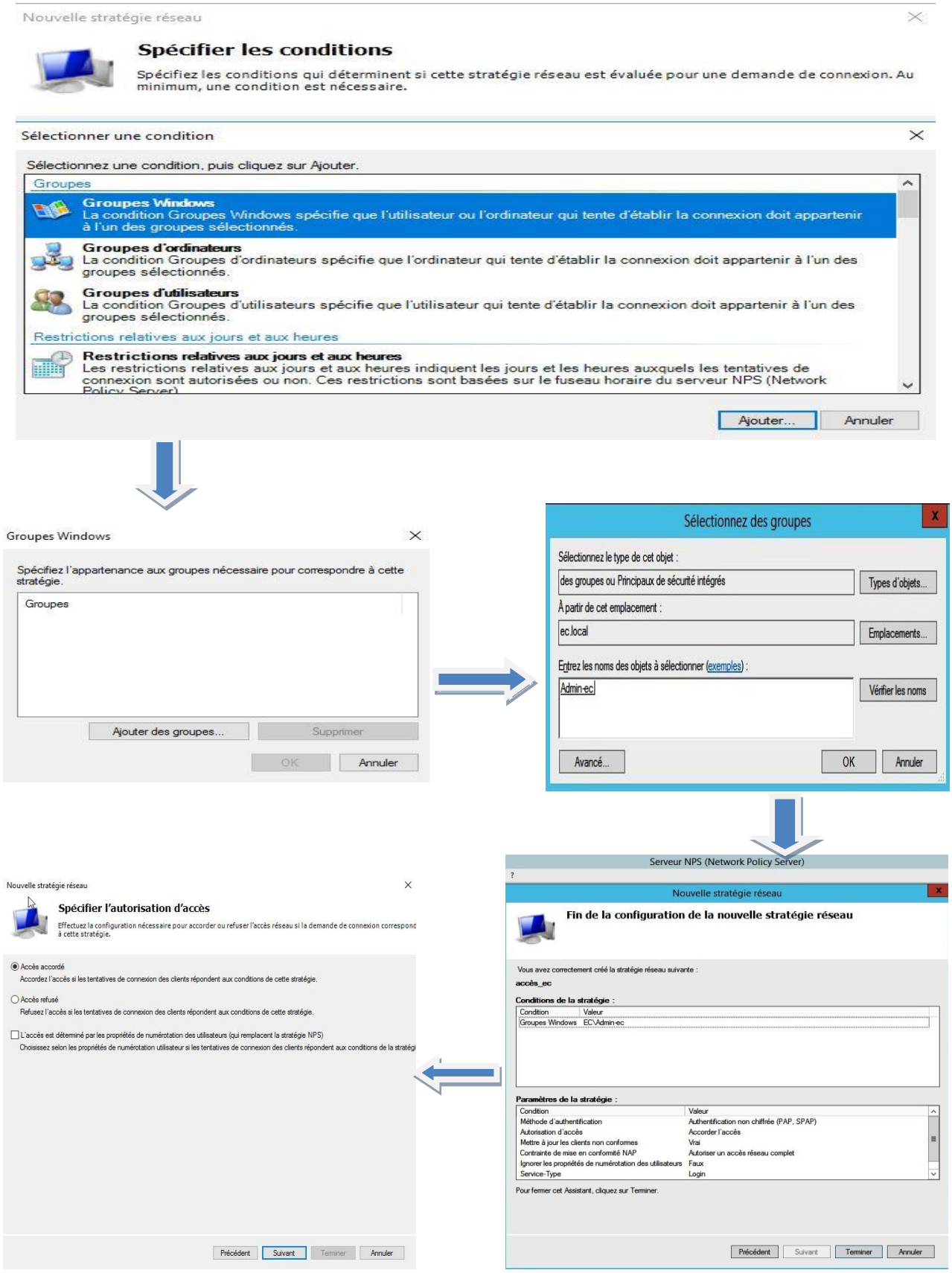

Figure III. 10: Configuration de la stratégie réseau 2

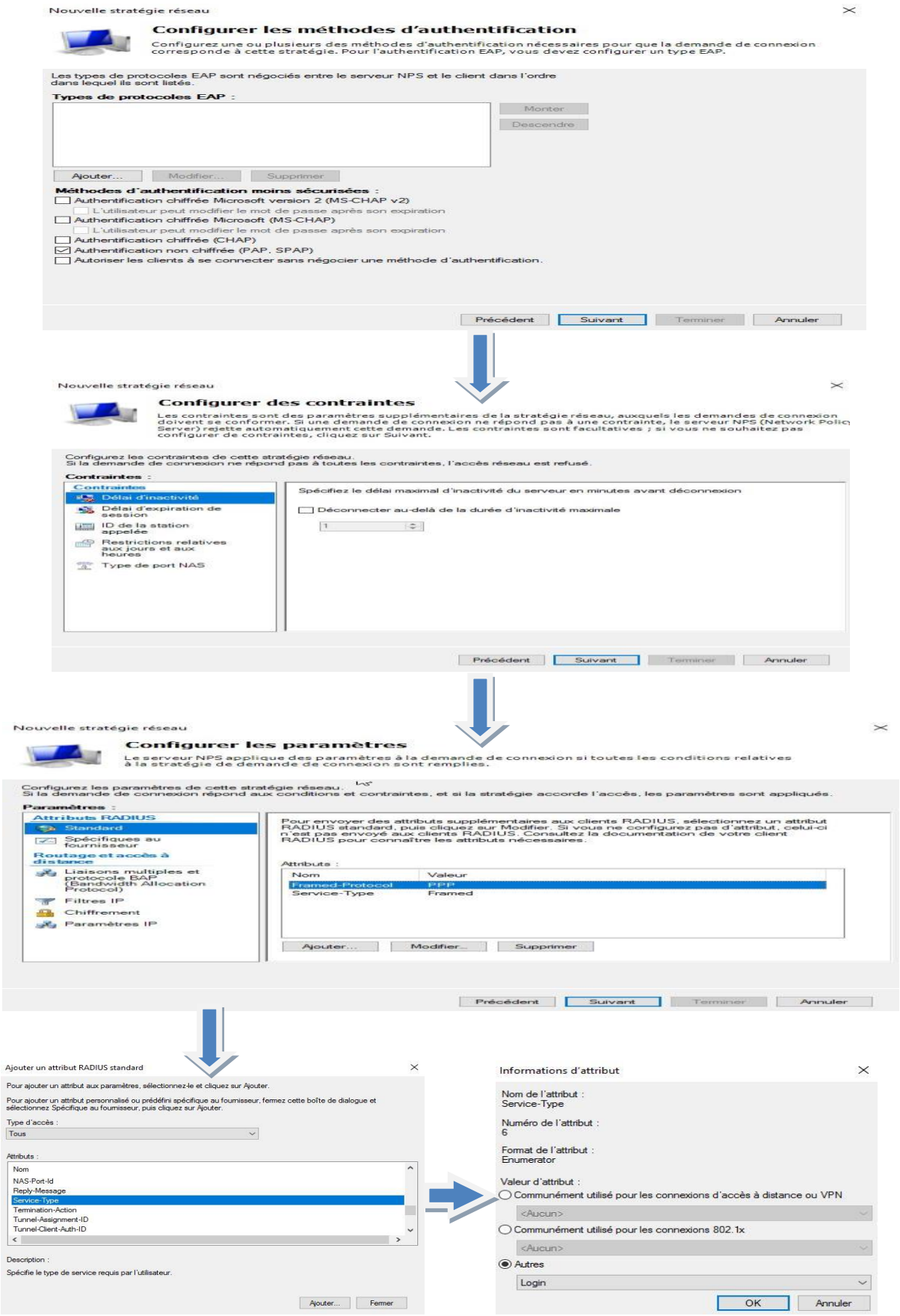

Figure III. 11: Configuration de la stratégie réseau 3

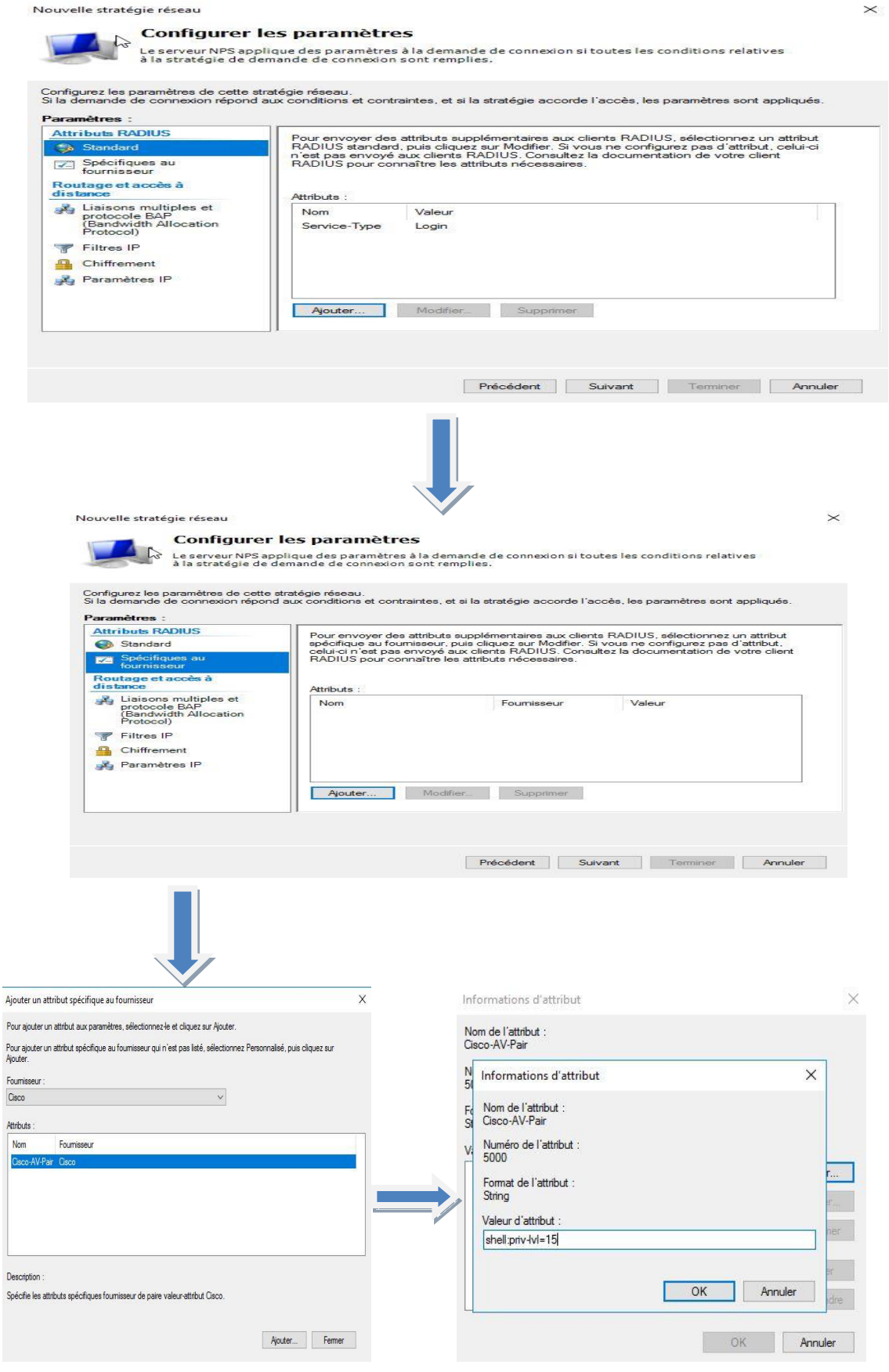

Figure III. 12: Configuration de la stratégie réseau 4

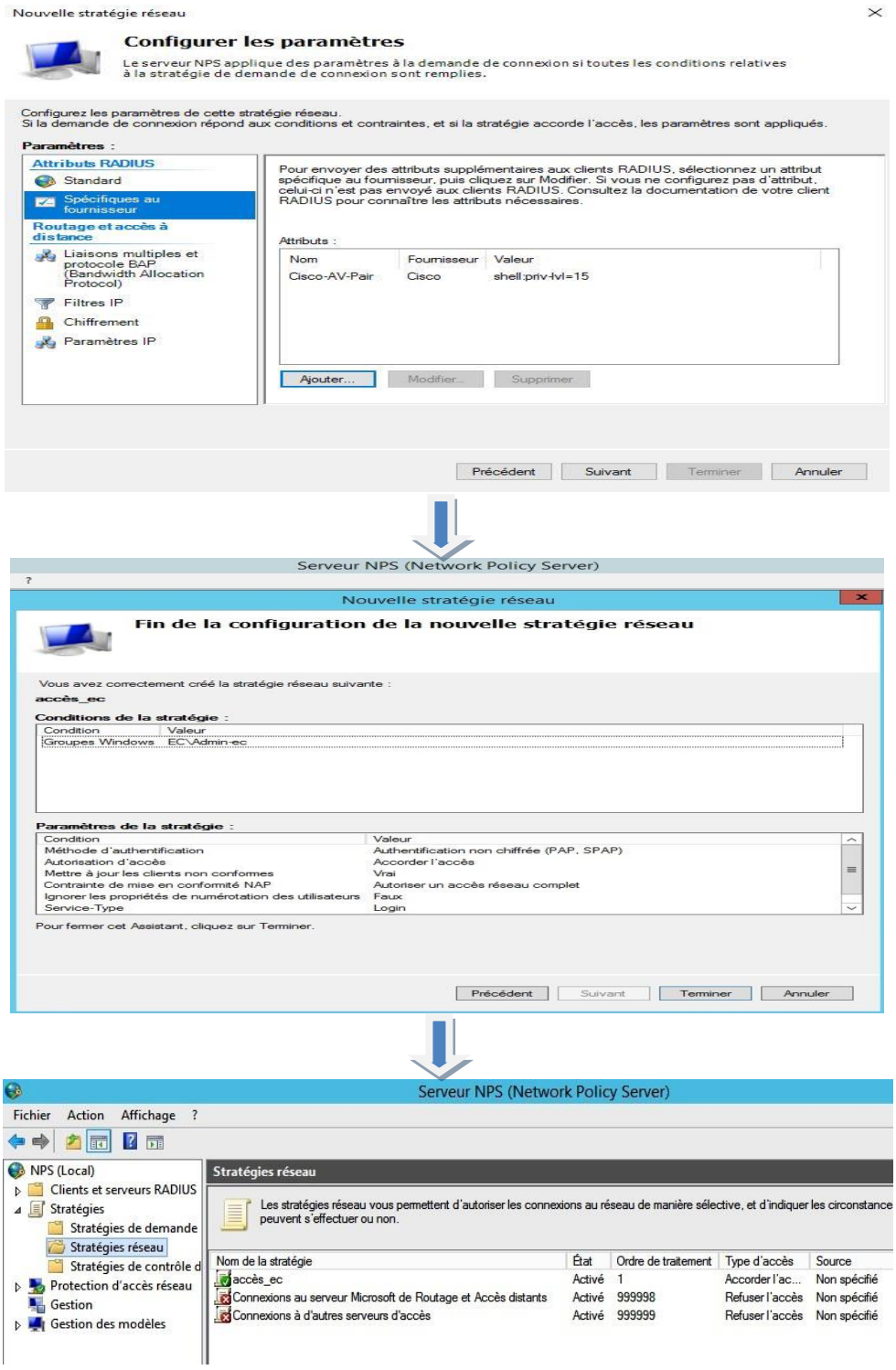

Figure III. 13: Configuration de la stratégie réseau 5

4 Conclusion

On a pu a présent, dans ce chapitre, l'installation et la configuration du serveur radius, qu'on va simuler, dans le chapitre 4, sous packet tracert.

Chapitre IV :
Déploiement de la solution RADIUS

1 Introduction

Dans cette partie, nous allons présenter la réalisation de notre projet, en expliquant les différentes configurations réalisées sur le réseau local de l'Etat Civil, en accentuant sur le stimulateur Cisco « Packet Tracer ».

Pour présenter notre travail de configuration, nous nous sommes servis des captures d'écrans qui illustrent les différentes étapes de configuration, et nous achevons par des testes de validations, pour la confirmation de fonctionnement du réseau.

2 Présentation du simulateur Cisco « Packet Tracer »

Packet Tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. L'objectif principal de ce simulateur est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau.

Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et de découvrir le fonctionnement des différents éléments constituants un réseau informatique.

La figure ci-dessous montrant l'interface principale du simulateur Cisco Packet Tracer :

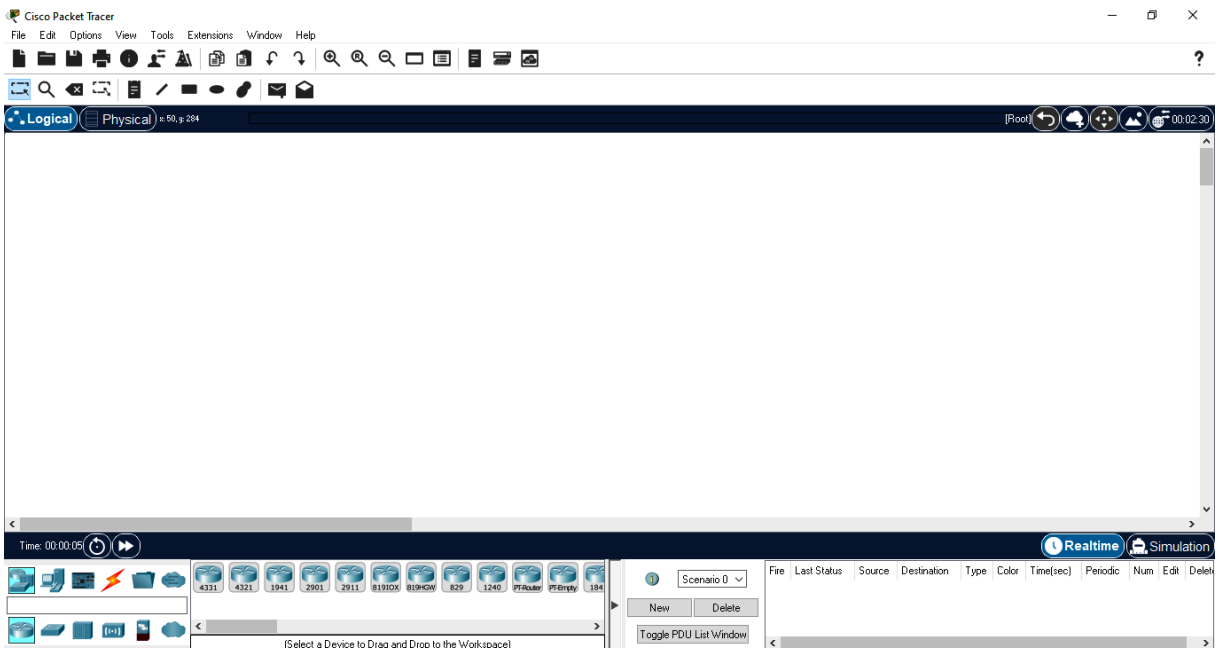

Figure IV. 1: L'interface principale du simulateur Cisco Packet Tracer

3 Création et configuration du réseau

3.1 Définition de l'architecture réseau

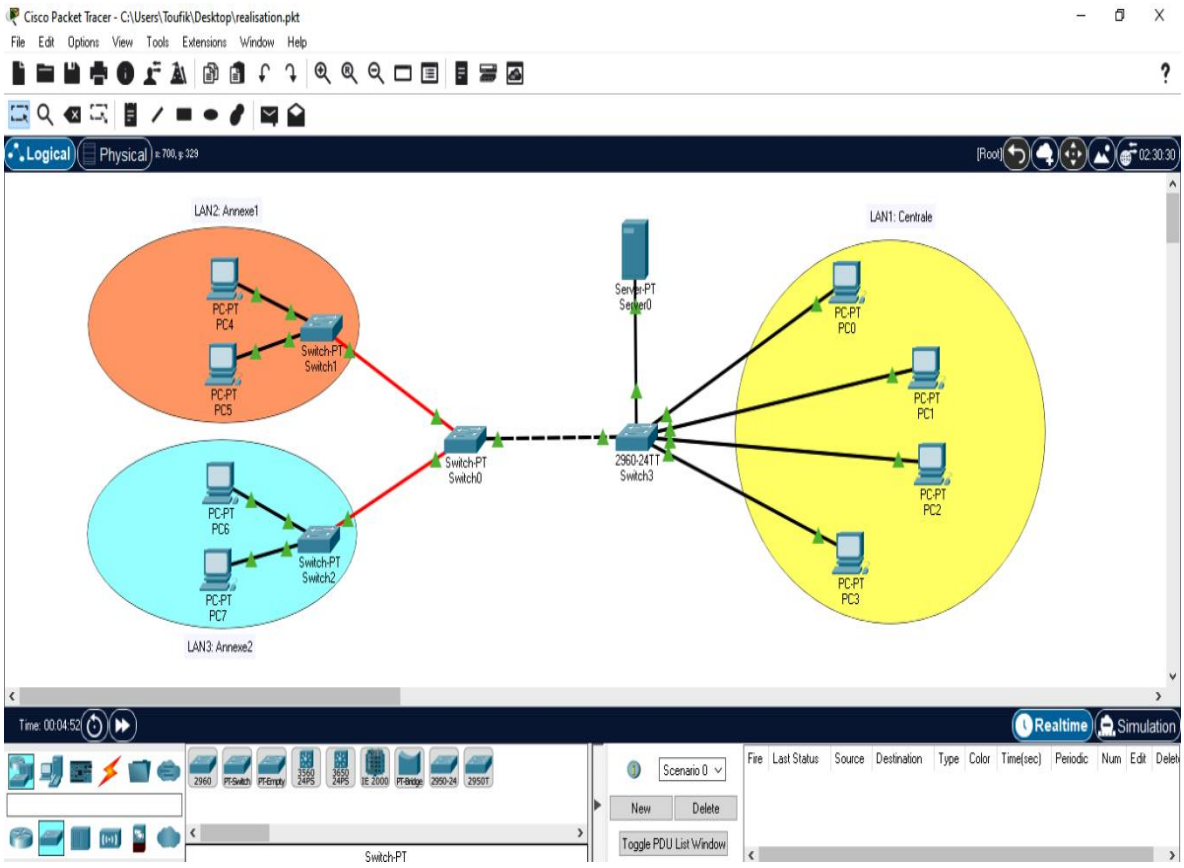

Figure IV. 2: Présentation de l'architecture

La figure ci-dessus montrant l'architecture réseau de l'Eat Civil de l'APC de Béjaia.

3.2 Configuration et paramétrage de base du réseau

A) Initialisation et redémarrage des commutateurs

- **Pour (Switch0, Switch1, Switch2)**

Etape 1 : Connectivité au commutateur.

```
Switch>enable
Switch#
```

Etape 2 : Détermination si des réseaux locaux virtuels (VLAN) ont été créés.

```
Switch#show flash:
Directory of flash:/
1 -rw- 3117390 <no date> pt3000-i6q4l2-mz.121-22.EA4.bin
64016384 bytes total (60898994 bytes free)
```

Etape 3 : Suppression du fichier de configuration initiale.

```
Switch#erase startup-config
```

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#

Etape 4 : Redémarrage du commutateur.
Switch#reload
Proceed with reload? [confirm]

- **Pour (Switch3)**

Etape 1 : Connectivité au commutateur.
Switch>enable
Switch#

Etape 2 : Détermination si des réseaux locaux virtuels (VLAN) ont été créés.
Switch#show flash
Directory of flash:/

1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)

Etape 3 : Suppression du fichier de configuration initiale.
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
Etape 4 : Redémarrage du commutateur.
Switch#reload
Proceed with reload? [confirm]

B) Configuration les hôtes (PCs et serveur)

La figure ci-dessous montrant la configuration pour les hôtes, PCs (PC0, PC1, PC2, PC3, PC4, PC5, PC6, PC7) et serveur (NPS-RADIUS-SERVER).

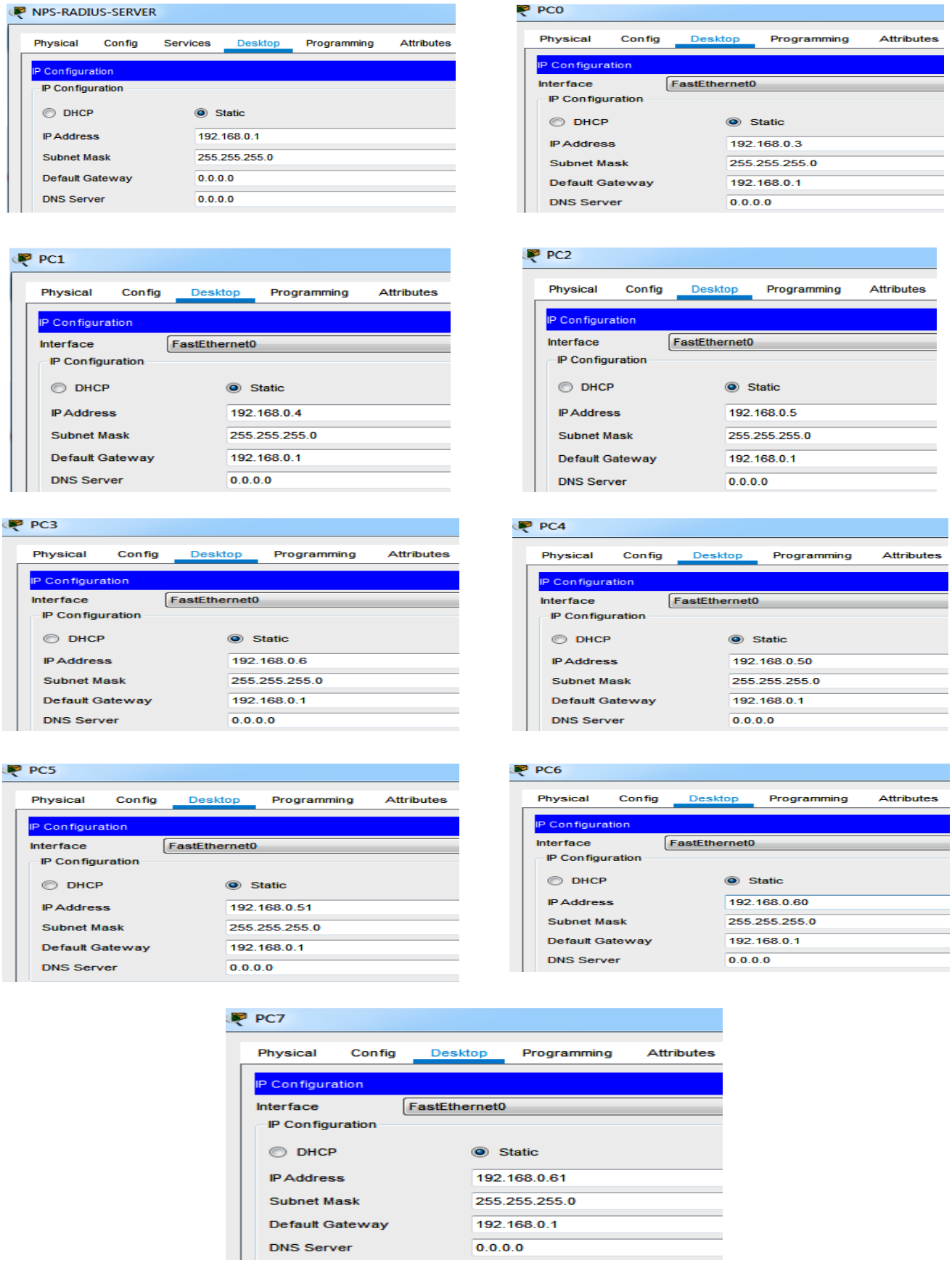

Figure IV. 3: Configuration des hôtes (PCs, Serveur)

C) Configuration du Hostname pour les commutateurs

Cette étape permet de donner un nom significatif à l'ensemble des équipements constituants les LANs (la nomination du commutateur)

- **Commutateur Switch0**

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW0
SW0(config)#
```

- **Commutateur Switch1**

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1 (config)#exit
SW1 #
```

- **Commutateur Switch2**

```
Switch>enable
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2 (config)#exit
SW2 #
```

- **Commutateur Switch3**

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname CLIENT-RADIUS
CLIENT-RADIUS(config)#
```

D) Configuration IP de commutateur CLIENT-RADIUS

```
CLIENT-RADIUS(config)#interface vlan 1
CLIENT-RADIUS(config-if)#ip address 192.168.0.2 255.255.255.0
CLIENT-RADIUS(config-if)#no shutdown
```

E) Test de la connectivité

Dans cette partie nous allons vérifier les communications entre quelques équipements en utilisant la commande « Ping » qui vérifié la réponse d'un équipement sur le réseau. En effet

si un équipement veut communiquer avec à un autre, le Ping permet d'envoyer des paquets au destinataire.
Si l'équipement récepteur reçoit ces paquets, donc, la communication est réussie Sinon, elle est échouée.

- De PC6 (LAN3) vers PC4 (LAN2) et PC0 (LAN1)
- De PC6 vers le commutateur (CLIENT-RADIUS) et le serveur (NPS-RADIUS SERVER)

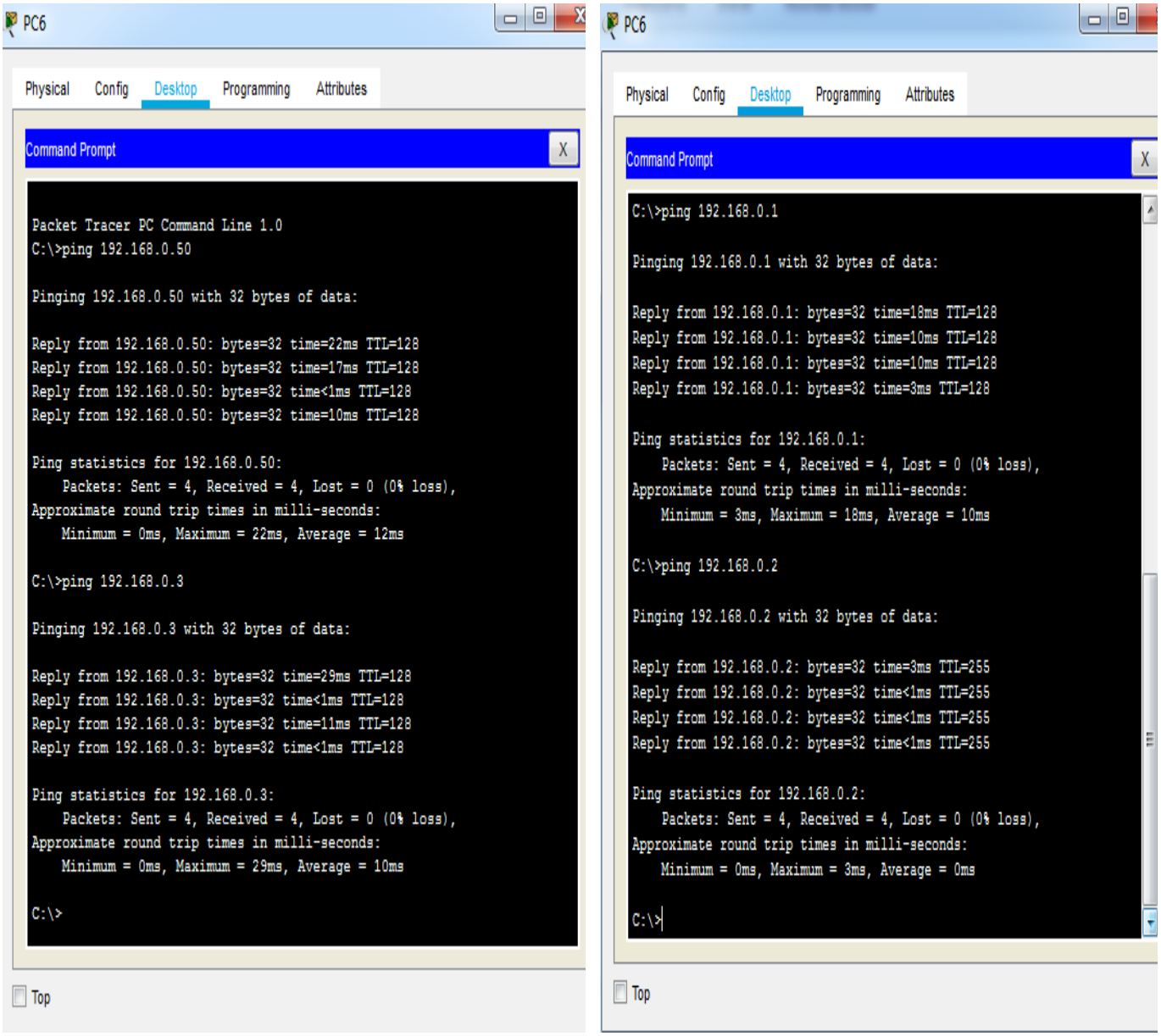

Figure IV. 4: Ping réussi

3.3 Configuration de commutateur CLIENT-RADIUS pour l'accès SSH

Secure Shell (SSH) est un protocole réseau qui permet d'établir une connexion d'émulation de terminal sécurisée avec un routeur ou un autre périphérique réseau. SSH chiffre toutes les informations qui transitent via la liaison réseau et assure l'authentification de l'ordinateur distant. Il est en train de remplacer rapidement Telnet en tant qu'outil de connexion à distance de prédilection des professionnels réseau. Ce protocole est très souvent utilisé pour se connecter à une machine distante et exécuter des commandes.

```
CLIENT-RADIUS(config)#no ip domain-lookup
CLIENT-RADIUS(config)#enable secret cisco
CLIENT-RADIUS(config)#line console 0
CLIENT-RADIUS(config-line)#password cisco
CLIENT-RADIUS(config-line)#login
CLIENT-RADIUS(config-line)#logging synchronous
CLIENT-RADIUS(config-line)#exec-timeout 3 0
CLIENT-RADIUS(config-line)#exit
CLIENT-RADIUS(config)#service password-encryption
CLIENT-RADIUS(config)#ip domain-name ec.local
CLIENT-RADIUS(config)#username ADMIN privilege 15 secret cisco
CLIENT-RADIUS(config)#crypto key generate rsa
The name for the keys will be: CLIENT-RADIUS.ec.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

CLIENT-RADIUS(config)#ip ssh ve
*Mar 1 0:40:59.611: %SSH-5-ENABLED: SSH 1.99 has been enabled
CLIENT-RADIUS(config)#ip ssh version 2
CLIENT-RADIUS(config)#line vty 0 15
CLIENT-RADIUS(config-line)#transport input ssh
CLIENT-RADIUS(config-line)#login local
CLIENT-RADIUS(config-line)#exit
CLIENT-RADIUS(config)#exit
CLIENT-RADIUS#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Etape 3 : Test de l'accès SSH vers CLIENT-RADIUS

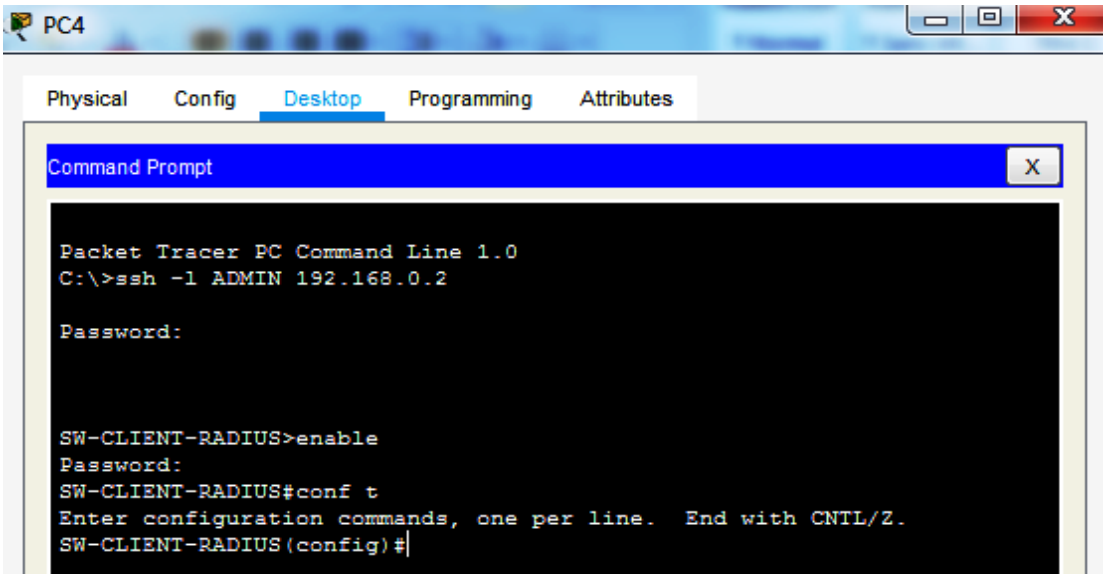

Figure IV. 5: Test de l'accès SSH vers CLIENT-RADIUS

3.4 Présentation de l'architecture réseau après configuration

La figure ci-dessous montrant l'architecture réseau de l'Eat Civil de l'APC de Béjaia après la configuration.

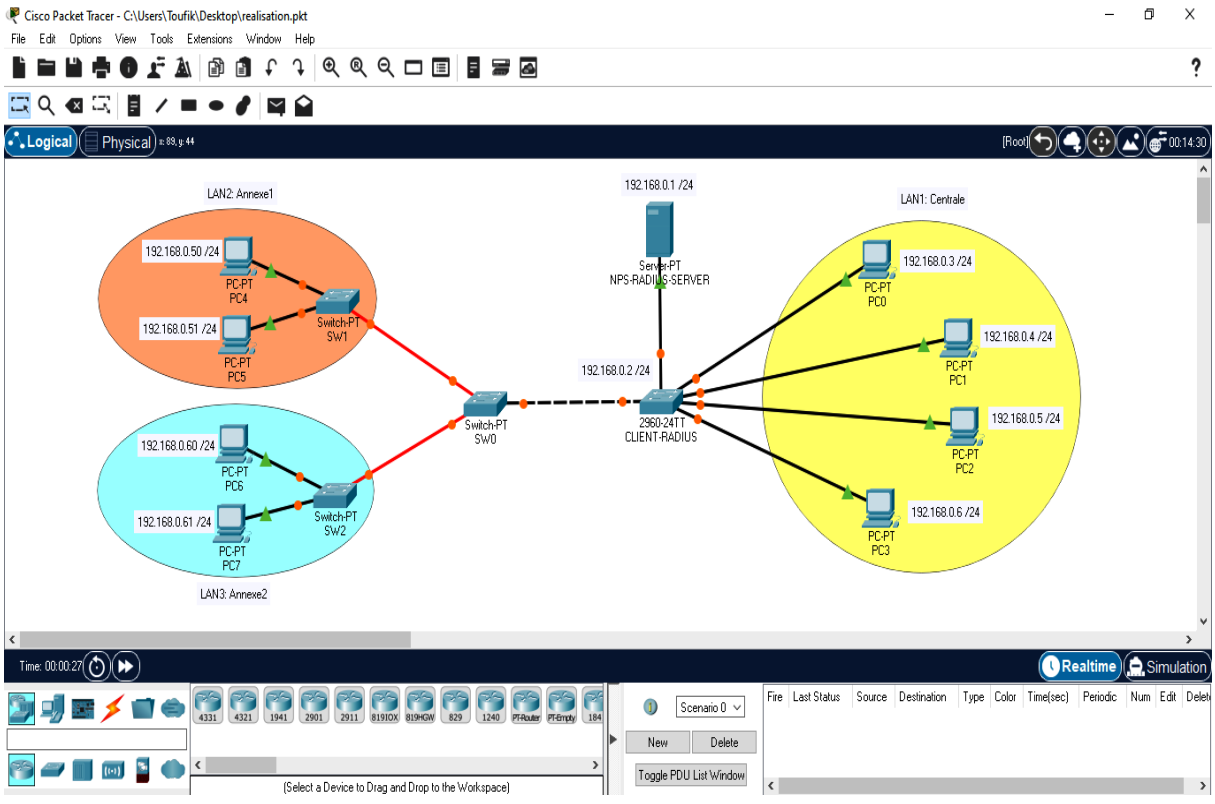

Figure IV. 6: Présentation de l'architecture après configuration

Après avoir configuré les adresses IP (configuration de l'adresse IP du serveur, configuration IP de l'interface VLAN du commutateur et la configuration IP PC) et le commutateur CLIENT-RADIUS pour l'accès SSH, on passe à la configuration pas à pas de l'authentification via un serveur RADIUS nommé NPS-RADIUS-SERVER.

4 Configuration pas à pas de l'authentification AAA (RADIUS)

Pour se faire, nous suivons quelques étapes de configuration du serveur RADIUS et le Switch Cisco. Ces étapes de configuration RADIUS sont données ci-dessous :

- Configuration de serveur RADIUS (NPS-RADIUS-SERVER**)**
- Configuration AAA sur le Switch (CLIENT-RADIUS)

4.1 Configuration de serveur RADIUS (NPS-RADIUS-SERVER)

Dans cette étape, aller dans **l'onglet Services**, sélectionner le champ **AAA** à gauche. Activer le service en sélectionnant « **On** » et faisons la configuration requise. Définir le nom du client, notre nom de client est Switch (**CLIENT-RADIUS**). Après cela, définir l'adresse IP du client qui est **192.168.0.2** (IP de l'interface VLAN 1). Sélectionner le type de serveur qui est **RADIUS**. Enfin, choisir une clé secrète **(xyz)** qui est partagée entre le serveur RADIUS et le Swicth. Avec le bouton « « **Add** » nous l'ajouterons à la configuration établie précédemment.

Ensuite, nous définissons la partie de configuration de l'utilisateur, nous tapons un nom d'utilisateur et un mot de passe, cliquons sur « **Add** » (garder les noms des PC comme noms d'utilisateurs), ces utilisateurs vont utiliser SSH pour se connecter. La figure ci-dessous montre la configuration du serveur radius sur Packet Tracer.

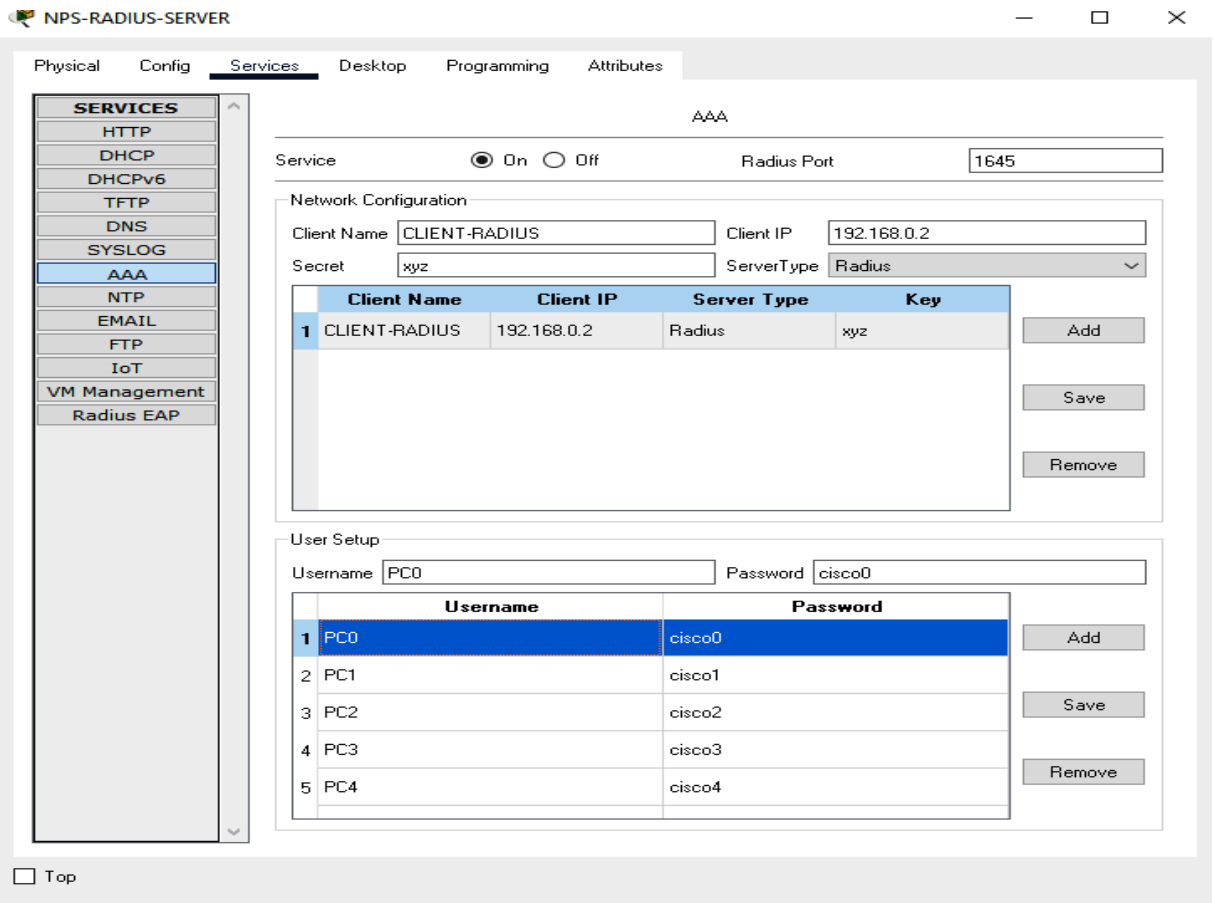

Figure IV. 7: Configuration du NP-RADIUS-SERVER sur Packet Tracer

4.2 Configuration AAA sur le Switch CLIENT-RADIUS

La fonctionnalité AAA (authentification, autorisation et comptabilité) du commutateur Cisco peut être utilisée comme solution centralisée pour sécuriser et contrôler l'accès des utilisateurs aux commutateurs. Les commutateurs Cisco sont capables d'implémenter la fonctionnalité AAA avec le protocole RADIUS. Pour utiliser AAA, nous devons l'activer, puis la connecter à un service AAA hébergé dans un serveur.

Etape 1 : Activation du modèle AAA

Pour activer les fonctions d'authentification, d'autorisation et de comptabilité nous utilisons le code :

```
CLIENT-RADIUS(config)#aaa new-model
```

Etape 2 : Activation de la configuration en mode local pour « l'Authentification »

```
CLIENT-RADIUS(config)#aaa authentication login default group radius local
```

Etape 3 : Configuration de la communication entre le Switch et le Serveur RADIUS

Pour que le Switch Cisco puisse communiquer avec le serveur RADIUS, il faut fournir l'adresse IP du serveur RADIUS (192.168.0.1), le port UDP du serveur avec lequel le Switch Cisco va communiquer (1645) et enfin la clé secrète utilisée entre le serveur RADIUS et le Switch Cisco qui est xyz.

```
CLIENT-RADIUS(config)#radius-server host 192.168.0.1 auth-port 1645 key xyz
```

Etape 4 : Attribution de l'authentification dans la ligne VTY

Lorsque les utilisateurs essaient d'accéder au commutateur par SSH par exemple, ils sont invités à saisir un nom d'utilisateur et un mot de passe.

```
CLIENT-RADIUS(config)#line vty 0 15
CLIENT-RADIUS(config-line)#login authentication default
```

Etape 5 : Activation de la configuration en mode local pour « l'Autorisation »

```
CLIENT-RADIUS(config)#aaa authorization exec default group radius local
```

Etape 6: Activation de la configuration en mode local pour « la comptabilité »

```
CLIENT-RADIUS(config)#aaa accounting exec default start-stop group radius
```

Etape 7: Vérification que ces éléments AAA sont bien pris par la configuration

```
CLIENT-RADIUS#show run | include aaa
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
CLIENT-RADIUS#show run | include radius
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius-server host 192.168.0.1 auth-port 1645 key xyz
```

Implique ➔ configuration réussie.

4.3 Test de connectivité RADIUS via SSH

Nous allons vérifier la connectivité sur le Serveur RADIUS par CLIENT-RADIUS pour les postes utilisateurs PC0 et PC7, comme illustré dans la figure ci-dessous.

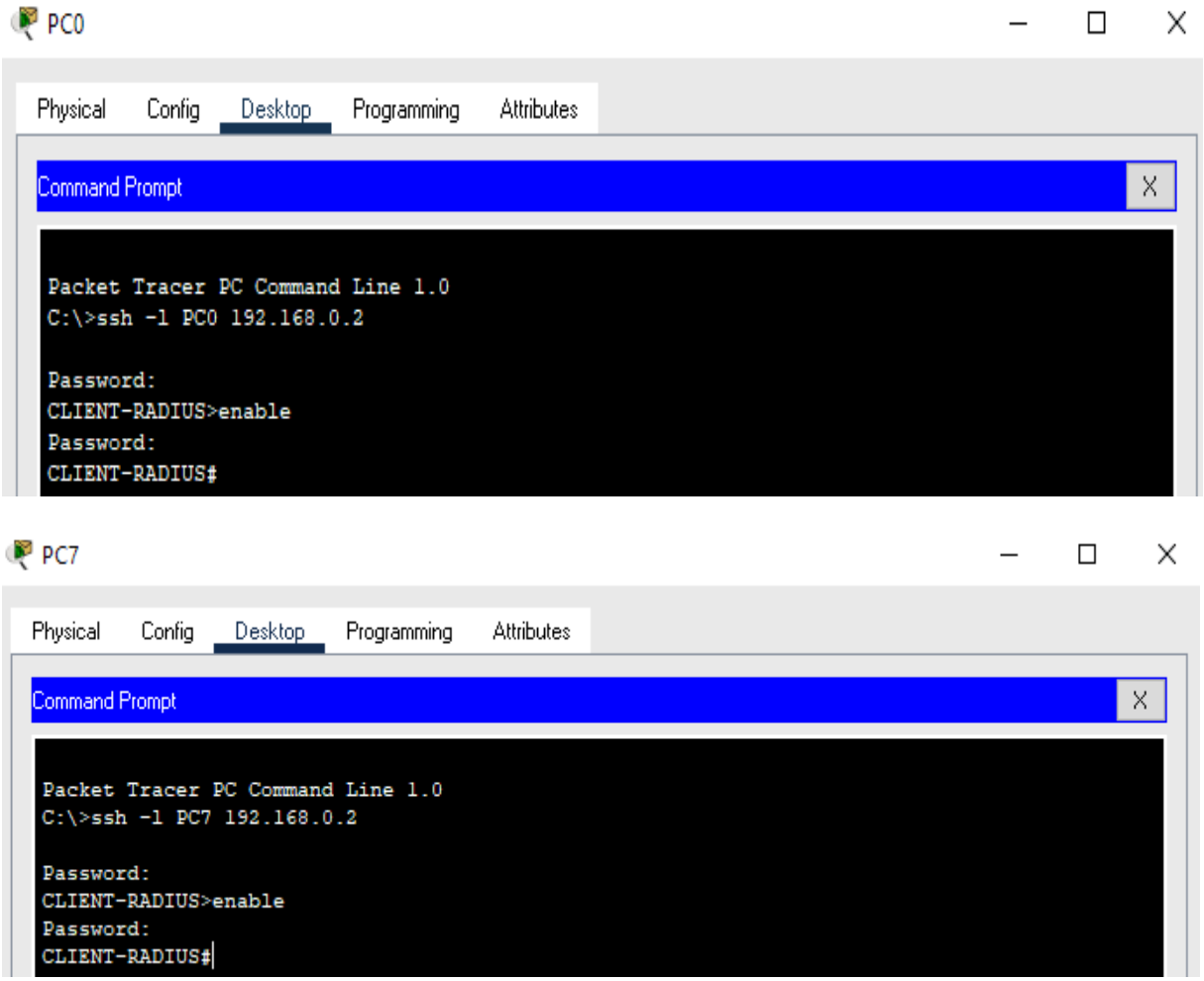

Figure IV. 8: Connectivité réussie sur le Serveur RADIUS par CLIENT-RADIUS

5 Conclusion

Nous avons vu à travers cette partie la présentation du simulateur Cisco Packet Tracer que nous avons utilisé pour la réalisation de notre travail. Nous avons proposé une nouvelle architecture pour le réseau de l'APC de Béjaia (Service Etat Civil et ces annexes). Nous avons illustré quelques interfaces portant sur l'ensemble des configurations réalisées pour cette architecture.

Pour la mise en marche, nous avons été amenés à configurer les différents équipements qu'on a utilisé, le Switch, le Serveur RADIUS, et le triple-A sur le CLIENT-RADIUS, enfin nous avons effectué un ensemble de tests de validation pour prouver l'efficacité du réseau.

Conclusion générale

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

Après une étude sur différents mécanismes d'authentification, nous avons constaté l'avantage de celui-ci concernant le contrôle d'accès des utilisateurs aux services demandés pour minimiser le risque des attaques menaçant le réseau. ce mécanisme s'agit en fait de la mise en place d'une solution d'authentification RADIUS basée sur un serveur RADIUS qui permet d'assurer l'authentification des clients avant tout accès au réseau de l'APC de Bejaia, ainsi de définir les droits d'accès à chacun de ces utilisateurs.

Pour la réalisation du service d'authentification RADIUS, nous avons utilisé Windows server 2012 qui inclut le serveur d'authentification RADIUS. Ce dernier fait appel à des services de domaines Active Directory permettant d'avoir des contrôleurs de domaines et aux services de stratégies d'accès qui nous permit de définir une méthode d'accès au réseau.

La mise en œuvre de ce projet, nous a permis d'apporter une contribution à l'APC de Bejaia, et aussi d'acquérir de nouvelles connaissances sur le protocole 'authentification RADIUS grâce à une étude détaillée sur son fonctionnement, ses principes et les protocoles qu'il utilise.

Enfin, comme perspectives pour ce projet, nous souhaitons également exploiter mieux les services qu'offre le protocole RADIUS notamment l'authentification des utilisateurs, on a proposé la procuration de l'équipement adéquat, un Switch de niveau 3, pour pouvoir réaliser notre solution sur le plan réel puisque le reste du matériels est disponible et mit totalement a notre disposition.

Bibliographie

[B1] : N. BATTAT, « les systèmes de sécurité », Cours Master 2 professionnel informatique, Université de Bejaïa, 2021.

[B2] : Z. Farah, « Cours introduction à la sécurité», Cours Master 1 professionnel informatique, Université de Bejaïa, 2019.

[B3] : M. CHOISNARD, « Réseaux et sécurité informatiques», Cours MIGS, Université de Bourgogne 2015.

[W1]:http://math.univ-lyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_generalites/generalites.html , consulté le 05/2022

[W2]:https://waytolearnx.com/2019/06/topologie-du-reseau-informatique.html, consulté le 05/2022

[W3]:https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_mod%C3%A8les_OSI_et_TCP, consulté le 05/2022

[W4]:https://www.frameip.com/tcpip/, consulté le 05/2022

[W5]:http://www.iro.umontreal.ca/~kropf/ift-6052/exercices/applets/applet5/introduc.htm, consulté le 05/2022

[W6]:https://www.it-connect.fr/routage-statique-et-routage-dynamique/, consulté le 05/2022

[W7]:https://www.universalis.fr/encyclopedie/reseaux-informatiques/6-securite-dans-les-reseaux/, consulté le 05/2022

[W8]:http://senhaji.net/category/securite-informatique/, consulté le 05/2022

[W9]:https://www.techno-science.net/glossaire-definition/Logiciel-malveillant.html, consulté le 05/2022

[W10] : https://all-it-network.com/installer-redonder-ad/, consulté le 06/2022

Résumé

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

Notre projet consiste à mettre en œuvre une solution d'authentification pour le réseau local du service Etat Civil de l'APC de Bejaïa, assurant le contrôle d'accès des utilisateurs, pour cela, nous avons choisi le protocole RADIUS qui est l'un des protocoles d'authentification les plus performants.

Pour la réalisation de ce travail, nous avons fait d'abord un rappel sur les notions de bases des réseaux et la sécurité informatique pour bien comprendre les concepts répondant à la problématique, et pour l'implémentation de la solution, nous avons choisi Windows Server 2012 qui inclut le serveur d'authentification RADIUS, la base de données Active Directory pour l'enregistrement des comptes utilisateurs et les services de stratégies d'accès.

Mots-clés : authentification, RADIUS, Windows Server 2012, Active Directory et stratégie réseau (NPS).

Abstract

Nowadays, computer security is almost essential for the proper functioning of a wired or wireless network, for these company network administrators must implement effective security mechanisms.

Our project consists in implementing an authentication solution for the local network of the service Registry Office of the APC Bejaia, ensuring the access control of the users, for this, we have chosen the RADIUS protocol which is one the most powerful authentication protocols.

For the realization of this work, we first made a reminder on the basic notions of networks and computer security to understand the concepts responding to the problem, and for the implementation of the solution, we chose Windows Server 2012 which includes RADIUS authentication server, Active Directory database for user account registration and access policy services.

Keywords : authentication, RADIUS, Windows Server 2012, Active Directory and network policy (NPS).