REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTRE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire

de fin d'études
En vue de l'obtention du diplôme
d'Ingénieur d'Etat en Electronique
Option : contrôle

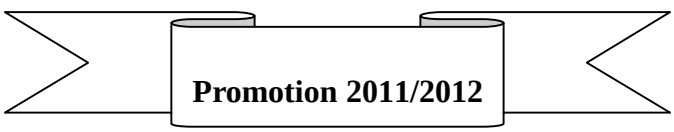
Implémentation d'un réseau Wi-Fi sécurisé à base d'un Contrôleur C 1000 d'Algérie Telecom au niveau de la résidence universitaire I.L.E de Tizi-Ouzou

Proposé et dirigé par :

Mr. Mourad LAHDIR
Mr. Abdenour HADOUS
Mr. Rachid AMRANE

Etudié par :

Melle: BOUGHIAS Naima
Melle: BAOUALI Kamilia
Melle: BOUDIA Lynda



Remerciement

***T**out d'abord nous remercions le clément et le miséricordieux, le bon dieu de nous avoir donné le courage, la volonté, mais aussi la patience afin de réaliser ce modeste travail.*

Nos remerciements les plus chaleureux vont à notre promoteur Mr. LAHDIR Mourad pour son encadrement, ses conseils judicieux et ses orientations qui nous ont favorablement assistés.

Nous tenons à exprimer notre entière gratitude et reconnaissance à notre encadreur Mr. HADOUS Abdenour (Ingénieur du service réseau et maintenance de Algérie Telecom) ainsi qu'a Mr. AMRANE Rachid (Ingénieur réseau à Algérie Telecom) pour leurs encouragements et la chance qu'ils nous ont donné afin de travailler sur un tel projet.

***O**n tient à remercier tous les membres de la Direction Régionale de Télécommunication (DRT) de Tizi-Ouzou qui nous ont permis d'effectuer notre travail dans les meilleures conditions matérielles et techniques que l'on puisse espérer. Particulièrement, pour toute l'équipe du Laboratoire Entretien Télécommunication (LET), pour leurs accueils chaleureux et sympathiques et surtout pour leur grande disponibilité, ainsi que pour l'ambiance amicale qui y règne.*

Nous témoignons notre grande gratitude à Mme BOUGHIAS Ouiza et Mr. OUALOUCHE Fathi, et nous tenons à les remercier pour leurs aides et précieux conseils.

Nos remerciements s'adressent à tous les membres du jury pour l'honneur qu'ils nous font en acceptant d'évaluer notre travail.

Nous remercions également le personnel de la cité universitaire « ILE », notamment le chef de service d'entretien Mr. LAFRAOUI Hamid pour son accueil chaleureux.

Dédicaces

Je dédie ce modeste travail :
A MES PARENTS
A qui
Je dois Ce Que Je Suis
Que Dieu Vous Protège
Vous Prête Une Bonne Santé
Et Une Longue Vie
A mes sœurs :Ouiza, Malika,Sabrina, Yasmina etHayet
A mes frères :Ahcene et Mourad
A Hamid qui m'a soutenu
A toute ma famille
A mes amis (es) qui ont été là pour moi
A tous ceux qui ne méritent pas d'être oublié.

B.Naima

Je dédie cet humble travail :
À mes très chers parents pour leur grand amour
Et leurs sacrifices
Que dieu leur procure bonne santé et longue vie
Aucun hommage ne pourrait être à la hauteur
De l'amour et l'affection dont ils ne cessent de me combler
À mes très chers frères : Amine, Mounir et Yazid
À mon bras droit Idir
À toute ma famille
À tous mes amis (es).

B. Kamilia

Je dédie ce modeste travail :
A mon ange père pour l'amour et l'éducation qui nous a offert
A ma courageuse mère pour sa patience énorme
Que dieu leur prête une bonne santé et une longue vie
J'espère qu'un jour je serai capable de leur donner le minimum
A mon très cher mari Rachid qui a été toujours à mes cotés
A mes chers frères : Ahcene, Mohammed et Ferhat
A mes chères sœurs : Djamila, Lydia et Soraya
A notre ange Sarah
A ma belle famille
A mes binômes et leurs familles
A tous mes amis (es)

B. Lynda

Sommaire

Chapitre II: Les différents protocoles

Chapitre III: La sécurité des réseaux sans fil

DEUXIEME PARTIE :

IMPLEMENTATION D'ARCHITECTURE RESEAU SANS FIL SECURISEE A LA RESIDANCE UNIVERSITAIRE « I L E » DE TIZI –OUZOU.

Chapitre I : conception et installation.

Chapitre II: Sécurisation et configuration des équipements.

Liste des figures

Première partie :

Deuxième partie :

Liste des tableaux :

Introduction générale

Se connecter à Internet sans le moindre câble, à domicile, au bureau, voir même dans les points d'accès publics appelés Hots pot et le besoin de plus en plus important de mobilité, ainsi que la diversification des réseaux a poussé les organismes à normaliser une nouvelle technologie nommée Wi-Fi (wireless fidelity) pour assurer une compatibilité entre les différents fabricants.

Les employés et les étudiants équipés d'ordinateurs portables compatible Wi-Fi peuvent rester connectés et productifs hors du bureau et à tout moment grâce aux qualités des services offerts par le wi-fi.

Ce travail est porté sur une étude détaillée sur les réseaux sans fil et leur implémentation ainsi que la configuration des différents équipements utilisés pour la résidence universitaire DIDOUCHE Mourad (ILE) de Tizi-Ouzou, en collaboration avec Algérie Telecom.

Il est indispensable de configurer son réseau de façon sécurisée. Cette étape comprend la configuration des différents équipements mais également l'audit périodique et la surveillance continuelle de son réseau.

La sécurité est aussi un objet qu'il ne faut pas négliger, puisqu'elle joue un rôle important dans un réseau sans fil ou le support de transmission est difficile voir impossible de contrôler. Pour cela on aessayé de donner les différentes attaques contre le Wi -Fi et quelques solutions pour y remédier.

On a mis en place un réseau Wi-Fi en mode infrastructure qui nécessite des points d'accès avec un nouveau matériel qui est le contrôleur C1000 qui supporte au maximum 200 points d'accès, alimentation redondante et ports Gigabit Ethernet Localisé à n'importe quel endroit du réseau.

Notre projet est composé de deux parties planifiées comme suit :

Dans la première partie

Le premier chapitre présente des généralités sur les réseaux sans fil ainsi qu'un aperçu sur le standard IEEE 802.11, la technologie la plus utilisée aujourd'hui comme interface sans fil pour échanger des données, nous finirons par les équipements utilisés lors d'installation d'un réseau sans fil.

Le deuxième chapitre, on a décrit les protocoles et leur mode de fonctionnement. L'utilisation de plusieurs protocoles de sécurité et d'authentification que nous examinons en détail dans les sections suivantes de ce chapitre. Plusieurs termes et protocoles seront abordés, en spécifiant les protocoles utilisés dans notre partie pratique qui son RADIUS et DHCP.

Le troisième chapitre expose le problème de sécurité dans un réseau sans fil, en commençant par citer les attaques contre ce standard et enfin nous énumérons les différentes solutions proposées pour faire face à ces attaques.

Dans la Deuxième partie

Le premier chapitre est consacré à l'étude avant installation du réseau tel qu'étudier le lieu, l'architecture utilisée, les différents équipements et leurs installations. Et on le termine par un schéma récapitulatif sur l'emplacement de ces différents équipements installés sur le site ainsi que l'inventaire de ces derniers.

Le deuxième chapitre illustre une configuration d'un réseau sans fil en mode infrastructure où on a configuré le contrôleur c1000, les points d'accès ainsi que le serveur DHCP et les Scalences.

Nous finirons ce thème par une conclusion générale et une bibliographie.

Présentation de l’organisme d’accueil

I - Présentation de l'organisme d'accueil

I.1 Présentation d'Algérie Telecom

Algérie Telecom est leader sur le marché Algérien des télécommunications qui connait une forte croissance. Offrant une gamme complète de services de voix et de données aux clients résidentiels et professionnels.
Cette position s'est construite par une politique d'innovation forte adaptée aux attentes des clients et orientée vers les nouveaux usages.

Algérie Telecom, est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques.

Sa naissance a été consacrée par la loi 2000/03 du 5 août 2000, relative à la restructuration du secteur des Postes et Télécommunications, qui sépare notamment les activités Postales de celles des Télécommunications

ALGERIE TELECOM est donc régie par cette loi qui lui confère le statut d'une entreprise publique économique sous la forme juridique d'une société par actions SPA.

I.2 Objectifs principaux d'Algérie Telecom

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs:
- Rentabilité
- Efficacité
- Qualité de service

Son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel.
Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie.

I.3 Missions essentielles d'Algérie Telecom

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles…
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications.
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

Algérie Telecom est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales.
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications.
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.

I.4 Organisation d'Algérie Télécom

ALGERIE TELECOM est organisée en Divisions, Directions Centrales, et Régionales, a cette structure s'ajoutent deux filiales:
- Mobile (Mobilis)
- Télécommunications Spatiales (RevSat)

ALGERIE TELECOM s'implique dans le développement socio-économique du pays a travers la fourniture des services de télécommunications.
En outre, ALGERIE TELECOM met en œuvre des moyens importants pour rattacher les localités isolées et les établissements scolaires.

Le Marketing et l'action commerciale pour réhabiliter l'image de marque d'ALGERIE TELECOM et fidéliser sa clientèle, notamment par la mise en place du système informatique « GAIA » qui permet :

1 - Le client aura un guichet unique au niveau de l'ACTEL, qui saisit la demande du client, ses coordonnées, l'adresse, etc… ;
2 - La suppression de l'échange de papier entre les services techniques du CECLI et l'Actel "gestion zéro papier" ;
3 - Permettre aux clients de consulter leurs factures à travers l'Internet.

Chapitre I :
Les réseaux sans fil

I .1- Introduction :

Les réseaux existent depuis longtemps, destinés à transporter l'information, ils peuvent être classés en trois catégories principales, selon le type et l'origine de cette information :

- Ø Réseaux téléphoniques des opérateurs de télécommunications.
- Ø Réseaux informatiques nés de posemètre de communique des ordinateurs.
- Ø Réseaux de diffusion acheminant les programmes audiovisuels.

Chacune de ces catégories présentes des caractéristiques liées aux applications téléphone, informatique, et de vidéo transportées par les différents réseaux.

I .2- Définition d'un réseau :

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.

Le terme réseau en fonction de son contexte peut designer plusieurs paramètres :

- désigne l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qu'est le cas lorsqu'on parle de l'Internet.
- décrire la façon dont les machines d'un site sont interconnectées.
- spécifier les protocoles qui sont utilisés pour que les machines communiquent(en parlant de réseau TCP/IP).

I.3 -Le modèle de référence OSI de ISO :

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocole privés, mais il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux si une norme internationale n'était pas établie.

Cette norme établie par l'internationale standard organisation (ISO) est la norme open system interconnexion (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipement hétérogènes et issus de constructeurs différents.

Le premier objectif de la norme OSI était de définir un modèle de toute architecture de réseau basé sur un découpage en sept couches. Chacune de ces couches correspond à une fonctionnalité particulière d'un réseau.

Les couches 1, 2,3 et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes.

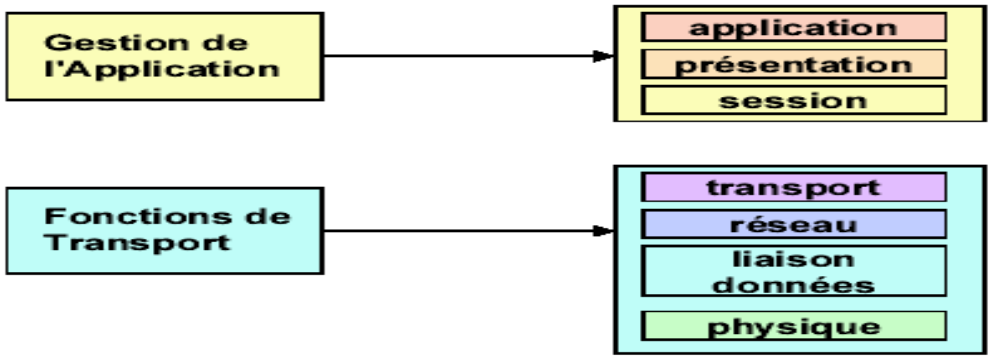


Figure I.1 : Le modèle OSI

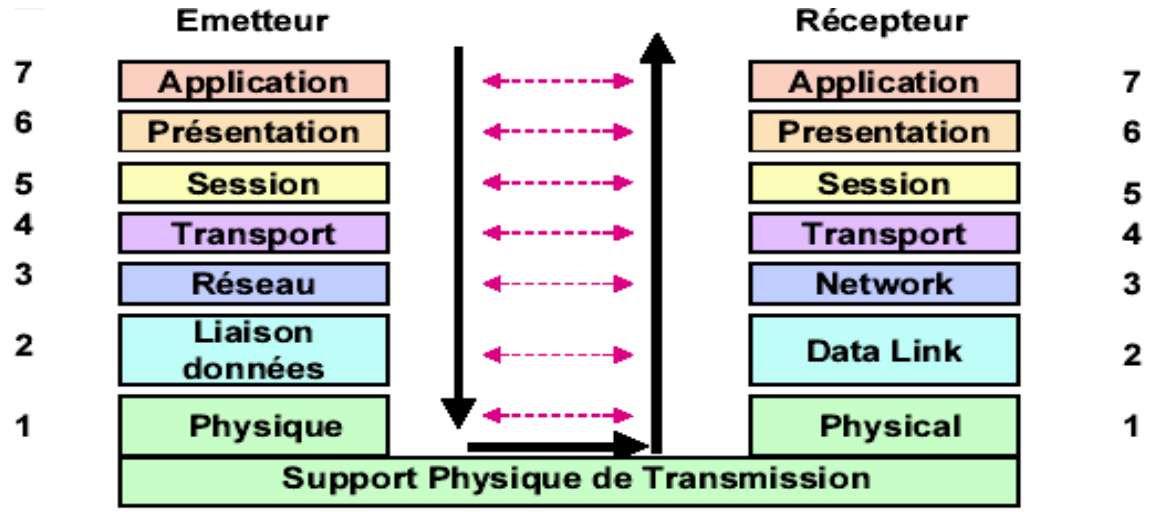


Figure I.2 : Les couches OSI

I.3.1 -La couche physique :

Cette couche définit les caractéristiques techniques, électriques, fonctionnelles et les procédures nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de la liaison de données.

I.3.2 -La couche liaison :

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique. Elle signale aussi à la couche réseau les erreurs irrécupérables.

I.3.3 -La couche réseau :

Cette couche assure toutes les fonctionnalités de service entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

I.3.4 -La couche transport :

Cette couche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).

Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requises par la couche session.

I.3.5 -La couche session :

Cette couche fournit aux entités de la couche présentation, les moyens d'organiser et de synchroniser les dialogues et les échanges de données.

Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

I.3.6 -La couche présentation :

Cette couche assure la transparence du format des données à la couche application.

I.3.7 -La couche application :

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisables par l'application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

I.4- Le protocole TCP/IP :

I.4.1- Introduction :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol).

Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

I.4.2 -Description du modèle :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

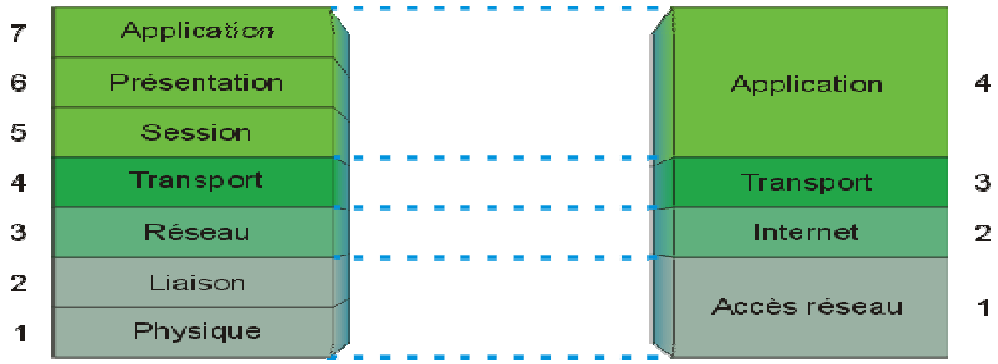


Figure I.3 : Le model TCP/IP et le model OSI

Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles. Il y a 4 couches principales dans l'environnement TCP/IP :

- La couche application : les applications interagissent avec les protocoles de la couche Transport pour envoyer ou recevoir des données.

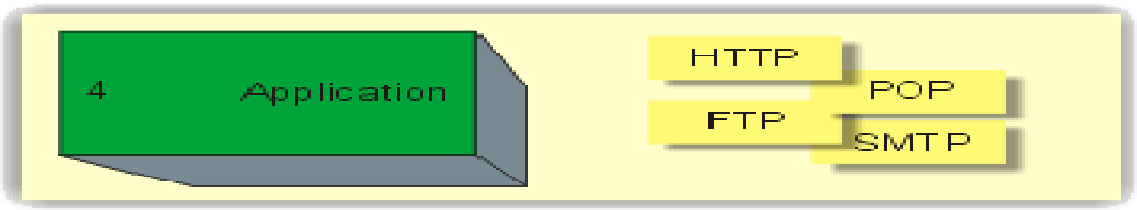


Figure I.4 : La couche application

- La couche transport : chargée de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agit en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.

Figure I.5 : La couche transport

- La couche Internet : encapsule les paquets reçus de la couche Transport dans des datagrammes IP. Mode non connecté et non fiable.

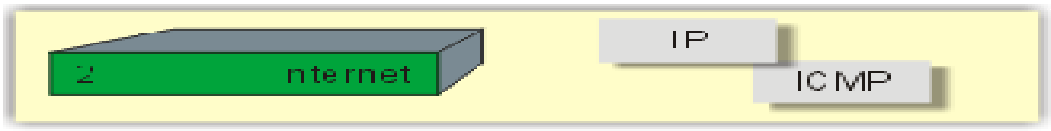


Figure I.6 : La couche internet

- La couche Hôte Réseau : assure la transmission d'un datagramme venant de la couche IP en l'encapsulant dans une trame physique et en transmettant cette dernière sur un réseau physique.

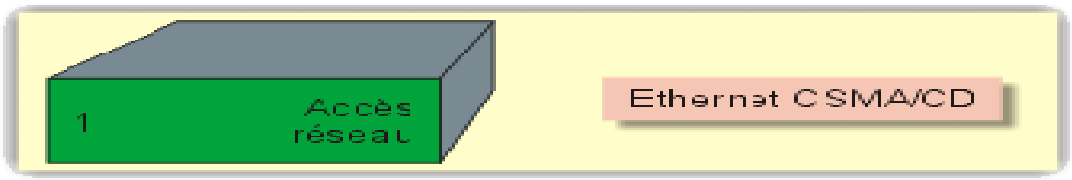


Figure I.7 : La couche réseau

I.4.3 -Les différentes classes d'adresses IP :

L'Internet est donc un réseau basé sur un ensemble de protocoles : les protocoles de la famille TCP/IP. La version actuelle est nommée IPV4 (version 4).

Pour localiser les machines, on fait usage d'adresses. Ces dernières sont utilisées à de nombreux niveaux dans les paquets qui transitent sur le réseau.

Les adresses IP peuvent donc être représentées sur 32 bits. Ces 32 bits sont séparés en deux zones de bits adjacentes :

- Network ID : une partie décrit le numéro du réseau local auquel est rattachée la station.
- Host ID : une partie correspond au numéro de la station dans le réseau local lui-même, appelée numéro d'hôte.

Selon l'adresse IP on définit différentes classes d'adresses. Il existe cinq classes d'adresses avec la version 4 (version courante) des protocoles TCP/IP, car les parties réseau et hôte n'ont pas toujours la même taille.

a)-Les adresses de la classe A

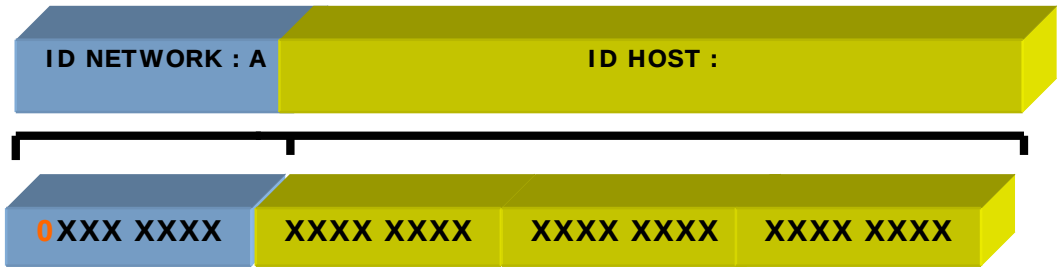


Figure I.8 : format d'adresse de la classe A

b) -Les adresses de la classe B

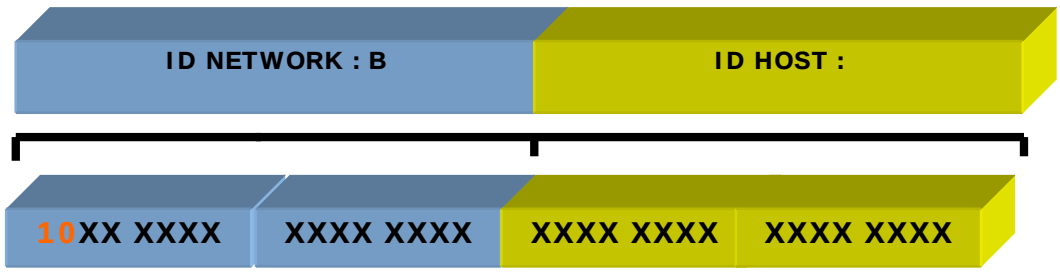


Figure I.9 : format d'adresse de la classe B

c) -Les adresses de la classe C

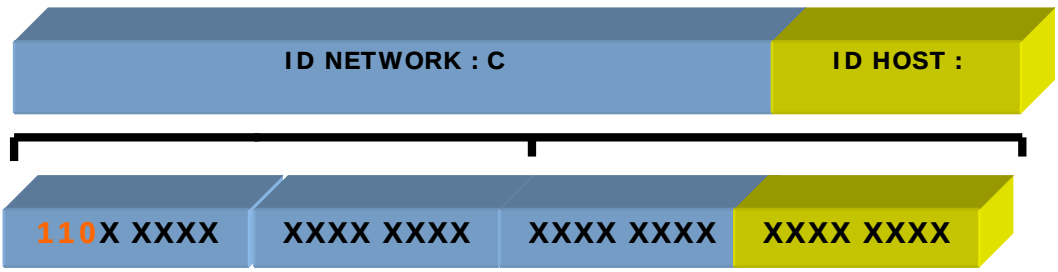


Figure I.10 : format d'adresse de la classe C

d) -Les adresses de la classe D :

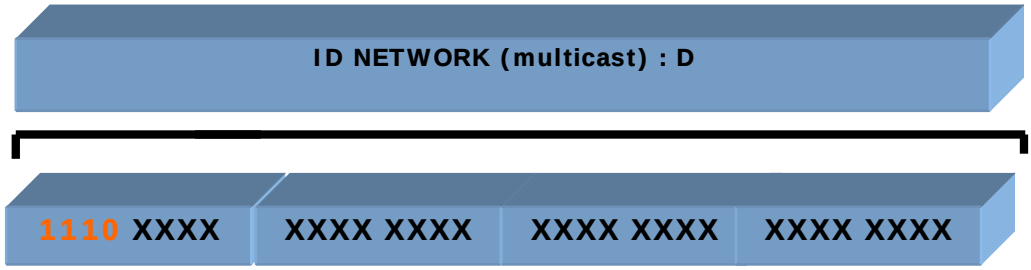


Figure I.11 : format d'adresse de la classe D

e) -Les adresses de la classe E

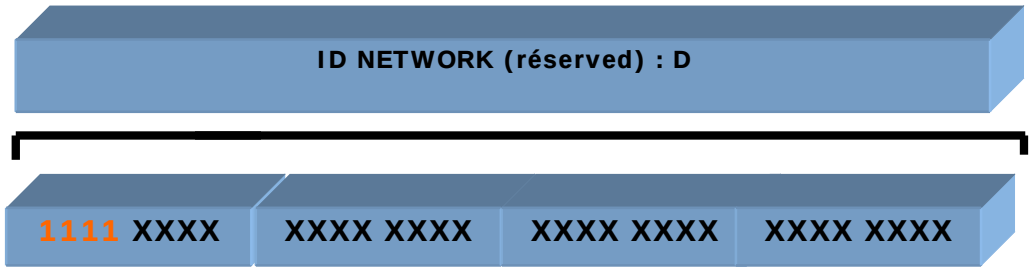


Figure I.12 : format d'adresse de la classe E

II.1 Définition des réseaux sans fil

Un réseau sans fil (en anglais *wireless network*) est un réseau dans lequel plusieurs terminaux communiquent sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) à la place de câble. Il existe plusieurs technologies que nous allons voir.

Elles se différencient par la fréquence d'émission utilisée, le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier des ordinateurs de quelques centimètres à plusieurs kilomètres.

Avec l'installation et l'utilisation d'un réseau sans fil il se pose le problème de la réglementation relative aux transmissions radio-électriques. En effet, les transmissions radio-électriques servent pour un grand nombre d'applications (militaires, scientifiques, amateurs, ...), et sont sensibles aux interférences, c'est la raison pour laquelle une réglementation est nécessaire dans chaque pays afin de définir les plages de fréquence et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation.

De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc possible pour un pirate de repérer et d'écouter un réseau.

Les informations transmises sur un réseau sans fil circulent en clair (c'est le cas par défaut). Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil.

II.2- Utilisation du Wi-Fi :

De nos jours les réseaux sans fil se développent très rapidement :

- pour des réseaux temporaires (salons, conférences, ...) ;
- pour des points d'accès haut débit dans les lieux publics (aéroports, gares, métros, ...) connus sous le nom de hotspot ou des lieux privés accueillant du public (hôtel, restaurant, ...) ;
- dans de nombreux organismes attirés par la souplesse des réseaux sans fil.

II.3-Fonctionnement du Wi-Fi

Un réseau sans fil est fondé sur une architecture cellulaire où chaque cellule appelée BSS (Basic Service Set) est contrôlée par un AP (Access Point) ou point d'accès, le tout formant un réseau appelé ESS (Extended Service Set). Ce mode de communication est appelé le mode infrastructure. Les points d'accès peuvent être reliés entre eux par des liaisons radio ou filaires et un terminal peut alors passer d'un point d'accès à un autre en restant sur le même réseau (concept du roaming).

Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil utilisent un identifiant de réseau (SSID).

Un point d'accès sur un réseau sans fil équivaut à un concentrateur (hub) sur un réseau filaire. Chaque terminal sans fil reçoit donc tout le trafic circulant sur le réseau. Si ce terminal scrute simultanément plusieurs canaux, il recevra alors le trafic de tous les réseaux qui l'entourent.

Le mode de communication ad-hoc est également disponible ; il s'agit d'un mode point à point entre des équipements sans fil. Avec ce mode de fonctionnement, il est possible d'utiliser des protocoles de routage proactifs (échange périodique des tables de routage pour la détermination des routes) ou des protocoles de routage réactifs (les routes sont établies à la demande) afin de reconstituer un réseau maillé.

II.4- Les avantages du Wi-Fi

Comme les autres réseaux sans fil, le Wi-Fi possède plusieurs avantages :

- **la facilité de déploiement** : un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- **le faible coût d'acquisition :** si leur installation est parfois un peu plus coûteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits ; sur le moyen terme, l'investissement est facilement rentabilisé.

- **la mobilité** : les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil et de ce fait sont plus enclins à utiliser le matériel informatique.

- **la simplification de la gestion :** L'ajout de nouveaux élément ou le déplacement d'éléments existants peuvent être réalisés rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

De plus, le Wi-Fi est interopérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

II.5 -Les inconvénients du Wi-Fi

- **Qualité et continuité du signal :** ces notions ne sont pas garanties du fait des problèmes pouvant venir des interférences, du matériel et de l'environnement.

- **Sécurité :** la sécurité des réseaux sans fil n'est pas encore tout à fait fiable du fait que cette technologie est novatrice.

II.6-Présentation des différents réseaux sans fil

En raison de leur facilité de déploiement et de leur coût relativement faible, les réseaux sans fil sont de plus en plus utilisés. Comme pour les réseaux filaires, on classe généralement les réseaux sans fil selon leur domaine de couverture : les réseaux personnels WPAN (Wireless Personal Area Networks), les réseaux locaux WLAN (Wireless Local Area Networks), les réseaux métropolitains WMAN (Wireless Métropolitain Area Networks) et les réseaux nationaux WWAN (Wireless Wide Area Networks).

II.6.1- Les réseaux sans fil de type WPAN

Les WPAN sont des réseaux sans fil de faible portée (quelques dizaines de mètres) qui, tel que leur nom l'indique, sont des réseaux à usage personnel. Ils sont déjà présents sous différents noms :

- **Bluetooth :** nom commercial de la norme IEEE 802.15.1, Bluetooth est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30 mètres, Bluetooth offre de nombreuses possibilités grâce à la faible consommation de ses équipements. On trouve des composants Bluetooth dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photo, téléphones portables, assistants personnels, ...). La norme IEEE 802.15.3 (Bluetooth2) est une évolution de la norme Bluetooth permettant des débits plus rapides et intégrants des mécanismes de sécurité très limités dans le protocole Bluetooth.

- **ZigBee :** avec un débit plus faible que Bluetooth, la norme IEEE 802.15.4 (ZigBee) pourrait être très utilisée dans les années à venir. Les équipements ZigBee moins consommateurs et moins onéreux que les équipements Bluetooth devraient trouver leur place dans les périphériques informatiques mais également en domotique (éclairage, système de sécurité, ...).

- **Les liaisons infrarouges :** elles sont majoritairement utilisées pour des communications courte distance, cependant leur sensibilité aux perturbations empêche le développement de cette technologie dans les réseaux sans fil supérieurs à une distance d'une dizaine de mètres. Néanmoins, la portée d'interception peut-être très supérieure.

II.6.2- Les réseaux sans fil de type WLAN (norme IEEE 802.11)

La norme IEEE 802.11 est un standard qui décrit les caractéristiques des réseaux sans fil et qui est équivalente à la norme IEEE 802.3 (Ethernet) pour les réseaux filaires.

La norme IEEE 802.11 est la norme initiale à partir de laquelle un certain nombre de normes dérivées ont été crées afin de répondre à des objectifs de sécurité. Les normes dérivées les plus connues aujourd'hui sont les normes IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11i, et IEEE 802.11n.

II.6.3- Les réseaux sans fil de type WMAN (norme IEEE 802.16)

La B.L.R. (Boucle Locale Radio) fait partie des réseaux sans fil de type WMAN. La BLR est une technologie sans fil capable de relier les opérateurs à leurs clients grâce aux ondes radio sur des distances de plusieurs kilomètres.

Les réseaux sans fil de type WMAN sont en train de se développer. Ce phénomène risque de s'amplifier dans les années à venir. La norme IEEE 802.16, est plus connue sous son nom commercial WiMax.

Comme dans le cas de la dénomination Wi-Fi, WiMax désigne en fait un ensemble de normes regroupées sous une appellation commune.

Techniquement, le WiMax permet des débits d'ordre de 70Mb/s avec une portée d'ordre de 50km. Actuellement, le WiMax peut exploiter les bandes de fréquence 2.4Ghz, 3.5Ghz et 5.8Ghz.

II.6.4-Les réseaux sans fil de type WWAN

Bien que ces réseaux ne soient pas connus sous ce nom, ce sont aujourd'hui les réseaux sans fil les plus utilisés. Les technologies cellulaires tel que le GSM (Global System for Mobile Communication), le GPRS (General Packet Radio Service) et l'UMTS (Universal Mobile Telecommunication System) font ou feront partie de ce type de réseau.

II.7- La technologie 802.11

II.7.1- La sous-couche LLC 802.11 :

La couche LLC a été définie par le standard IEEE 802.2. Cette couche permet d'établir un lien logique entre la couche MAC et la couche de niveau 3 du modèle OSI, la couche réseau. Ce lien se fait par l'intermédiaire du Logical Service Access Point (LSAP).

La couche LLC fournit deux types de fonctionnalités :

- un système de contrôle de flux;
- un système de reprise après erreur.

La trame LLC contient une adresse en en-tête ainsi qu'une zone de détection d'erreur en fin de trame: le forward error correction (FEC).

Son rôle principal réside dans son système d'adressage logique, qui permet de masquer aux couches hautes les informations provenant des couches basses. Cela permet de rendre interopérables des réseaux complètement différents dans la conception de la couche physique ou de la couche MAC possédant la couche LLC.

Il existe trois types de LLC définis :

- LLC de type 1 : correspond à un service en mode sans connexion sans acquittement de données. Elle offre un service non fiable mais qui est largement répandu actuellement.
- LLC de type 2 : correspond à un service en mode avec connexion avec acquittement de données.
- LLC de type 3 : correspond à un service en mode sans connexion avec acquittement de données.

II.7.2- La sous-couche MAC 802.11 :

Nous savons maintenant comment les stations 802.11 se partagent l'accès au réseau [22]sans fil. Voyons à présent comment les stations 802.11 choisissent un AP et communiquent avec lui et comment fonctionne le mode d'économie d'énergie.
Voici les trois échanges requis entre une station est un AP pour communiquer:

• Le processus de **sondage**, ou probe;
• Le processus d'**authentification**;
• Le processus d'**association**.

Le processus de sondage, consiste généralement, à émettre une trame de requête probe sur chaque canal. Cette trame contient notamment des informations sur la station émettrice (les plus importantes sont les débits supportés (**IE Supported Rates** et l'ensemble de services auquel elle appartient (**IE SSID**)). Ce processus à pour but de permettre à la station de connaître les APs qui se trouvent à proximité.

Lorsque la station reçoit les trames de réponse probe des APs, elle peut, suivant la configuration, se connecter automatiquement à un AP ou alors attendre la décision de l'utilisateur de la station.

Le processus d'authentification est très important dans les WLAN, il permet de déterminer celui qui est autorisé à accéder au réseau. Le standard 802.11 possède deux modes différents: Open System et Shared Key. En résumé, la station envoie une requête d'authentification et l'AP lui renvoie une réponse d'authentification.

Le processus d'association autorise ou non un AP à assigner un port logique à la station sans fil. Il est initié par la station au moyen d'une trame de requête et se termine par une réponse de l'AP lui indiquant le succès ou l'échec.

Une des fonctions intéressantes de la sous-couche MAC 802.11, est l'économie d'énergie. Le principe est simple; la station désactive son dispositif sans fil. L'AP auquel elle est associée met alors les trames destinées à la station dans un tampon. À intervalles réguliers, la station réactive le dispositif radio et attend l'arrivée d'une trame d'AP lui indiquant la présence de trames à son intention. Un intervalle d'écoute ou de réveil est défini par le client.

II. 7.3- La couche physique 802.11 :

La couche physique (couche 1 du modèle OSI) est chargée de gérer les connexions matérielles. Elle est divisée en deux parties: **PLCP** (*Physical Layer Convergence Protocol*) et **PMD** (*Physical Medium Dependant*).
L'encapsulation des informations fournies par la couche liaison de données est réalisée par la sous-couche PMD grâce à deux méthodes:

Il faut, en premier lieu, choisir une méthode de transmission des informations, puis une méthode de codage.

Pour que les stations puissent communiquer entre elles, le standard 802.11 définit trois couches physiques:

• **Le FHSS** (*Frenquency Hopping Spread Spectrum*)
• **Le DSSS** (*Direct Sequence Spread Spectrum*)
• **L'IR** (*Infra-Red*) que nous ne détaillerons pas.

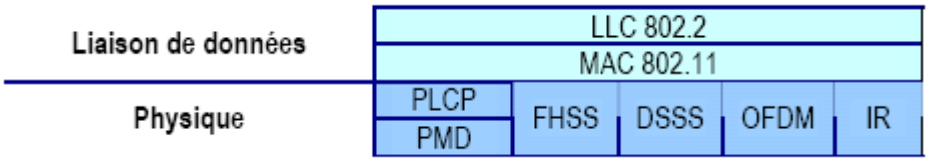


Figure I.13 : Modèle IEEE 802.11

II.8- Les différentes normes IEEE 802.11 :

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbit/s. Des révisions ont été apportées à la norme originale afin d'améliorer le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11n appelées normes 802.11 physiques) ou de spécifier des détails de sécurité ou d'interopérabilité.

Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification **(tableau 1)** :

Norme	**Nom**	**Description**
802.11a	Wi-Fi 5	La norme 802.11a (baptisée *Wi-Fi 5*) permet d'obtenir un haut débit (dans un rayon de 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels). La norme 802.11a spécifie 52 canaux de sous-porteuses radio dans la bande de fréquences des 5 GHz (bande U-NII = Unlicensed - National Information Infrastructure), huit combinaisons, non superposées sont utilisables pour le canal principal.

802.11b	Wi-Fi	La norme 802.11b est la plus répandue en base installée actuellement. Elle propose un débit théorique de 11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu'à 300 mètres (en théorie) dans un environnement dégagé. La plage de fréquences utilisée est la bande des 2,4 GHz (Bande ISM = Industrial Scientific Medical) avec, en France, 13 canaux radio disponibles dont 3 au maximum nonK superposés (1 - 6 - 11,1 - 7 – 13)
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi, cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance	La norme 802.11f est une recommandation à l'intention des vendeurs de points d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming Protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (roaming).
802.11g		La norme 802.11g est la plus répandue dans le commerce actuellement. Elle offre un haut débit (54 Mbit/s théoriques, 25 Mbit/s réels) sur la bande de fréquences des 2,4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. Cette aptitude permet aux nouveaux équipements de proposer le 802.11g tout en restant compatibles avec les réseaux existants qui sont souvent encore en 802.11b. Le principe est le même que celui de la norme 802.11a puisqu'on utilise ici 52 canaux de sous-porteuses radio mais cette fois dans la bande de fréquences des 2,4 GHz. Ces sous-porteuses permettent une modulation OFDM autorisant de plus haut débit que les modulations classiques BPSk, QPSK ou QAM utilisé par la norme 802.11g. Cette modulation OFDM étant interne à l'une des 14 bandes 20MHz possibles, il est donc toujours possible d'utiliser

802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (Hiperlan 2, d'où le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie.
802.11i		La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les standards 802.11a, 802.11b et 802.11g.
802.11IR		La norme *802.11IR* a été élaborée de manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.
802.11n	WWiSE (World Wide Spectrum Efficiency) ou TGn Sync	La norme *802.11n* est disponible depuis le 11 septembre 2009. Le débit théorique atteint les 300 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 100 mètres) grâce aux technologies MIMO (Multiple-Input Multiple-Output) et OFDM (Orthogonal Frequency Division Multiplexing). En avril2006, des périphériques à la norme 802.11n commencent à apparaître basés sur le *Draft 1.0* (brouillon 1.0) ; le *Draft 2.0* est sorti en mars 2007, les périphériques basés sur ce brouillon seraient compatibles avec la version finale du standard. Des équipements qualifiés de «pré-N» sont disponibles depuis 2006 : ce sont des équipements qui mettent en œuvre une technique MIMO d'une façon propriétaire, sans rapport avec la norme 802.11n. Le *802.11n* a été conçu pour pouvoir utiliser les fréquences 2,4 GHz ou 5 GHz. Les premiers adaptateurs 802.11n actuellement disponibles sont généralement simple-bande à 2,4 GHz mais des adaptateurs double-bande (2,4 GHz ou 5 GHz au choix) ou même double-radio (2,4 GHz et 5 GHz simultanément) sont également disponibles. Le 802.11n saura combiner jusqu'à 8 canaux non superposés, ce qui permettra en théorie d'atteindre une capacité totale effective de presque un gigabit par seconde.
802.11s	Réseau Mesh	La norme *802.11s* est actuellement en cours d'élaboration. Le débit théorique atteint aujourd'hui 10 à 20 Mbit/s. Elle vise à implémenter la mobilité sur les réseaux de type Ad-Hoc. Tout point qui reçoit le signal est capable de le retransmettre. Elle constitue ainsi une toile au-dessus du réseau existant. Un des protocoles utilisé pour mettre en œuvre son routage est OLSR.

II.9- Les topologies des réseaux sans fil :

Un réseau sans fil est fondé sur deux types de topologie à savoir:

II.9.1- **Le mode Infrastructure :**

Le mode infrastructure est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès qui agissent comme des concentrateurs.

Autrefois, ce mode était essentiellement utilisé en entreprise. Dans ce cas la mise en place d'un tel réseau oblige de poser à intervalle régulier des bornes dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID : Service Set IDentifier) afin de pouvoir communiquer. L'avantage de ce mode, en entreprise, est de garantir un passage obligé par le AP, il est donc possible de vérifier qui accède au réseau. En revanche, le réseau ne peut pas s'agrandir, hormis en posant de nouvelles bornes.

Actuellement les FAI, les boutiques spécialisées et les grandes surfaces fournissent aux particuliers des routeurs sans fil qui fonctionnent en mode Infrastructure, tout en étant très facile à configurer.

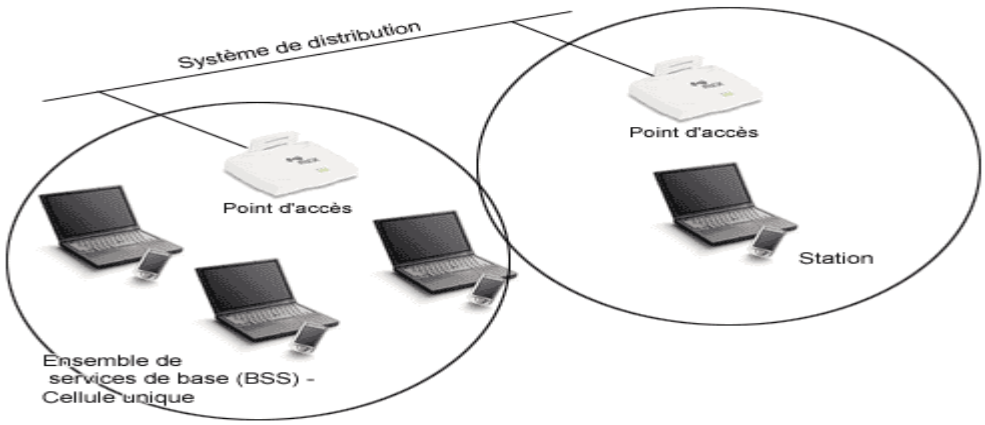


Figure I.14 : Mode infrastructure

II.9.2- **Le mode Ad Hoc :**

Le mode Ad Hoc est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire. La mise en place d'un tel réseau se borne à configurer les machines en mode Ad Hoc (au lieu du mode Infrastructure), la sélection d'un canal (fréquence), d'un nom de

réseau (SSID) communs à tous et si nécessaire d'une clé de cryptage. L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de points d'accès. Des protocoles de routage dynamique rendent envisageable l'utilisation de réseaux maillés autonomes dans lesquels la portée ne se limite pas à ses voisins.

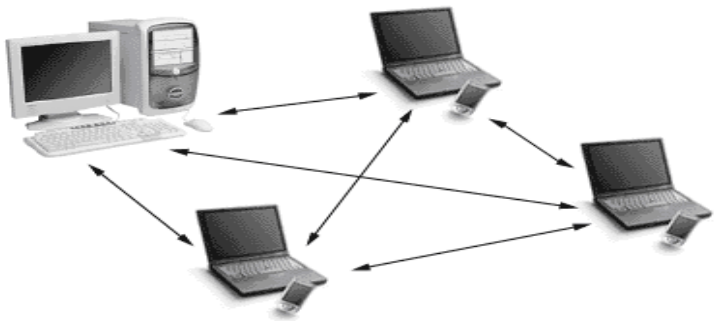


Figure I.15: Mode ad-hoc

II.10- Le SSID :

SSID est une abréviation de Service Set Identifier, un identificateur unique pour éviter les interférences sur un réseau sans fil, et il se réfère aussi à ESSID (Extended Service Set Identifier). Le SSID est une valeur de 32 bits ou moins et il est assigné au point d'accès. L'appareil réseau sans fil que vous désirez associer au réseau sans fil doit correspondre au point d'accès.

Le point d'accès et les appareils réseau sans fil envoient régulièrement des paquets d'informations (référées en tant que beacon), qui contiennent l'information SSID. Lorsque votre appareil réseau sans fil reçoit un beacon, vous pouvez identifier le réseau sans fil qui est suffisamment proche des ondes radio afin de pouvoir atteindre votre appareil.

II.11- Présentation du matériel :

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil WIFI :

II. 11.1 Les adaptateurs sans fil ou carte d'accès :

Les adaptateurs sans fil ou cartes d'accès (en anglais *wireless adapters* ou *network interface controller*) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wifi sont disponibles dans de nombreux

formats (carte PCI, carte PCMCIA, adaptateur USB, carte compactflash, ...). On appelle station tout équipement possédant une telle carte.

Fig. I.16 : Adaptateurs sans fil

II. 11.2 Les points d'accès :

Un point d'accès Wifi est un équipement réseau qui permet à votre ordinateur de se connecter sur le réseau sans fil. Il possède une antenne radio supportant les normes 802.11b et 802.11g, il joue le rôle de passerelle entre le réseau sans fil et le réseau filaire.

Fig. I.17 : Point d'accès

II. 11.2 Contrôleur :

HiPath wireless Controller est un routeur complet de couche 3 qui rassemble et coordonne tous les points d'accès afin de former des sous-réseaux IP gérés centralement et visibles au reste durés eau.

Par conséquent, la gestion réseau est considérablement simplifiée, car il n'est plus nécessaire de visiter physiquement les points d'accès distants. En outre, le contrôleur fonctionne à une vitesse filaire pour un débit maximum.

Le contrôleur sans fil gère également l'authentification et la sécurité des utilisateurs, la détection des AP sauvages, le roaming transparent des utilisateurs sur le réseau sans fil, la gestion avancée des fréquences radio et la segmentation des politiques utilisateurs, notamment la gestion de la qualité de service et les autorisations d'application.

Il est capable de gérer un maximum de 200 points d'accès.

Les contrôleurs sont disponibles en différentes configurations pour différentes capacités de déploiement.

Le contrôleur C10 => supporte au maximum 30 points d'accès, alimentation unique et ports Fast Ethernet

Le contrôleur C100 => supporte au maximum 75 points d'accès, alimentation redondante et ports Fast Ethernet
Le contrôleur C1000 => supporte au maximum 200 points d'accès, alimentation redondante et ports Gigabit Ethernet Localisé à n'importe quel endroit du réseau, le contrôleur gère de façon centralisée les différents points d'accès quelque soient les sous-réseaux IP de votre réseau LAN. Outre les fonctions de redondance, comme les alimentations redondantes et la présence de plusieurs ports de données, les contrôleurs peuvent être déployés par paires, de sorte que les fonctions du contrôleur primaire puissent être reprises par un contrôleur secondaire en cas de défaillance.

Fig. I.18 : Le Contrôleur

II. 11.3 **Switch :**

C'est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permettent de créer des circuits virtuels. La commutation est l'un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage. Dans les réseaux locaux (LAN), il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub). Il existe aussi des commutateurs pour tous les types de réseau en mode point à point.

Fig. I.19: Le Switch

II. 11.4 Hub:

Le hub est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports. Il présente les mêmes inconvénients que le répéteur. Il assure en fonction annexe une auto-négociation du débit entre 10 et 100 Mbits/s, il est utilisé en extrémité du réseau et doit être couplé en un nombre maximum de 4 entre deux stations de travail.

Fig. I.20: Le hub

II. 11.5 Scalence :

Les points d'accès SCALANCE sont utilisés pour construire le réseau sans fil et fournir à ses clients l'accès à la radio, par exemple, SCALANCE clients, les appareils sans fil ou les ordinateurs portables. Pour les grandes infrastructures, plusieurs points d'accès couvrent le réseau sans fil et aussi soutenir la transition en douceur des clients entre les points d'accès. Selon la version du produit, ils peuvent être utilisés soit en tant que points d'accès à l'intérieur ou à l'extérieur.

Avec des points d'accès SCALANCE toutes les données de configuration peuvent être sauvegardées sur une option C-Plug. Dans le cas d'un défaut, cette fiche de configuration peut être simplement insérée dans un dispositif de nouveau sans la nécessité de reconfigurer le dispositif.

Fig. I.21: Le Scalence

II. 11.6 Câbles :

- Fibre optique :

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestre et océanique de données. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et supports. Un réseau « large band » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longe distance et à des débits jusqu'alors impossible, les fibres optiques ont constitué l'un des éléments clef de la révolution des télécommunications optiques. Ses propriétés sont également exploitées dans le domaine des capteurs (température, pression, etc.) et dans l'imagerie.

Un nouveau type de fibre optique , fibres à cristaux photoniques, a également été mis au point ces dernières années, permettant des gains significatifs de performances dans le domaine du traitement optique de l'information par des techniques non linéaires, dans l'amplification optique ou bien encore dans la génération de super continus utilisables par exemple dans le diagnostic médical.Dans les réseaux informatiques de type Ethernet, pour la relier à d'autres équipement, on peut utiliser un émetteur-récepteur.

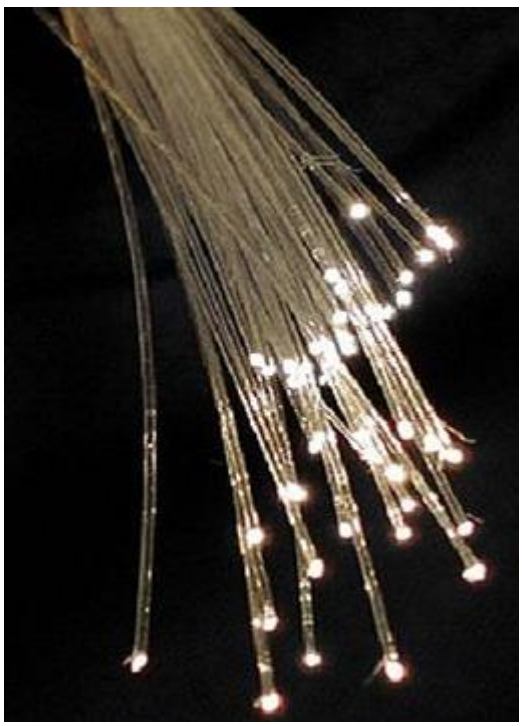


Fig. I.22: câble optique

- FTP :

FTP (Foiled Twisted Pair) également d'impédance 100 ohms et écranté ; Il est constitué d'un simple feuillard d'aluminium enroulant les quatre paires torsadées protégées par une gaine externe.

Fig. I.23: câble FTP

-paires torsadées :

Un câble paires torsadées décrit un modèle de câblage où une ligne de transmission est formée de deux conducteurs enroulés en hélice l'un autour de l'autre, cette configuration à pour but de maintenir précisément la distance entre les fils et de diminuer la diaphonie.

Le maintien de la distance entre fils de paire permet de définir une impédance caractéristique de la paire, afin de supprimer les réflexions de signaux aux raccords et en bout de ligne. Les contraintes géométriques (épaisseur de l'isolant/diamètre du fil) maintiennent cette impédance autour de 100 ohm :

- 100 ohm pour les réseaux ethernet en étoile
- 100 ou bien 120 ohm pour les réseaux de téléphonie
- 90 ohm pour les câbles USB.

Plus le nombre de torsades est important, plus la diaphonie est réduite. Le nombre de torsades moyen par mètre fait partie de la spécification du câble, mais chaque paire d'un câble est torsadée de manière légèrement différente pour éviter la diaphonie. L'utilisation de la signalisation différentielle symétrique permet de réduire davantage les interférences.

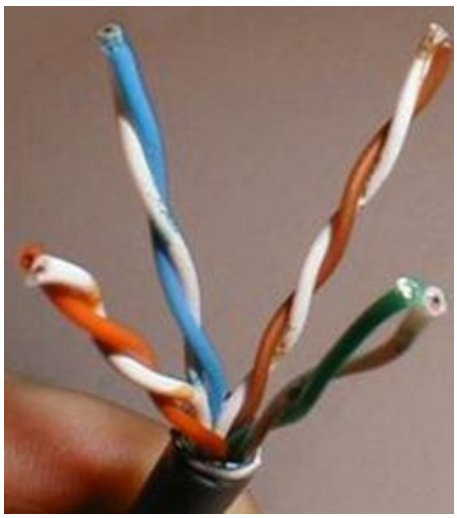


Fig. I.24: câble paires torsadées

III-Conclusion :

Les réseaux sans fil en général, et le Wi-Fi en particulier sont des technologies intéressantes et très utilisées dans de divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation (absence de câblage), la disponibilité ; Mais la sécurité dans ce domaine reste un sujet très délicat, car depuis l'utilisation de ce type de réseaux plusieurs failles ont été détectées.

Chapitre II:

Les différents Protocoles

I. Introduction :

L'accès à l'Internet se fait traditionnellement depuis le domicile, l'université, le bureau, ou les salles de conférence. Dans chacun de ces cas, la station d'accès est un équipement fixe ou éventuellement mobile dans une faible mesure (inférieur à 100 mètres pour l'Ethernet sans fil). Avec le déploiement des mobiles, il est devenu nécessaire de développer des protocoles permettant à des utilisateurs de se déplacer de réseau en réseau.
Nous présenterons les différents protocoles et serveurs qui permettent aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et d'assurer la sécurité.

II. Les protocoles AAA :

AAA signifie Authentification, Authorization, Accounting, soit authentification, autorisation et compte. La signification de ces termes est la suivante :

– Authentification : l'authentification consiste à vérifier qu'une personne/équipement est bien celle qu'elle prétend être. Ceci est généralement réalisé en utilisant un secret partagé entre l'utilisateur et le serveur mère AAAH ou à l'aide de certificats.

– Autorisation : l'autorisation consiste à permettre l'accès à certains services ou ressources. Un utilisateur peut par exemple demander à avoir une certaine bande passante. Le serveur AAA lui autorisera ou non cette demande.

– Compte : le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources. Ceci permet à un opérateur de facturer un utilisateur suivant sa consommation.
En pratique, une architecture client-serveur AAA permet de rendre l'ensemble de ces services. Les serveurs AAA dans les domaines mère et visité permettent de gérer les utilisateurs. Les clients AAA sont hébergés sur des routeurs ou sur des serveurs d'accès au réseau.

Les protocoles implémentant du AAA sont essentiellement utilisés par des opérateurs offrant des services de télécommunications à des utilisateurs. Ces protocoles leur permettent de contrôler l'accès à leurs réseaux et de connaître l'utilisation de leurs ressources. Ils peuvent ainsi facturer selon le temps de connexion ou selon la quantité d'informations téléchargées.

Ci-dessous un schéma représentant l'architecture AAA :

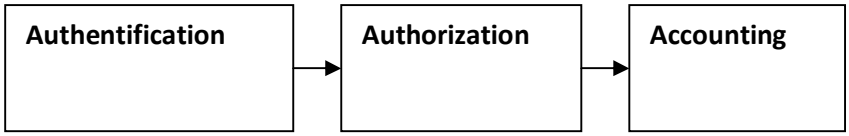


Fig. II.1: Architecture du protocole AAA.

III. RADIUS:

III.1. Description :

Le protocole RADIUS acronyme de Remote Authentication Dial-In User Service, est actuellement utilisé pour faire du AAA avec des utilisateurs qui se connecte via des modems téléphoniques à Internet. Il envoie des informations permettant de l'authentifier (login/password) au serveur d'accès. Celui ci les envoie alors à un serveur RADIUS qui se charge de l'authentifier. Si l'utilisateur est correctement authentifié, le serveur RADIUS lui permet l'accès à Internet. RADIUS a été conçu pour supporter un nombre limité d'équipements et donc un nombre limité d'utilisateurs. Actuellement, les opérateurs doivent pouvoir rendre des services et authentifier des milliers d'utilisateurs utilisant des technologies différentes. Ils doivent aussi être capables de rendre des services à des utilisateurs venant d'opérateurs différents, de préférence de façon sécurisée.

Exemples d'utilisation de RADIUS représenté ci-dessus :

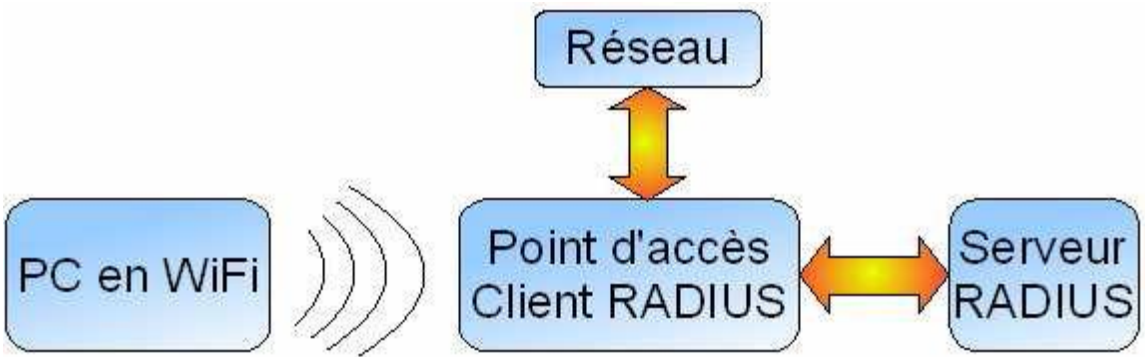


Fig. II.2: Utilisation de RADIUS

III.2. Format des paquets :

Les données sont échangées entre un client et le serveur en paquets RADIUS. En fait, un paquet RADIUS est encapsulé dans un paquet UDP (User Datagram Protocole). Chaque paquet contient les informations suivantes :

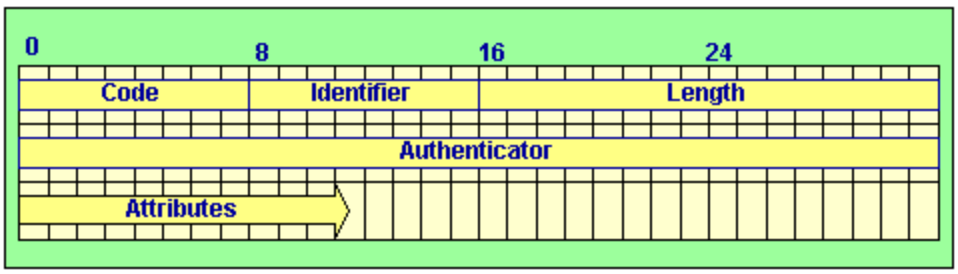


Fig. II. 3: Format d'un paquet RADIUS

Les champs d'un paquet RADIUS sont les suivants :

- Code - octet contenant la requête/réponse RADIUS
- Identifier - octet utilisé pour comparer la requête et la réponse.
- Length – longueur du paquet (2 octets).
- Authenticator - Valeur utilisée pour authentifier la réponse du serveur RADIUS, et utilisée dans l'algorithme de masquage du password.
- Attributes – les données appartenant à la requête ou à la réponse.

La communication RADIUS utilise le paradigme de requête-réponse, les requêtes sont envoyées par le client au serveur, et les réponses sont envoyées par le serveur au client.

III.3.Diagramme de séquence :

Ci-dessous un schéma d'un diagramme de séquence lorsqu'un utilisateur accède au réseau à travers un NAS (Network Access Server) et se déconnecte lui-même.

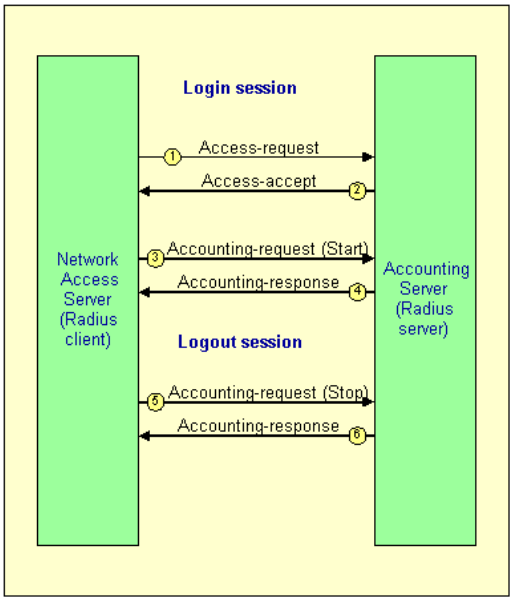


Fig. II.4: Flux de messages RADIUS.

1. Le NAS récupère le login/password d'un utilisateur à distance, crypte ces informations avec une clé partagée et envoie cela avec une "access-request" à un serveur (phase Authentification).

2. Lorsque la combinaison login/password est valide, alors le serveur RADIUS envoie un message "accept-accept" avec des informations supplémentaires (par exemple : adresse IP, masque de réseau, etc.) au NAS (phase Autorisation).

3. Le NAS envoie un message "accounting-request (start)" pour indiquer que l'utilisateur est connecté sur le réseau (phase Comptabilité).

4. Le serveur RADIUS répond avec un message “Accounting-response” lorsque l’information de comptabilité est stockée.

5. Lorsqu’un utilisateur se déconnectera, le NAS va envoyer un message ”Accounting-request (Stop)” avec les informations suivantes :

- Delay time, le temps d’essai d’envoi de ce message.
- Input octets, le nombre d’octets reçus par le client.
- Output octets, le nombre d’octets envoyés par le client.
- Session time, le nombre de secondes que le client s’est connecté.
- Input packets, le nombre de paquets reçus par le client.
- Output packets, le nombre de paquets envoyés par le client.
- Reason, la raison pour laquelle le client s’est déconnecté.

6. Le serveur RADIUS répond avec un message “accounting-response” lorsque l’information de comptabilité est stockée.

IV. DIAMETER :

IV. 1 Description :

Contrairement à RADIUS, le nom du protocole DIAMETER est un jeu de mot, signifiant diamètre en anglais, qui est le double du rayon (radius en anglais).
Le protocole DIAMETER successeur du protocole RADIUS est un protocole AAA. Il permet aux opérateurs d’authentifier des utilisateurs, de leur autoriser certains services et de collecter des informations sur l’utilisation des ressources. Il s’agit du protocole le plus à même de satisfaire les nouveaux besoins suscités par la mobilité. En particulier, il permet aux opérateurs d’authentifier un utilisateur ayant souscrit un abonnement auprès d’un autre opérateur.

Il est constitué d’un protocole de base qui définit le format des messages, comment ils sont transportés, les messages d’erreurs ainsi que les services de sécurité que toutes les implémentations doivent supporter. À ce protocole de base s’ajoutent les applications : Mobile IP, NAS et CMS.

- L’application Diameter Mobile IPv4 permet de faire du AAA avec un utilisateur utilisant Mobile IPv4 ;
- L’application Diameter NAS permet l’accès au réseau, il s’agit de l’amélioration de RADIUS ;
- L’application Diameter CMS permet de protéger les échanges Diameter au niveau applicatif entre serveurs ou entre un serveur et son client.

Diameter a été conçu dans l’idée d’être facilement extensible. Pour cette raison, le protocole de base est séparé de ses applications.

IV.2 Diagramme de séquence :

Le schéma ci-dessous représente un diagramme de séquence où un utilisateur accède au réseau par le biais d'un NAS et se déconnecte.

Les messages affichés dans le diagramme de séquence sont envoyés en utilisant le protocole de transport UDP. Un protocole de fenêtrage est utilisé par-dessus ce protocole non fiable pour garantir une transmission correcte. Ce protocole introduit un message ZLB (un message DIAMETER sans commande) qui est utilisé pour envoyer un acquittement de message reçu. Ces messages n'ont pas été inclus au diagramme de séquence.

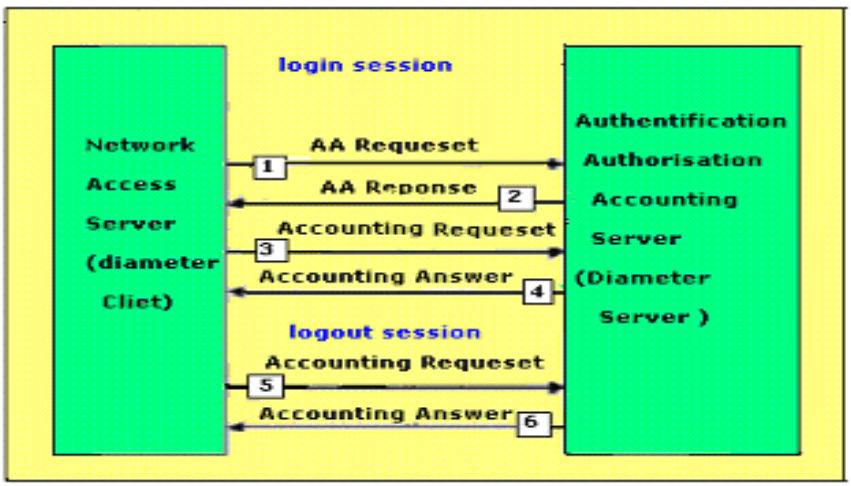


Figure. II.5 : Flux de messages DIAMETER.

V. Serveur DHCP :

V.1. Définition

DHCP signifie (Dynamic Host Configuration Protocol). Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur). Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configuration propres à un hôte donné.

V.2. Fonctionnement du protocole DHCP

Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.

Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour faire ça, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local. Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast (n'oubliez pas que le client n'a pas forcement son adresse IP et que donc il n'est pas joignable directement) contenant toutes les informations requises pour le client.

On pourrait croire qu'un seul paquet peut suffire à la bonne marche du protocole. En fait, il existe plusieurs types de paquets DHCP susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client :

- **DHCPDISCOVER** (pour localiser les serveurs DHCP disponibles)
- **DHCPOFFER** (réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres)
- **DHCPREQUEST** (requête diverse du client pour par exemple prolonger son bail)
- **DHCPACK** (réponse du serveur qui contient des paramètres et l'adresse IP du client)
- **DHCPNAK** (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
- **DHCPDECLINE** (le client annonce au serveur que l'adresse est déjà utilisée)
- **DHCPRELEASE** (le client libère son adresse IP)
- **DHCPINFORM** (le client demande des paramètres locaux, il a déjà son adresse IP)

Le premier paquet émis par le client est un paquet de type DHCPDISCOVER. Le serveur répond par un paquet DHCPOFFER, en particulier pour soumettre une adresse IP au client. Le client établit sa configuration, puis fait un DHCPREQUEST pour valider son adresse IP (requête en broadcast car DHCPOFFER ne contient par son adresse IP). Le serveur répond simplement par un DHCPACK avec l'adresse IP pour confirmation de l'attribution. Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace, mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP...

V.2. La sécurité du DHCP :

Le DHCP a été construit directement sur le protocole UDP et le protocole IP (Internet Protocole), respectivement la couche Transport et la couche Réseau du modèle OSI. Ces deux protocoles (UDP et IP), n'étant pas sécurise à 100%, rendent donc le DHCP assez vulnérable et insécurisé.

Des serveurs DHCP non-autorisés peuvent être facilement montés. Des serveurs de ce genre pourraient envoyer de fausses informations aux clients, comme des adresses incorrectes ou déjà utilisées ou bien même des routes erronées, etc.

Un faux client DHCP pourrait se faire passer pour un vrai client et s'accaparer de toutes les ressources disponibles, rendant ainsi l'accès aux connexions, par les clients légitimes, impossible. Pour résoudre ce problème des faux clients, il est possible pour le serveur DHCP de se bâtir une liste de MAC adresse (adresse matérielle individuelle de chaque carte réseau existante), différente pour chaque carte de tous les ordinateurs ayant le droit d'être client DHCP sur ce serveur. Avant d'envoyer une adresse IP, le serveur vérifiera dans sa table pour voir si ce poste est éligible ou pas. L'adresse MAC, étant unique pour chaque carte réseau, permet donc vraiment de contrôler les postes se connectant au serveur DHCP.

VII. Le serveur DNS

Le service DNS, né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques, il associe un nom à une adresse IP à chaque machine connectée au réseau. Ce principe de fonctionnement suscite une unicité des noms et le respect d'un nommage hiérarchique avec des domaines existants.

Pour déployer un serveur DNS dans un réseau, il faut définir l'adresse du réseau ; pour des organisations désirant donner un accès public à leur domaine, il faut acheter un nom de domaine chez un prestataire de services tout en assurant son unicité sur internet. Dans un réseau subdivisé en plusieurs sous réseaux, il doit y avoir un serveur DNS primaire par zone (sous réseau) et plusieurs serveurs secondaires sur lesquels on effectue des copies régulières des informations primaires pour des mesures de sécurité. Dans ce cas, une configuration des sous-domaines s'imposent.

Chapitre III :

La sécurité des réseaux sans fil.

I. Introduction :

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau vu sa nature physique aérienne, Il est donc indispensable de sécuriser les réseaux sans fil dès leurs installations. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut être réalisée à différents niveaux : configuration des équipements et choix des protocoles et aussi de prendre en compte tous les risques possibles, tels que les attaques volontaires, les accidents, les défauts logiciels ou matériels, ou encore les erreurs humaines et les réduire autant que possible.

II. Politique globale :

La sécurité mise en place au niveau WIFI peut devenir dérisoire si elle n'est pas accompagnée d'une politique globale. En effet, l'enjeu d'une politique de sécurité consiste à regarder le système dans son ensemble, à identifier les vulnérabilités les plus graves et les plus probables, et à y remédier .Idéalement, l'ensemble des processus doit être analysé en prenant en compte les aspects humains, techniques, légaux, organisationnels et stratégiques.

III. Les services de sécurité :

Cinq types de service de sécurité sont définis :

- **La confidentialité des données** : a pour but d'éviter toute divulgation d'informations à l'utilisateur, une entité ou un processus non autorisé.
- **L'authentification** : permet de s'assurer que celui qui se connecte est bien celui qui correspond au nom indiqué.
- **L'intégrité** : garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé et se préserver des pertes d'informations.
- **La non-répudiation** : assure qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié.
- **Le contrôle d'accès** : a pour fonction la prévention de l'accès à des ressources sous des conditions définies et par des utilisateurs spécifiés.

Dans chacun de ces services, il peut exister des conditions particulières

Si l'on reprend les cinq services de sécurité présentés précédemment en étudiant les besoins de l'émetteur et du récepteur et en les répertoriant, on obtient le processus suivant :

1. Le message ne doit parvenir qu'au destinataire.

2. Le message doit parvenir au bon destinataire.

3. L'émetteur du message doit pouvoir être connu avec certitude.

4. Il doit y avoir identité entre le message reçu et le message émis.

5. Le destinataire ne peut contester la réception du message.

6. L'émetteur ne peut contester l'émission du message.

7. L'émetteur ne peut accéder à certaines ressources que s'il en a l'autorisation.

IV. Principales attaques :

L'attaque d'un réseau nécessite l'utilisation d'une station espionne située dans la zone de couverture ou en dehors de celle-ci à condition qu'elle soit munie d'une antenne directive.

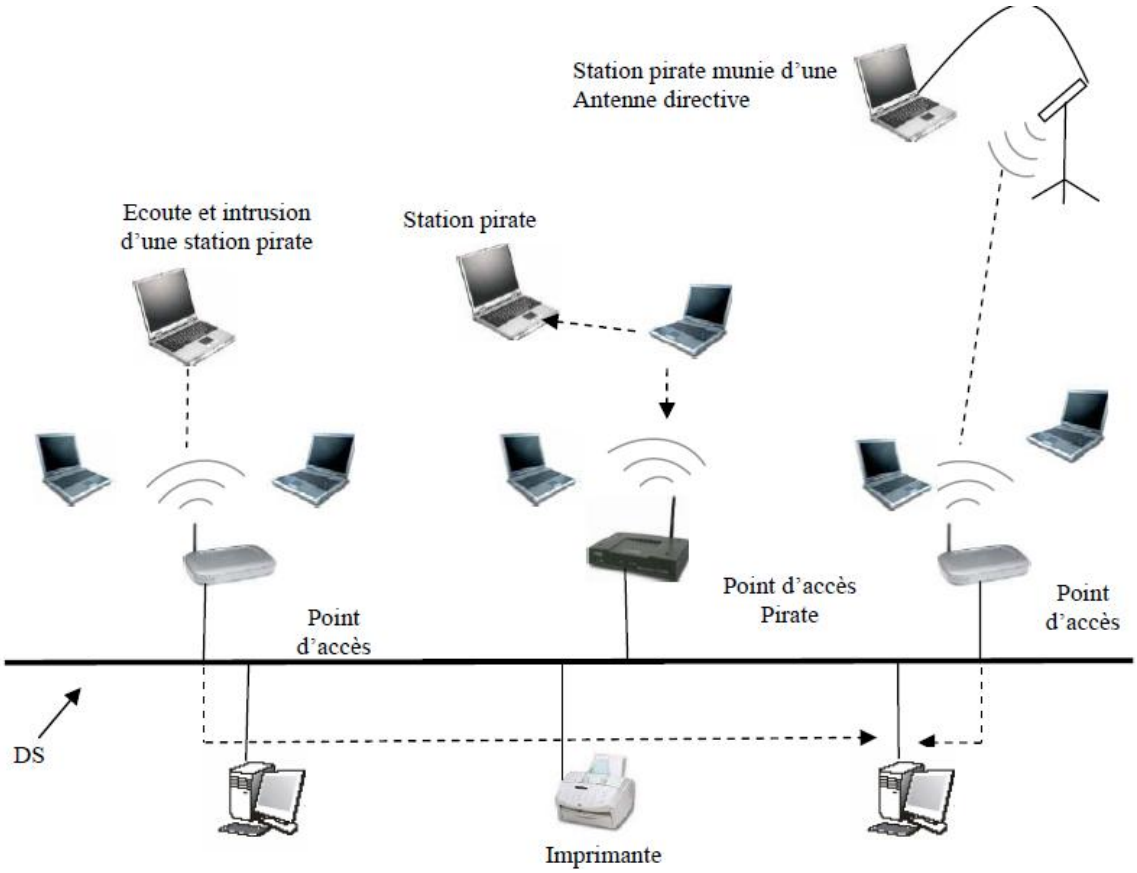


Figure III.1: Différents cas d'attaques

- L'interception des données:

En absence de système de cryptage efficace, il est facile de récupérer le contenu des données qui circulent sur le médium.

− **L'intrusion dans le système :** Elle consiste, pour une station étrangère au réseau, à se connecter au point d'accès puis à intégrer le réseau.

− **Attaque de l'homme au milieu :** Il suffit de mettre en place un point d'accès étranger dans la zone de couverture du réseau WLAN afin d'intégrer le réseau. Les stations cherchent alors à se connecter à ce point d'accès (pirate) en fournissant ainsi les informations concernant le réseau auquel elles sont rattachées. L'exploitation de ces informations permet aux pirates de se connecter au réseau.

− **Attaque par porte dissimulée :** Cette technique est identique à la précédente, la seule différence provient du fait que le point d'accès pirate est directement raccordé au système de distribution du réseau.

V. Les risques liés aux réseaux sans fil :

V.1. Le manque de sécurité :

Les ondes radioélectriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations).

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau.

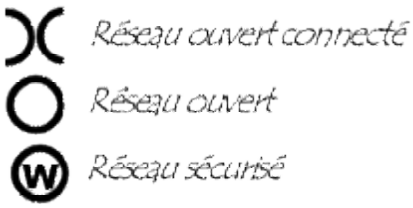
Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques" dans le rayon de couverture du point d'accès !

V.2. Le War-driving

Etant donné qu'il est très facile d'"écouter" des réseaux sans fil, une pratique venue tout droit des Etats-Unis consiste à circuler dans la ville avec un ordinateur portable (voir un assistant personnel) équipé d'une carte réseau sans fil à la recherche de réseaux sans fil, il s'agit du war driving (parfois noté wardriving). Des logiciels spécialisés dans ce type d'activité permettent même d'établir une cartographie très précise en exploitant un matériel de géolocalisation (GPS, Global Positionning System).

Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés, offrant même parfois un accès à internet ! De nombreux sites capitalisant ces informations ont vu le jour sur internet, si bien que des étudiants londoniens ont eu l'idée d'inventer un "langage des signes" dont le but est de rendre visible les réseaux sans fils en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau wireless, il s'agit du « war-chalking » (francisé en craieFiti ou craie-fiti). Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la

présence d'un réseau sans fil ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé.



V.3. Les risques en matière de sécurité :

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- **L'interception de données :** consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
- **Le détournement de connexion :** dont le but est d'obtenir l'accès à un réseau local ou à internet
- **Le brouillage des transmissions :** consistant à émettre des signaux radio de telle manière à produire des interférences
- **Les dénis de service :** rendant le réseau inutilisable en envoyant des commandes factices

1. L'interception de données:

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

2. L'intrusion réseau :

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.

Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

3. Le brouillage radio :

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

4. Les dénis de service :

Consiste à saturer les ressources d'un système de façon à le rendre inopérant, afin d'empêcher l'accès à celui-ci.

La personne générant ce type d'attaque ne porte pas donc atteinte à l'intégrité des informations de l'entreprise mais rend inutilisable le service réseau. Une personne n'arrivant pas à se connecter à un réseau sans fils peut très bien lancer un grand nombre de requêtes de connexion pour ainsi surcharger le point d'accès et empêcher les utilisateurs habilites de s'y connecter. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

VI. La sécurité élémentaire :

Elles permettent uniquement de résoudre le problème du contrôle d'accès. Il s'agit de trois techniques qui peuvent éventuellement être utilisées de façon complémentaire

VI.1. L'identificateur de réseau :

Il s'agit de l'ESSID (Extended Service Set Identifier), souvent appelé SSID que l'utilisateur doit connaître pour se connecter au réseau. Cette protection est en fait très sommaire, vus que les points d'accès envoient périodiquement et en clair le SSID dans les trames balises. Il suffit d'une simple écoute du réseau pour obtenir le SSID.

VI.2. Le mot de passe :

Pour se connecter au réseau, l'utilisateur doit donner le mot de passe. Cette protection est également très simpliste. Il est facile pour un intrus de capturer le mot de passe et de l'utiliser par la suite pour se connecter au réseau.

VI.3. La protection par adresse MAC :

Chaque adaptateur réseau possède une adresse physique unique appelée adresse MAC, représentée par douze chiffres hexadécimaux.

Les points d'accès permettent généralement dans leur interface de configuration, de gérer une liste de droits d'accès basée sur les adresses MAC des équipements autorisés à se connecter au réseau. Le filtrage MAC peut aussi être contourné. Une écoute passive du réseau permet de récupérer les adresses MAC reconnues par le réseau.

Aussi, de nombreux adaptateurs radio permettent de modifier par logiciel leurs propres adresses MAC.

VI.4. Sécurité des points d'accès :

Changer la configuration par défaut des points d'accès est une première étape essentielle dans la sécurisation de son réseau sans fil. Pour cela il est nécessaire de :

- changer les mots de passe par défaut (notamment administrateur) par des mots de passe blindés;
- modifier la configuration par défaut (adressage privé utilisé avec DHCP ou adresse de l'interface par exemple) ;
- désactiver les services disponibles non utilisés (SNMP, Telnet...) ;
- régler la puissance d'émission du point d'accès au minimum nécessaire.

Il est également important de mettre à jour le firmware de son point d'accès dès que le constructeur propose une mise à jour (résolution d'un problème de sécurité sur un des services disponibles par exemple). Cette mise à jour suppose des tests préalables poussés afin de vérifier la compatibilité avec l'existant une fois la mise à jour effectuée.

Changer le SSID par défaut est une bonne pratique, largement recommandé dans la plupart des cas. Il est judicieux de ne pas choisir un SSID attractif. La plupart des points d'accès donne la possibilité de désactiver la diffusion du SSID. Il ne s'agit nullement d'une mesure de sécurité car une personne informée pourra obtenir le SSID très facilement : le SSID est une donnée qui est visible lors de l'association d'un client.

Ensuite, il s'agit de configurer le point d'accès en activant les options de sécurité répondant aux objectifs choisis en matière de sécurité.

Enfin, au-delà de la sécurité logique, il est nécessaire de prendre en compte la sécurité physique des points d'accès. Le vol d'un point d'accès dans le but d'analyser sa configuration et récupéré des informations importantes : Adressage IP, mot de passe, clé de chiffrement WEP statique, pour éviter les conséquences d'un tel vol, on utilise un Switch WLAN pour qu'aucune information importante n'est stockée physiquement sur le point d'accès, en plus de démontage physique des interfaces inutiles.

VII. Méthodes de sécurisation :

VII.1. Sécurité des protocoles liés aux réseaux sans fil :

De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux sans fil. Les objectifs sont les suivants :

- garantir la confidentialité des données ;
- permettre l'authentification des clients ;

- garantir l'intégrité des données.
  (Cette méthode a été détaillée dans le deuxième chapitre).

VII.2. Sécurité de la technologie :

De par sa technologie le Wi-Fi est un protocole qui diffuse les données vers toutes les stations qui sont aux alentours. Un utilisateur mal intentionné peut se placer dans le périmètre des équipements du réseau afin de récupérer les informations qui lui permettront d'avoir accès au réseau.

La sensibilité au brouillage est une autre vulnérabilité induite par la technologie des réseaux sans fil. Elle peut entraîner un déni de service des équipements du réseau, voir la destruction de ces équipements dans le cas de bruit créé artificiellement.

VII.3. Sécurité après la mise en place du réseau sans fil

Afin de conserver un niveau de sécurité satisfaisant de son réseau sans fil, il est nécessaire d'appliquer les mêmes procédures que pour les réseaux filaires, à savoir :

- informer les utilisateurs : la sécurité d'un réseau passe avant tout par la prévention, la sensibilisation et la formation des utilisateurs ;
- gérer et surveiller son réseau : la gestion et la surveillance d'un réseau sans fil peut, elles aussi, s'effectuer à deux niveaux. La surveillance au niveau IP avec un système de détection d'intrusions classique (prelude, snort, ...) et la surveillance au niveau physique (sans fil) avec des outils dédiés (Kismet, ...).
- auditer son réseau : l'audit d'un réseau sans fil s'effectue en deux parties. Un audit physique pour s'assurer que le réseau sans fil ne diffuse pas d'informations dans des zones non désirées et qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser. Un audit informatique, comme pour les autres réseaux, pour mesurer l'écart entre le niveau de sécurité obtenu et celui désiré.

La sécurité d'un réseau sans fil comprend aussi sa gestion. Gérer un réseau sans fil nécessite de s'appuyer sur une équipe ayant une bonne connaissance des réseaux et de la sécurité des systèmes d'information.

VII.4. Chiffrement du trafic :

Afin de sauvegarder la confidentialité et l'intégrité des données circulant sur le lien sans fil, il est indispensable de chiffrer le trafic de telle sorte qu'il ne soit intelligible que par les destinataires légitimes.

Les techniques de saut de fréquence radio sur un WLAN est facilement ou volontairement calculable par les récepteurs, il est donc indispensable de mettre en place un système de chiffrement au niveau réseau pour sécuriser le trafic sur la partie radio.

VII.4.1 Le WEP :

La couche MAC du 802.11 offre un mécanisme optionnel de chiffrement des données (cryptage) s'appelle le Wired Equivalent Privacy (WEP) qui utilise l'Algorithme de chiffrement RC4. Tous les périphériques et tous les APs du réseau doivent être configurés avec une même clé statique secrète de 40 ou 104 bits, qui permet de chiffrer les communications. Le cryptage WEP est suffisamment simple pour être réalisé très rapidement, de sorte qu'il ne pénalise pas (ou peu) le débit.

Il a toutefois plusieurs inconvénients : d'abord, il suppose qu'une même clé soit configurée sur tous les équipements du réseau (AP et périphériques clients). Cette clé étant connue de tous les utilisateurs du réseau, le risque de « fuite » est plus important car il suffit d'une indiscrétion d'un seul employé pour compromettre toute la sécurité du réseau. En outre, si la clé est compromise, il faudra la changer sur tous les périphériques et tous les AP, ce qui est très loin d'être pratique. Pour finir, malgré son nom qui signifie littéralement « sécurité équivalente à un réseau filaire », le cryptage WEP a été « cassé » par des chercheurs qui y ont trouvé plusieurs failles. Il existe même des logiciels gratuits pour déchiffrer toutes les communications WEP, donc ce mécanisme ne garantit pas une efficacité à 100 %.

VII.4.2. Le WPA:

Pour pallier les insuffisances du WEP, un remplaçant est à l'étude appelé WPA (Wi-Fi Protected Access), son fonctionnement repose sur un système d'échange de clés dynamiques, suivie d'un cryptage robuste des communications renouvelées tous les 10 ko de données Ce procédé, appelé TKIP (Temporal Key Integrity Protocol). Le WPA Entreprise repose sur le 802.1x et sur un serveur RADIUS, il permet d'assurer une authentification très sécurisée protège mieux les clés du décryptage et devrait améliorer sensiblement la sécurité des réseaux sans fil même si l'algorithme utilisé reste inchangé.

Pour avoir un bon niveau de sécurité, il faut mettre en place la solution WPA. À part pour les très petits réseaux, il est alors nécessaire d'installer et configurer un serveur RADIUS

Remarque :

La vitesse de transmission sans fil est réduite en cas d'activation des protocoles WEP, WPA-PSK(TKIP) en raison des délais nécessaires au chiffrement et au déchiffrement.

Pour conclure ce chapitre, passons rapidement en revue ce que nous avons appris :

– Un système d'information est sécurisé s'il assure la confidentialité et l'intégrité des données, ainsi que la disponibilité du système : on parle des qualités CID. Des mécanismes de non-répudiation peuvent également être mis en œuvre.

– Assurer la sécurité d'un système impose une vision globale et pas uniquement technique : cela implique de mettre en place une organisation de sécurité transversale et indépendante dans l'entreprise, de définir une politique globale, et d'assurer la sécurité à tous les échelons : en particulier aux niveaux organisationnel, humain, données, logiciels, réseau et physique.

L'ensemble du système informatique doit être compartimenté et les droits des utilisateurs doivent être restreints pour éviter qu'une personne connectée au réseau, comme un visiteur ou même un employé, puisse tout faire.

– Le wardriving a mis en évidence l'importance de sécuriser les réseaux sans fil contre les attaques de réels pirates ou de simples curieux.

– Les attaques possibles contre un réseau Wifi peuvent être classées en quatre catégories : espionnage, intrusion, modification des données et déni de service.

– Les parades possibles incluent : le cryptage des données échangées, un mécanisme fiable d'identification des utilisateurs, le contrôle rigoureux de l'intégrité des messages échangés, un mécanisme pour empêcher la relecture d'anciens messages. Tout cela est mis en œuvre dans le WPA Malheureusement, il n'existe aucune parade contre le déni de service au niveau Wi-Fi, mais heureusement ces attaques sont rares car l'intérêt est limité et le pirate doit se situer à proximité du réseau sans fil.

– Des mesures de sécurité générales sont à mettre en œuvre, autant que possible :

Limiter le débordement radio, éviter les AP pirates, réaliser une supervision radio permanente et placer le réseau sans fil dans son propre VLAN.

Chapitre I :

Conception et installation

I. Introduction :

Ce dernier consiste à la résolution de notre problématique et l'application de celle-ci (l'installation et la configuration du réseau Wi-Fi). Nous développerons notre travail dans un cadre spécifique.

Dans cette partie nous allons mettre en évidence la méthodologie d'installation et la configuration d'un réseau sans fil local (Wi-Fi). Nous allons représenter les différentes étapes d'installation par un ensemble de fenêtres en induisant aussi les différentes configurations.

II. L'étude du site :

Dans cette étape, on présente le site, le mode d'architecture et le matériel utilisé pour la réalisation de ce réseau.

II.1 Présentation du site :

Durant notre étude au sein de l'entreprise nationale Algérie Telecom, nous avons pu nous focalisé sur un domaine d'étude bien définie, que nous avons réalisé dans le site figuré dans l'image qui suit.

II.2. Mode d'architecture :

Suite a l'étude effectuer on a opté pour le mode infrastructure qui est plus adéquat pour ses divers avantages par rapport au mode Ad Hoc, car il nécessite l'utilisation d'un point d'accès (jeu le rôle d'un SWITCH), et caractériser par un débit de transmission plus élevé qui peut aller jusqu'à 54 Mb/s, par contre le mode Ad Hoc utilise un débit en maximale 4 Mb/s. **(Fig. I.1)**

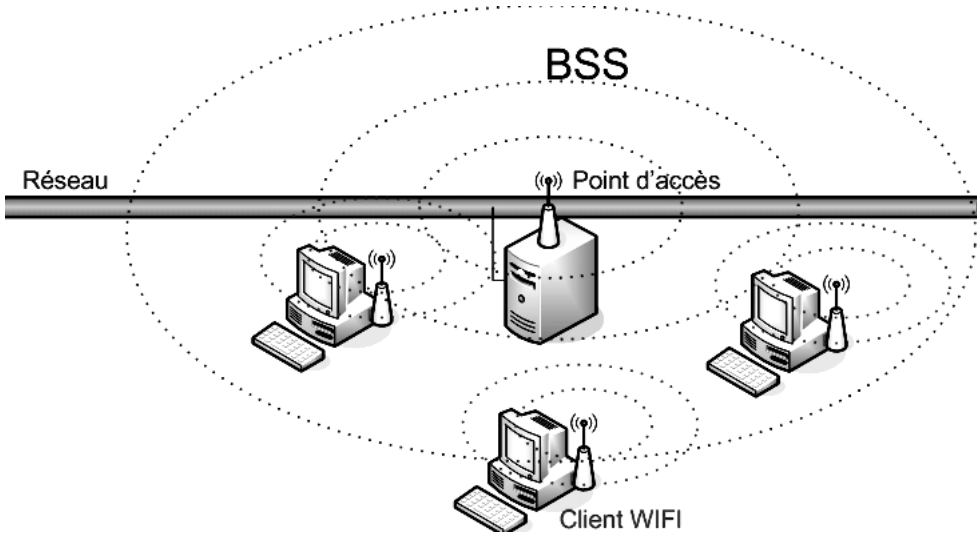


Fig. I.1 : Mode Infrastructure.

II.3. Le Matériel utilisé:

Après l'étude réalisée sur le site (I.L.E), on a choisit le matériel selon les besoins du projet et suivant la structure des blocs de champ d'étude.

II.3.1. Le câblage :

Nous avons utilisé deux types de câbles qui sont présentés ci-dessous, dans le but d'interconnecter les points d'accès avec le contrôleur.

a) Câble paire torsadé FTP :

Le câble FTP est utilisé pour l'interconnexion des points d'accès avec les Switchs.
Ce câble appartient à la catégorie 5 (blinder). Il est caractérisé par une longueur maximale de 100 m et un débit maximal de 100 Mb/s. (**Fig. I.2**).

Fig. I.2 : Câble paire torsadé FTP

b) Câble fibre optique:

Ce câble de fibre optique est utilisé pour l'interconnexion du contrôleur avec le Switch optique, car le contrôleur contient deux ports SFP (Giga Ethernet). La fibre optique qu'on a utilisé est connue sous le nom **Jarretières Optiques (Fig. I.3)**, qui est caractérisée par :

- Monomode SC/SC.
- Longueur : 5 m.
- Réf. 87060.
- Débit = 2.4 Gbps.

Fig. I.3 : câble fibre Jarretières SC/SC.

II.3.2. Le Switch optique HUAWEI :

Pour interconnecter les points d'accès avec le contrôleur on a utilise le Switch optique HUAWEI (Quidway S2000). Ce Switch fonctionne au niveau de la couche 3 (OSI), qui possède 24 ports d'interfaces 10/100Base-T type RJ-45 (Fast Ethernet) et 2 ports SFP 1000Base-FX (Giga Ethernet). **(Fig. I.4)**

Fig . I.4: Switch Huawei Quidway S2000

II.3.3 Hub Level one (POH – 0850 TX):

Dans notre cas le hub est utilisé pour alimenté les APs dans le but d'évité de placé a chaque AP une prise d'alimentation et réduire des lignes électriques encombrantes. On a utilisé Level One PoE-Hub 19 (POH-0850 TX) qui est un Hub/Switch, administrable, 8 ports RJ-45. (**Fig. I.5).**

Fig .I.5: Hub Level One.

II.3.4.Les points d'accès :

On a choisis les points d'accès Siemens (HiPath Wireless Access point (AP)) car ils peuvent supporter les deux standards radios 802.11a +b/g et plusieurs SSID. Les deux types d'APs utilisés sont : APs 2620 avec antennes extérieures et APs 2610 avec antennes intégrées (Fig. I.6)

Fig. I.6 : Points d'Accès Wi-Fi de (HiPath Wireless).

Remarque:

L'AP 2620 possède deux antennes radio pour améliorer la puissance du signal.

II.2.5. Le Contrôleur C1000

Le Contrôleur **(HiPath Wireless Controller (HWC))** est un équipement ou un serveur qui permet une gestion centralisée du réseau sans fil. On peut le placer sur n'importe quel réseau IP. Il permet de contrôler tous les points d'accès, de gérer des sessions et de router le trafic IP des utilisateurs. Il existe trois types de contrôleur (C10, C100 et C1000).

Dans notre étude on a choisi le contrôleur C1000 qui peut gérer 200 point d'accès. **(Fig. I.7).**

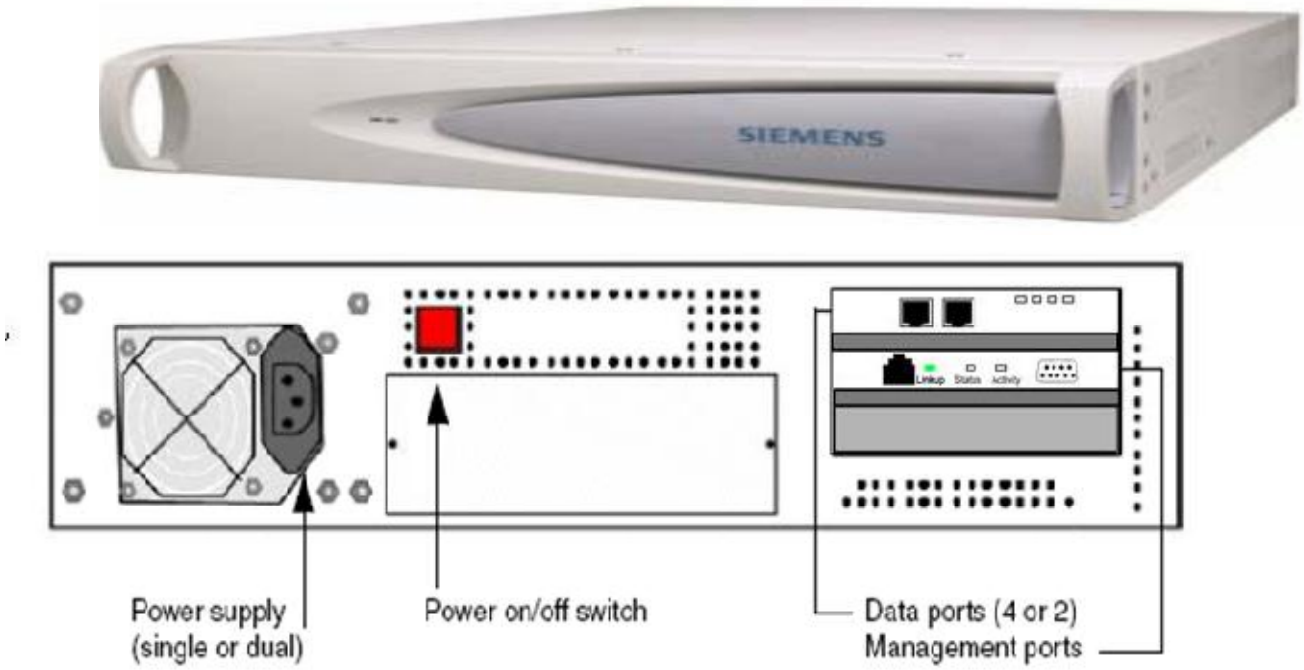


Fig. I.7 : Contrôleur HWC C1000 (Hipath Wirelesse Controller).

II.2.6 Scalence W 788- 1 PRO

L'utilisation des Scalence sert pour interconnecté le bloc administration avec les deux blocs A et B et évité d'utilisé les câbles qui sont sensible aux intempéries et la chaleur extérieur.
Le scalence w 788-1 PRO s'appuis sur les standards WLAN selon les IEEE 802.11 b/g et 802.11 a. **(Fig. I.8).**

Fig. I.8 : Le scalence w788.

II.2.7 Convertisseur optique TP- Link :

On a utilisé deux convertisseurs optiques, le 1^{ér} est placé au niveau du C.A et le 2^{éme} dans l'armoire de brassage de l'administration de l'I.L.E, dans le but de convertir le lien optique entre la cité universitaire et le centre d'Amplification d'Algérie Telecom en faste Ethernet, pour que notre lien de transmission soit adapté avec les switchs utilisés. **(Fig. I.9)**

- TP-LINK est un convertisseur d'interface Ethernet pour fibre optique 62,5/125 µm ou 50/125 µm, qui a :

- 1 connecteur RJ45 UTP Ethernet10/100 jusqu'à 200 Mbps.
- 1 connecteur optique (double avec 1 transmission + 1 réception) de type SC.

Fig. I.9 : Convertisseur TP-Link.

II.2.8 onduleur EMERSON (LIEBERT) :

L'onduleur est de conception Line Interactive, incluant la technologie de régulation automatique de tension. Il protège des variations de tension du réseau électrique en augmentant ou diminuant la tension au niveau requis par les équipements connectés. Ainsi l'onduleur augmente la durée de vie de ses batteries en restant connecté un maximum de temps au secteur avant de passer en mode secours.

Spécifiquement conçus pour:

- Les ordinateurs de bureau
- Les stations de travail professionnelles
- Les serveurs
- Les armoires réseau
- Les matériels réseaux critiques

Dans notre cas on a utilisé un onduleur EMERSON**. (Fig . I.10)**

Fig. I.10 : onduleur EMERSON.

II.2.9 Injecteur Level One (POI 2000) :

Level One POI-2000 est un dispositif avec une alimentation interne afin de réduire des lignes électriques encombrantes et la gestion de prises électriques. Le produit s'intègre au réseau d'origine pour distribuer du courant et des données au dispositif à distance à travers d'un câble Ethernet standard existant. **(Fig. I.11).**

Fig. I.11 : Injecteur Level One (POI 2000)

III. Logiciels : les principales parties de logiciel sont :

1) **System de supervision** : le HWCS **(HiPath Wireless Convergence Software V4.0)** est un système d'exploitation qui réside principalement dans le contrôleur**.** Il assure l'administration, le management, la supervision du contrôleur et les Point d'Accès (AP) qui son connecter au contrôleur.
2) **Système d'exploitation :** Windows 2003 serveur et Windows xp.
3) **Serveurs :** le **s**erveur **DHCP** attribue des adresses IP dynamiques pour les points d'accès.

IV. L'installation :

Pour l'installation de notre réseau on a procédé aux étapes suivantes :

- L'installation des armoires de brassages.
- L'installation des gollotes.
- L'installation des points d'accès sur les murs.
- Tirage des câbles entre les points d'accès et les Switchs.

IV.1. L'installation des armoires de brassages :

On a utilisé 03 armoires de brassage de marque TELESYSTEM 9U qu'on a fixé au mur dans les trois blocs de la résidence ILE comme suite :

Avant toute chose, on doit placer les armoires dans un endroit précis (sécurisé et aéré). Soit fixé au sol ou sur le mur**.**

Pour le bon fonctionnement du réseau, on a installé trois armoires à la cité universitaire, les trois fixés sur les murs des différents blocs :

- La 1^{ére} au bloc administration**. (Fig. I.12)**.
- La 2ème au bloc A**. (Fig. I.13)**.
- La 3ème au bloc b. **(Fig. I.14)**.

Une quatrième est au niveau de centre d'amplification (C.A de la nouvelle ville de Tizi –Ouzou), ou on a branché le contrôleur pour une meilleur gestion des APs, qu'on expliquera par la suite.

Fig. I.12 : Armoire de brassage du bloc administration.

Fig. I.13 : Armoire de brassage du bloc A.

Fig. I.14 : Armoire de brassage du le bloc B.

Le contrôleur C1000 peut gérer jusqu'à 200 APs, après l'étude effectué sur le site on a installé 15 APs. Pour la bonne exploitation de ce dernier on a opté du placé au niveau de C.A , pour pouvoir lui interconnecté d'autres réseaux jusqu'à sa saturation, et avoir le privilège d'accéder à tout moment sans être dans l'obligation de se déplacer sur les différents sites connecter a ce contrôleur. **(Fig. I.15).**

Fig. I.15 : L'armoire de brassages au niveau de la C.A**.**

IV.2. L'installation des gollotes :

L'étude et la conception constituent la première étape de l'installation. Cette phase consiste à identifier les besoins en fonction de l'architecture des lieux. L'élaboration d'un plan du bâtiment avec les emplacements des gollotes est fortement conseillée. Cette étude déterminera les longueurs des fils et des goulottes utilisées.

L'étape suivante est la réalisation. Pour l'installation des goulottes voici les étapes à suivre :

1. Le marquage des chemins de câble sur les murs
2. La fixation des goulottes à l'aide de colles ou de chevilles
3. Le tirage des câbles dans les goulottes
4. Le recouvrement des goulottes

Avant de sceller définitivement les installations, veillez à tester les circuits avec un testeur et à vérifier toutes les connexions.

Fig. I.16: Goulotte informatique

Goulotte après installation.

IV.3. Installation des points d'accès :

Avant de faire une installation du réseau sans fil sur un site (entreprise, aéroport, université…), il est utile et nécessaire de faire une étude sur l'environnement du projet; Cette étude concerne les distances, la qualité des murs, les hauteurs, le nombre d'APs utilisés…etc.

Dans les tests de mise en service on a ajouté deux APs pour la simulation du bon fonctionnement de la configuration du contrôleur.

L'installation des APs sur les différents blocs est répartie comme suit :

- 11 APs siemens 2610 :

1. Un au bloc A droite 1ère étage (BLOC A-D-1).
2. Un au bloc A droite 2ère étage (BLOC A-D-2).
3. Un au bloc A droite 3ère étage (BLOC A-D-3).
4. Un au bloc A droite 4ère étage (BLOC A-D-4).
5. Un au bloc B droite raie de chaussé (BLOC B-RDC).
6. Un au bloc B 1ère étage (BLOC B-1).
7. Un au bloc B 2ère étage (BLOC B-2).
8. Un au bloc Administration raie de chaussé (BLOC ADMIN RDC).
9. Un au bloc Administration 1ère étage (BLOC ADMIN 1ER).
10. Un à la salle de lecture (S/LECTURE).
11. Un au cyber de la cité (CYBER).

- 4 APs Siemens 2620 :

1. Un au bloc A gauche 1ère étage (BLOC A-G-1).
2. Un au bloc A gauche 2ère étage (BLOC A-G-2).
3. Un au bloc A gauche 3ère étage (BLOC A-G-3).
4. Un au bloc A gauche 4ère étage (BLOC A-G-4).

On fixe les points d'accès sur les murs comme suit :

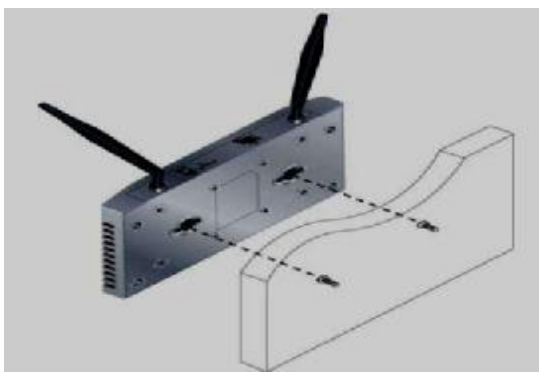


Fig. I.17. Fixation APs sur les murs.

Image d'un AP fixé ou mur dans le bloc administration 1ére étage **(Fig. I.18)** :

Fig. .I.18: AP (A-D-1).

Après avoir fixé les APs siemens on a installé les deux scalence comme suit :

- Un au bloc administration (SCAL-AD);
- L'autre au bloc B (SCAL-B).

IV.4. Tirage des câbles :

Avant de commencer, on détermine les distances entre les points d'accès et les armoires de brassages où on choisit le chemin le plus court et on tire les câbles dans les gollotes entre les points d'accès et les Switchs. A la fin on doit confectionner les câbles et placé les RG 45 à leurs bouts.

Fig. I.19. Tirage des câbles.

Et par la suite on doit placer et interconnecté tous les points de connexion (Switch, hub, injecteurs…) dans l'armoire de brassages, et aussi relier les APs au réseau filaire avec un Switch.

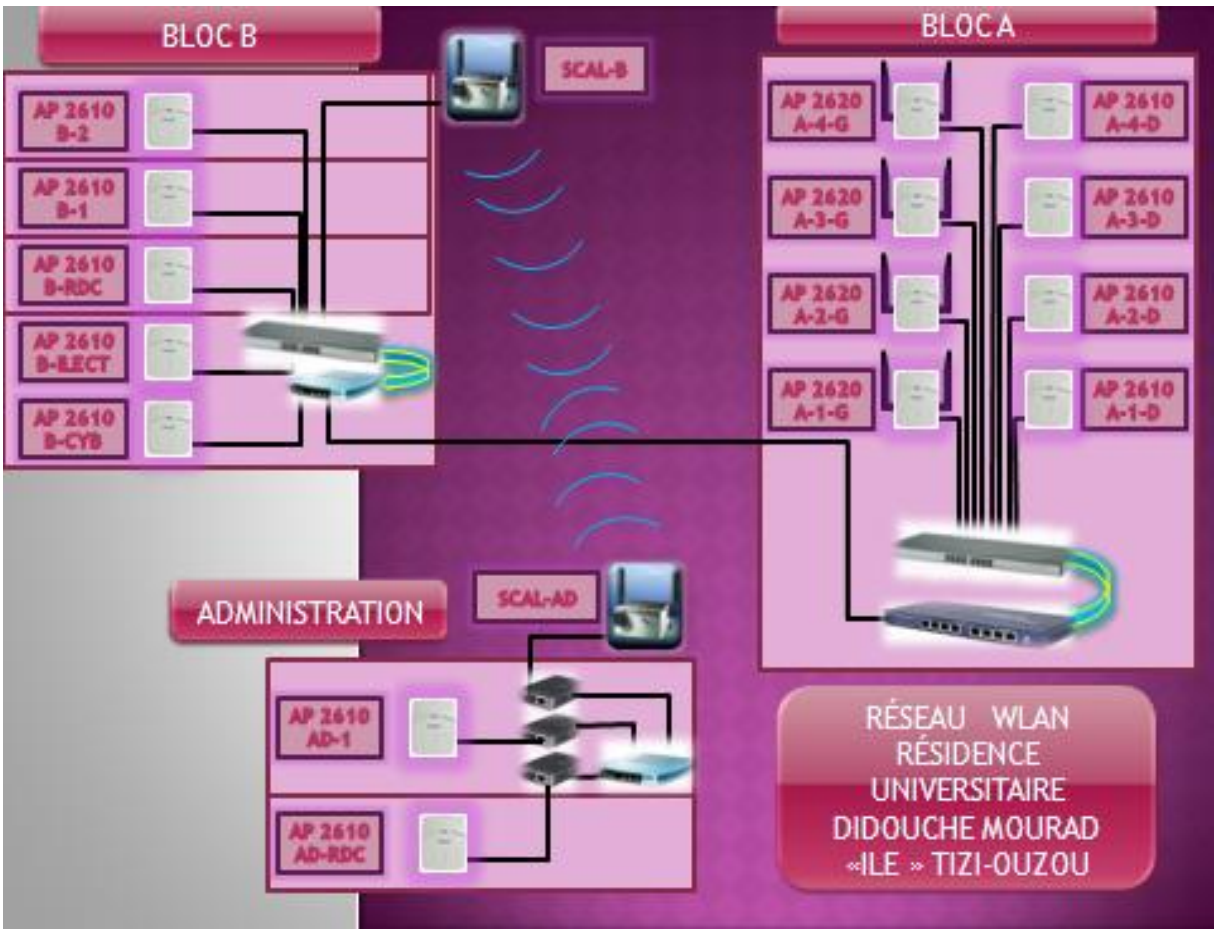
Fig. I.20. Raccordement du port RJ45

Après le montage et l'installation de l'ensemble des appareils nécessaires, il sera procédé à un essai définitif de la mise en service du réseau.

V. L'emplacement des équipements :

V.1 Plan d'implantation:

L'emplacement des différents équipements sont représenté dans le plan suivant :



V.2 Le mode de fonctionnements :

Après la mise en place et la configuration des différents équipements on passe a La mise en service du réseau qui permet de connecter les ordinateurs, et cela se fait par la propagation des ondes radio. Dans notre cas on a réalisé le réseau par le mode infrastructure, où les points d'accès sont nécessaires.
Dans ce qui suit, nous allons donner les différentes étapes pour mettre en service notre réseau:

1-interconnecter les équipements qui se trouvent dans les armoires.
2-Interconnecter les scalences et les points d'accès vers le Switch.
3-En branche le câble optique du lien de transmission dans le convertisseur qui se trouve dans l'armoire de l'administration puis on branche le câble sortant vers le Switch.
5-mettre en marche toute les équipements.

VI. Inventaire des équipements installé à la résidence universitaire (tableau)

EQUIPEMENTS INSTALLES RESIDENCE UNIVERSITAIRE DIDOUCHE MOURAD EX I-L-E

EQUIPEMENT	Qte	MARQUE	REFERENCE	N° DE SERIE	BLOC
ARMOIRE DE BRASSAGE TELESYSTEM 9U	03	TELESYSTEME	9U		
SWITCH 16 PORTS TRENDnet	01	TRENDnet	TE-100-S16	0445A2A17401	BLOC A
SWITCH 08 PORTS TRENDnet	02		TE-100-S8P	0447E2A30613	BLOC ADMIN
			TE-100-S8P	0447E2A30646	BLOC B
BANDEAU D'ALIMENTATION	03	TELESYSTEME	09 P		
HUB 08 PORTS	02	LEVEL ONE	POH 0850 TX	6120548986	BLOC B
			POH 0850 TX	6120548987	BLOC A
INJECTEUR 01 PORT	03	LEVEL ONE	POI 2000	7060939988	BLOC ADMIN
				7060939982	BLOC ADMIN
				7060939952	BLOC ADMIN
BORNE WIFI SCALANCE	02	SIEMENS	1 Pro	SVP V8052868	BLOC ADMIN
				SVP V8054125	BLOC B
BORNE WIFI	11	SIEMENS	AP 2610	500006492052327	BLOC A-D-1

				500006492052283	BLOC A-D-2
				500006492052297	BLOC A-D-3
				500006492052228	BLOC A-D-4
				500006492051951	BLOC B-RDC
				500006492052197	BLOC B-1
				500006492051970	BLOC B-2
				500006492052237	BLOC ADMIN RDC
				500006492052159	BLOC ADMIN 1ER
				500006362051024	S/LECTURE
				500006492052381	CYBER
BORNE WIFI	04	SIEMENS	AP 2620	500006332051032	BLOC A-G-1
				500006332051082	BLOC A-G-2
				500006332051073	BLOC A-G-3
				500006332051014	BLOC A-G-4
ONDULEUR	03	EMERSON	LIEBERT	09020R2199AF043	BLOC ADMIN
				09020R2140AF043	BLOC A
				09020R2203AF043	BLOC B
CABLE FTP CAT 6	800 M				
CONNECTEUR RJ 45 CAT 05	68				
CABLE CONNEXION HUB/SWITCH	17				
GOULOUTTE 12,5X20	400 M				
GOULOUTE 40X20	80 M				
GAINE A RESSORT	50 M				

Chapitre II :

Sécurisation et Configuration des équipements

Introduction :

Pour la configuration des points d'accès, nous avons choisi un contrôleur, qui nous permet de configurer, d'administrer et de superviser notre réseau sans fil. Avant de commencer la configuration des points d'accès, il est nécessaire d'installer un serveur DHCP option 78 et 79 qui assigne des adresses IP dynamique pour assurer l'enregistrement (l'identification) des points d'accès sur le contrôleur. Les étapes de la configuration sont :

- Configuration de serveur DHCP.
- Configuration des scalences.
- Configuration du contrôleur.
- Configuration des APs.

I. La configuration de serveur DHCP :

I.1- Installation du composant DHCP :

DHCP n'est pas un composant installé par défaut lors d'une installation normale de Windows Server 2003.Vous pouvez le configuré lors de l'installation de Windows 2003 ou ultérieurement. On clic sur **Démarrer, Gérer votre serveur** puis **Ajouter un rôle**. **Fig. II.1**

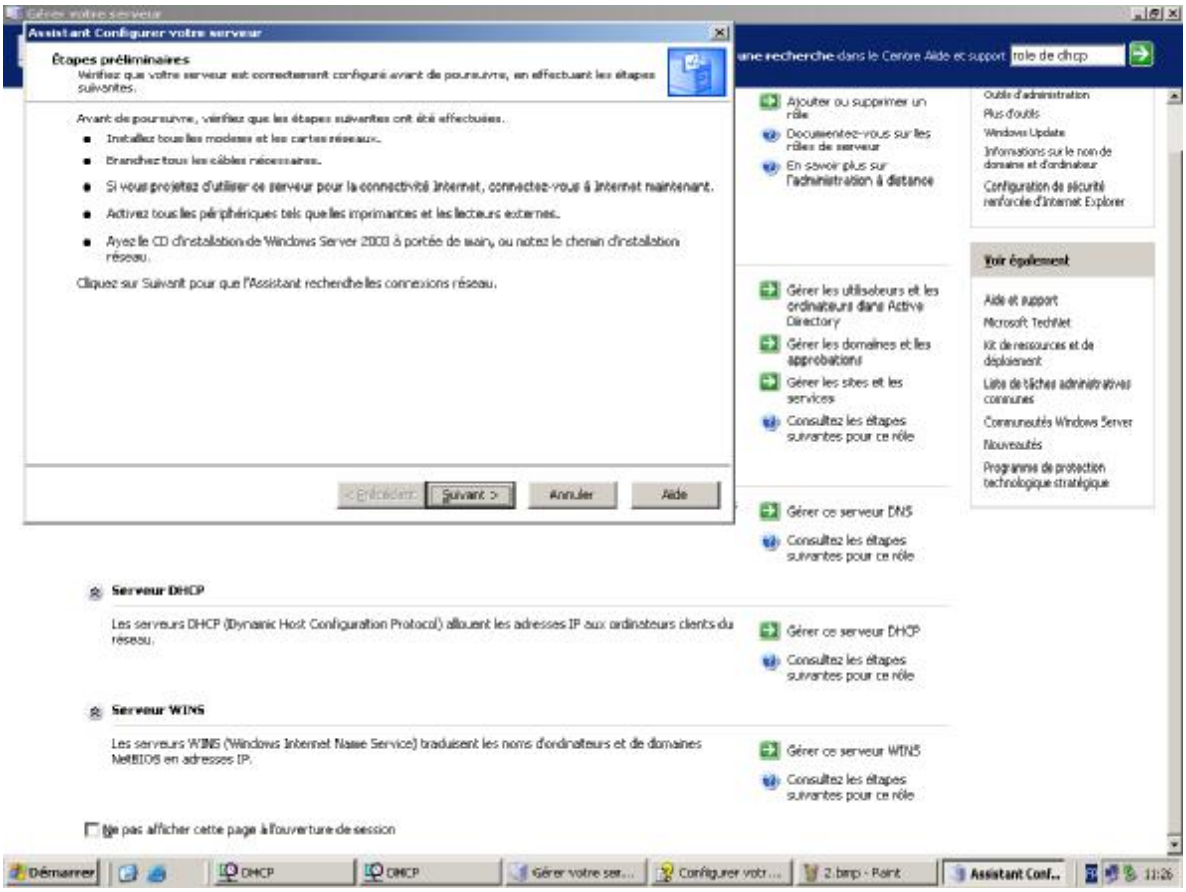


Fig. II.1 Ajouter un rôle

Pour l'installation du serveur DHCP sur Windows 2003 serveur. On a procédé comme suit:

- Clique sur le bouton **Démarrer**, **Panneau de Configuration** puis **Ajout/Suppression de programmes**.
- Ensuite un autre clique sur le bouton **Ajouter ou Supprimer des composants Windows**.
- On fait un double clic sur **Services de mise en réseau**.
- A la fin, on coche la case **Protocole DHCP (Dynamic Host Configuration Protocol)** pour activer le serveur. Cliquer sur les boutons **OK**, ensuite sur **Suivant**, puis **Terminer**. **Fig. II.2**

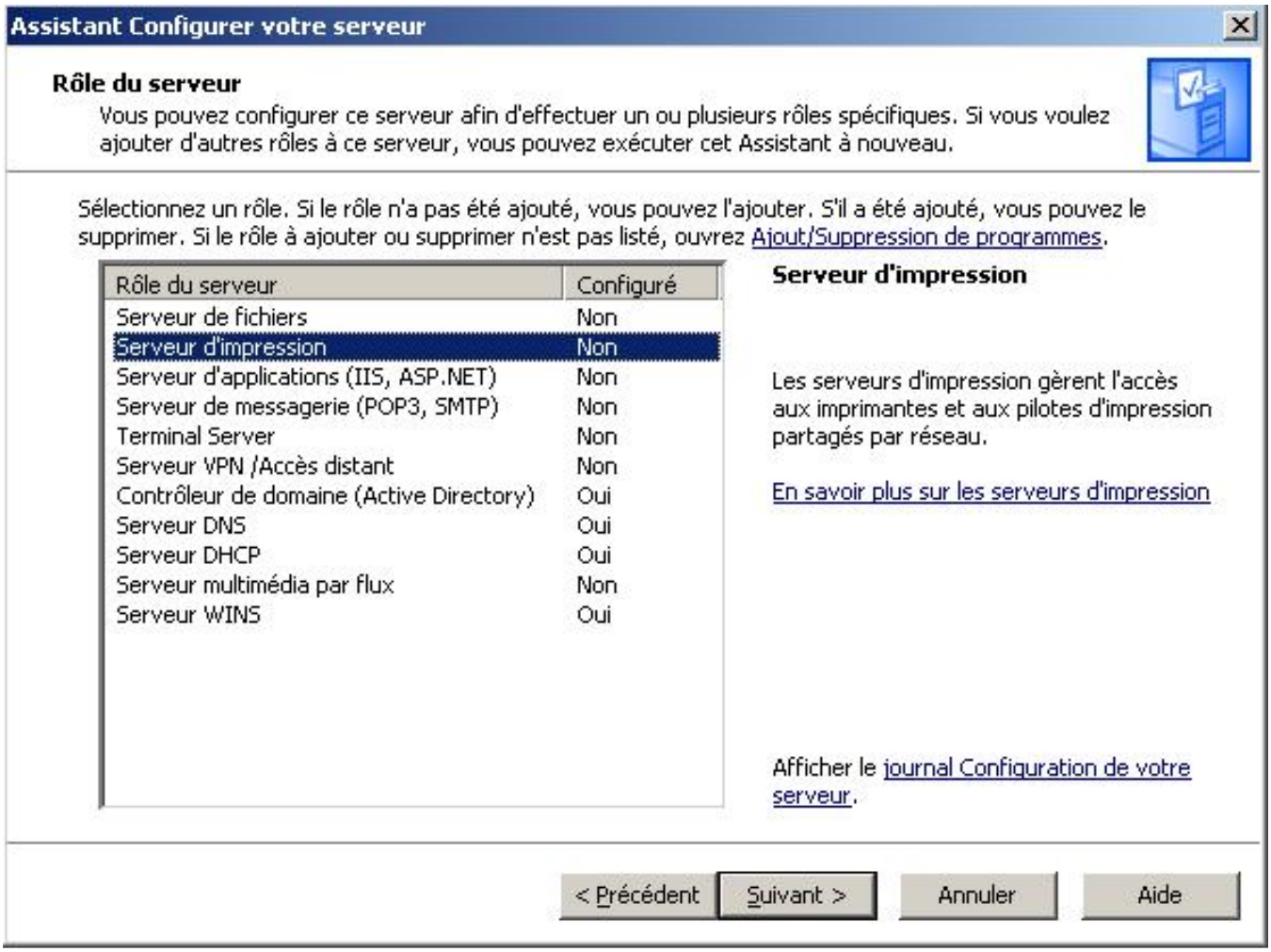


Fig. II.2 : Installation de DHCP

I.2- Configurer un serveur DHCP :

La configuration du serveur DHCP se fait après son installation. Il se trouve dans les services de mise en réseau qui sont accessibles. Pour le configurer, il faut suivre ces étapes : **Panneau de configuration > Ajout/Suppression de programmes > Composants Windows. Fig. II.3**

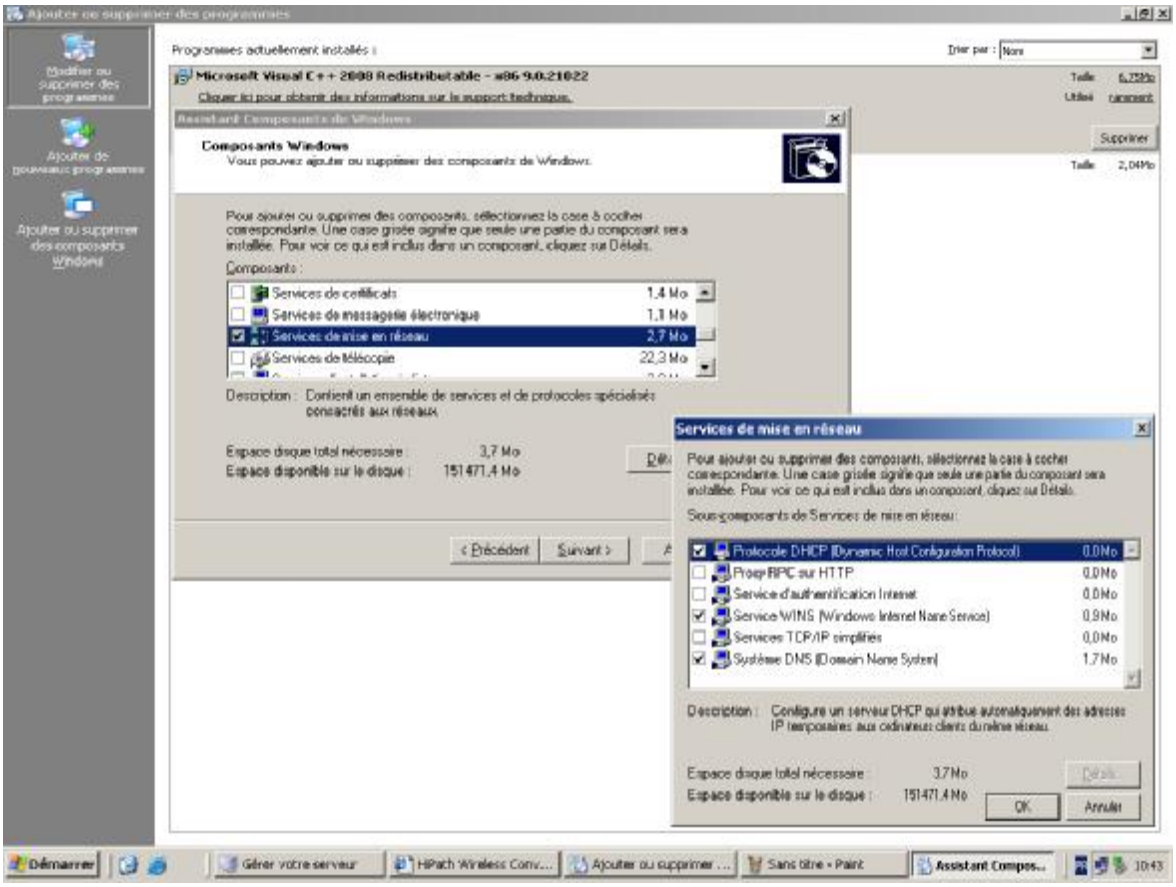
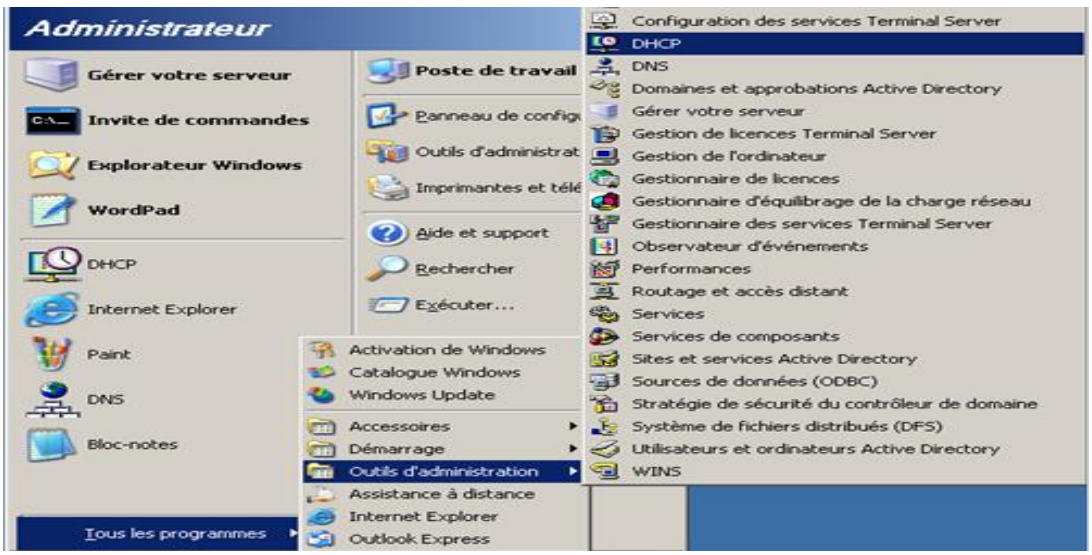
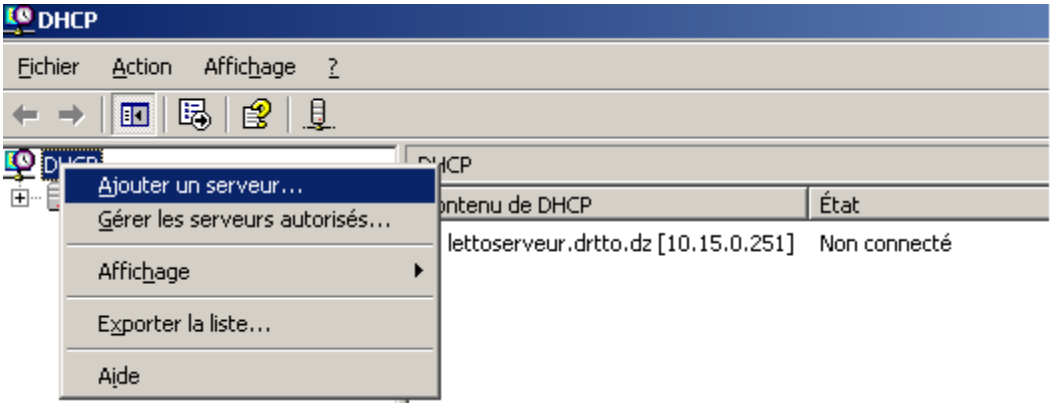


Fig. II.3 : Lancement de l'installation

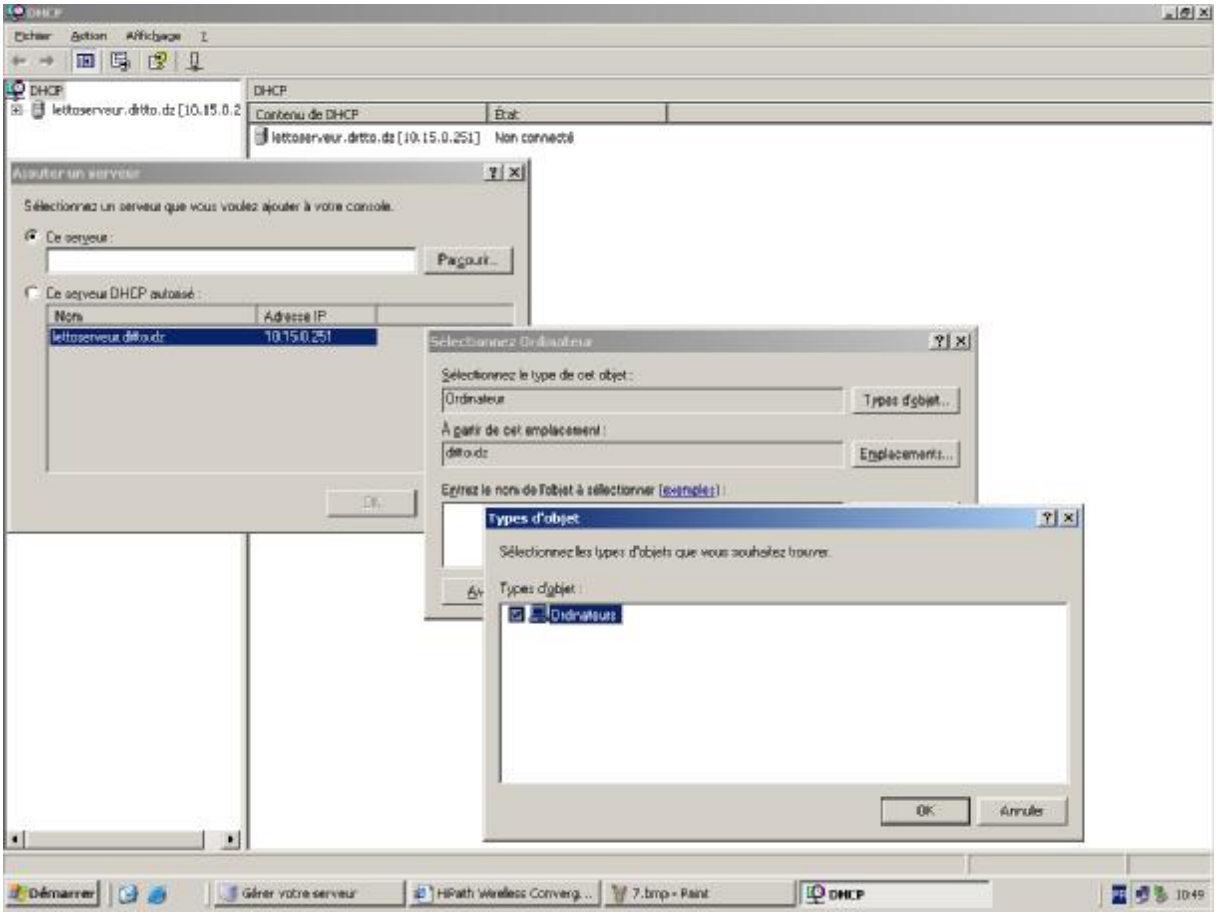
- L'installation se lance et une fois finie, on va dans menu **Démarrer > Programmes > Outils d'administration > DHCP.**



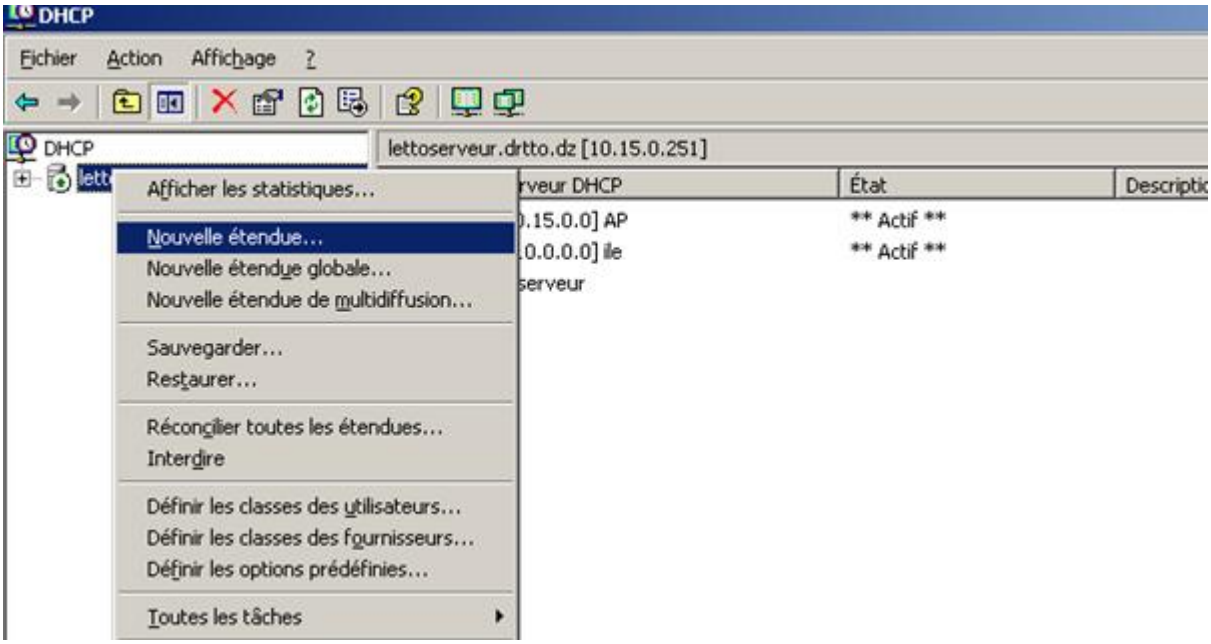
- On clique sur DHCP afin de lancer la console d'administration du serveur DHCP.
- On ajoute un serveur en faisant un clique droit sur Ajouter un serveur.



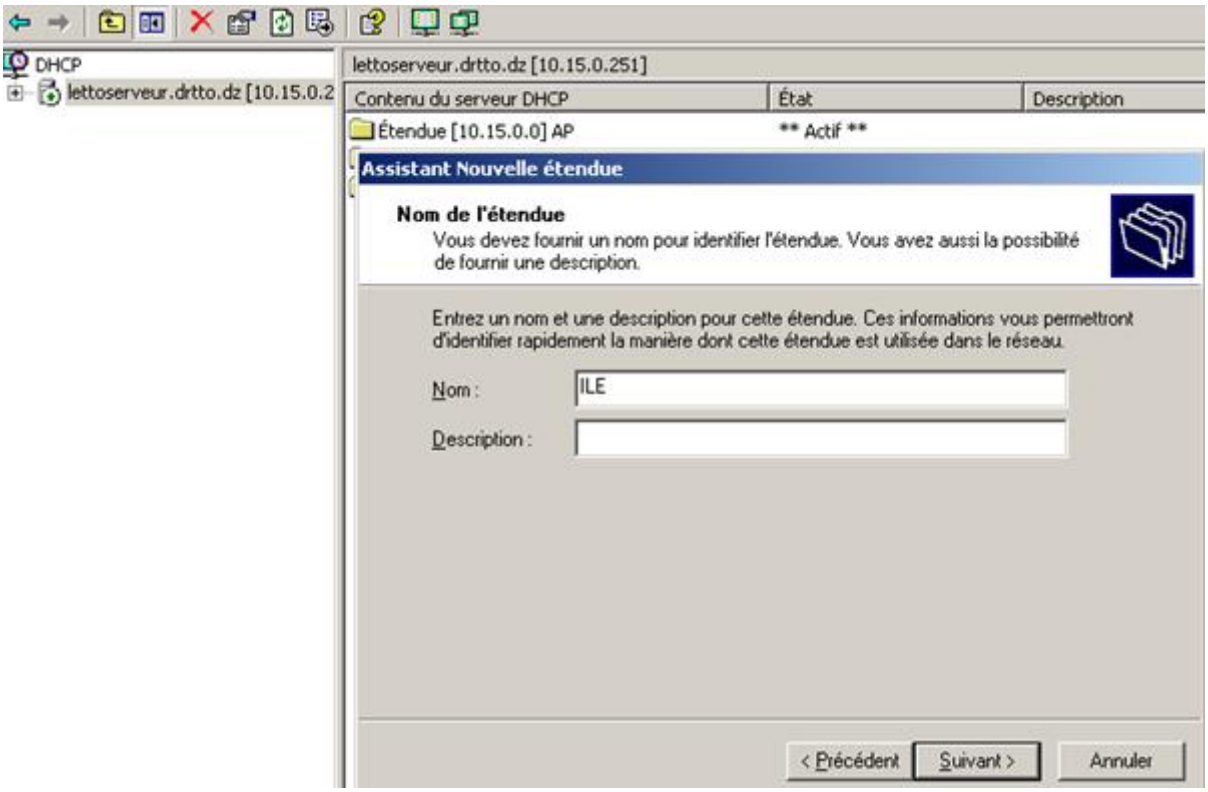
- Cocher ce serveur et faires parcourir. Sélectionner le PC qui servira de serveur DHCP. Dans notre cas c'est « ordinateur ».



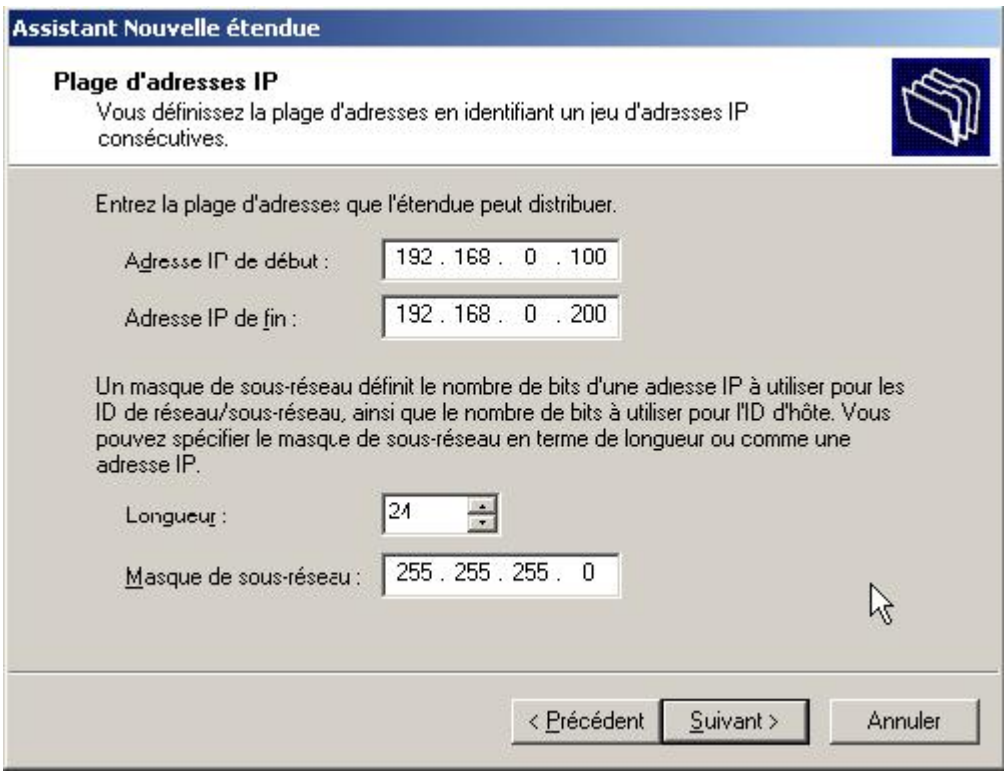
- Faites un clic droit sur le serveur et choisissez la plage d'adresse « Nouvelle étendue ». Un assistant apparaît, cliquer sur suivant. Ensuite, donner un nom puis faire suivant.



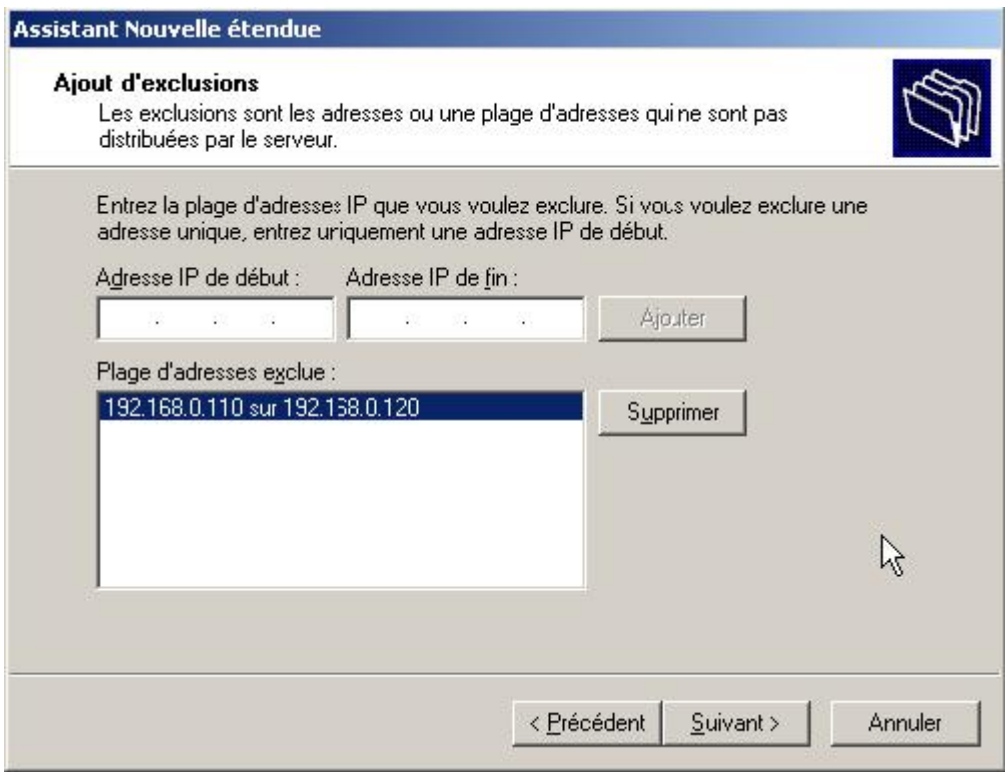
- Donner un nom a la nouvelle étendue, dans notre cas on a met ILE.



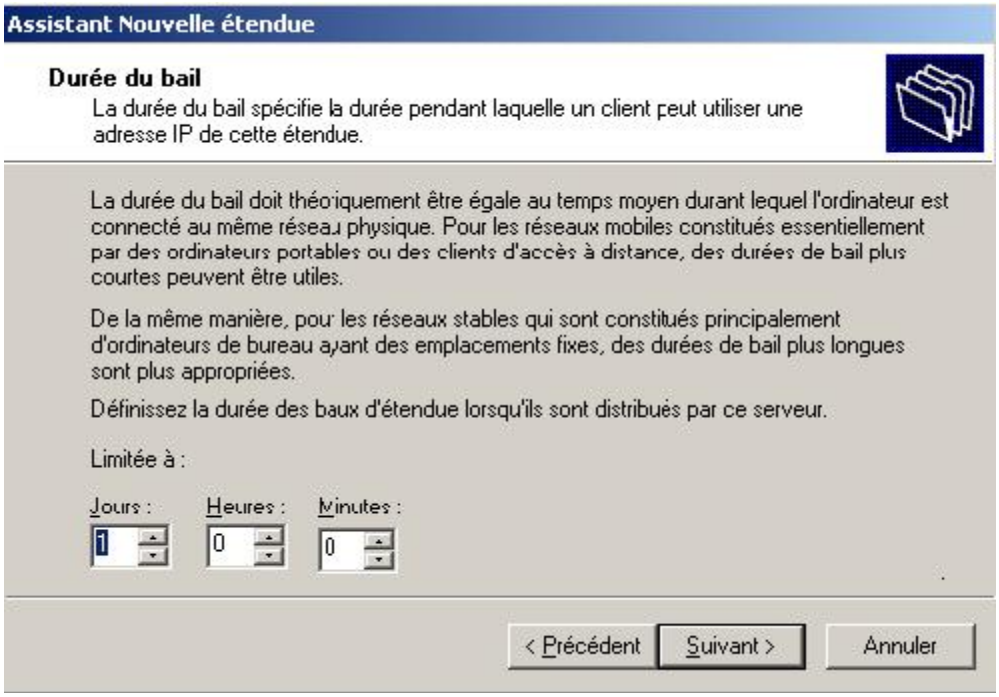
- Remplir les deux premières plages d'adresses IP que votre serveur pourra distribuer aux APs clients (la première et la dernière). Cliquer sur le bouton Suivant.



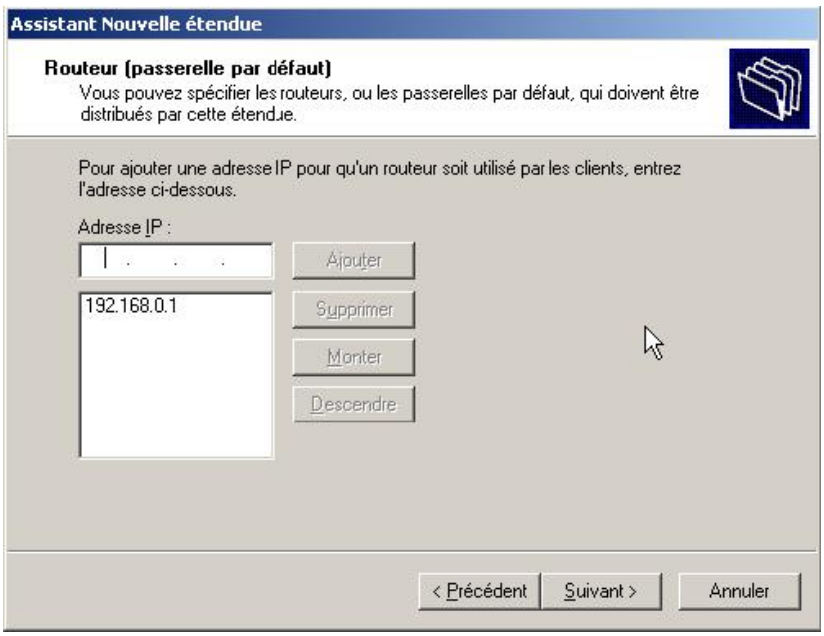
- Dans ce cas, on peut exclure des adresses (ou des plages d'adresse). Faire entrer les adresses IP à exclure de la plage et cliquer sur le bouton Ajouter



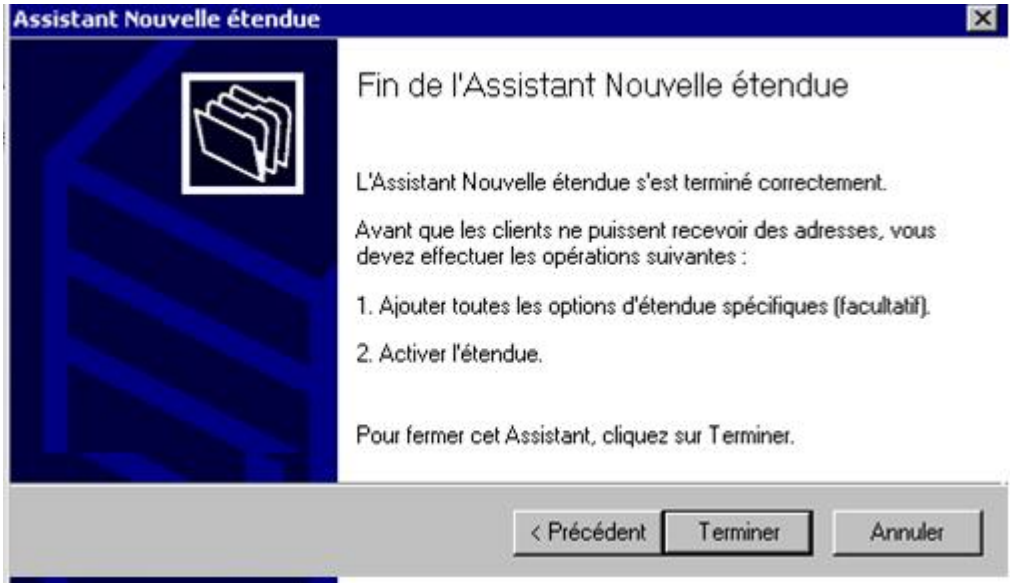
- On spécifie la durée du bail alloué aux adresses IP, et on suit les instructions données.
- Par exemple on a met 1 jour, cliquer sur le bouton Suivant.



- Cliquer sur le bouton Suivant, ensuite sur le bouton **Oui je veux configurer ces options maintenant** pour permettre à l'assistant de configurer l'étendue avec les options les plus courantes. Cliquez sur Suivant.
- Ajouter ensuite l'adresse IP de la passerelle par défaut, puis cliquer sur le bouton **Suivant**



- On clic sur terminer.



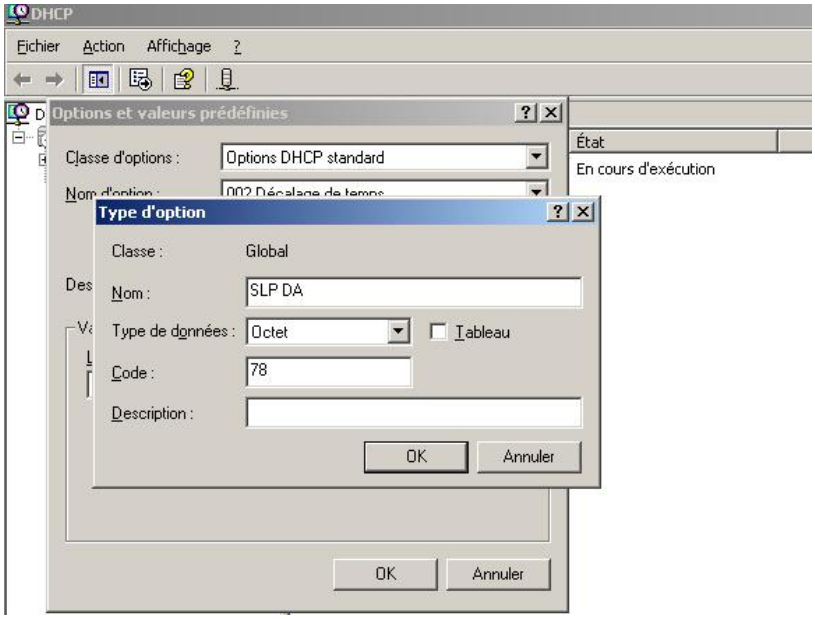
Remarque :

Pour la configuration des points d'accès ou le paramétrage des adresses IP de ces derniers, on doit cocher sur la case « Obtenir une adresse IP automatiquement »**.**

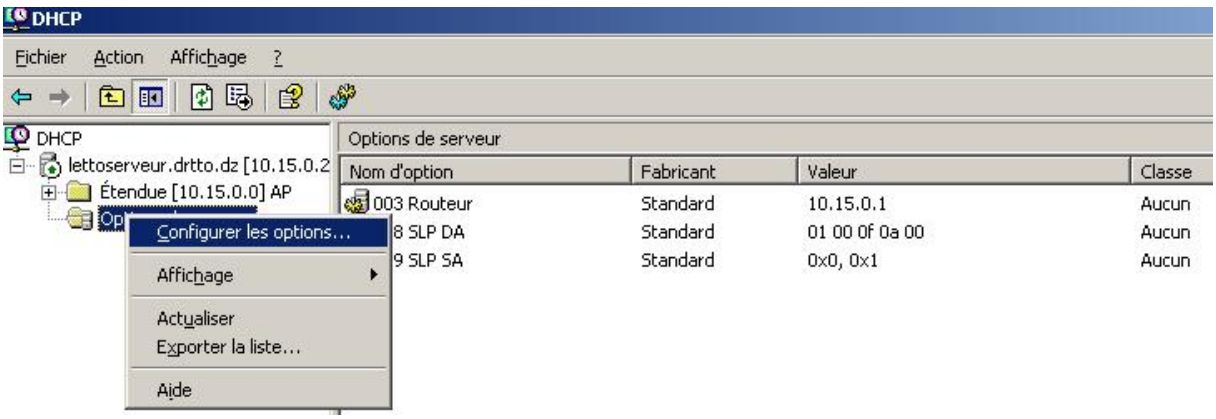
v Option 78 et 79 :

Avant de finaliser la configuration du serveur DHCP on doit crée l'option 78 comme un tableau d'octets et l'option 79 comme un tableau encapsulé.
Pour cela on va procédez comme suit :

1. Cliquer sur le bouton droit, ensuite sur le nœud du serveur puis cliqué sur le bouton **définir les options prédéfinies.**
2. Cliquer sur le bouton **ajouté** puis tapez un nom pour l'option, par exemple « SLP DA ».
3. Définir le type de données d'octets puis sélectionné la case à cocher sur le **tableau**.
4. Dans la zone appelé **code** taper le chiffre **78**.



5. Cliquer sur le bouton droit pour ouvrir le nœud **option de serveur**, puis cliquer sur le bouton **configurer les options.**



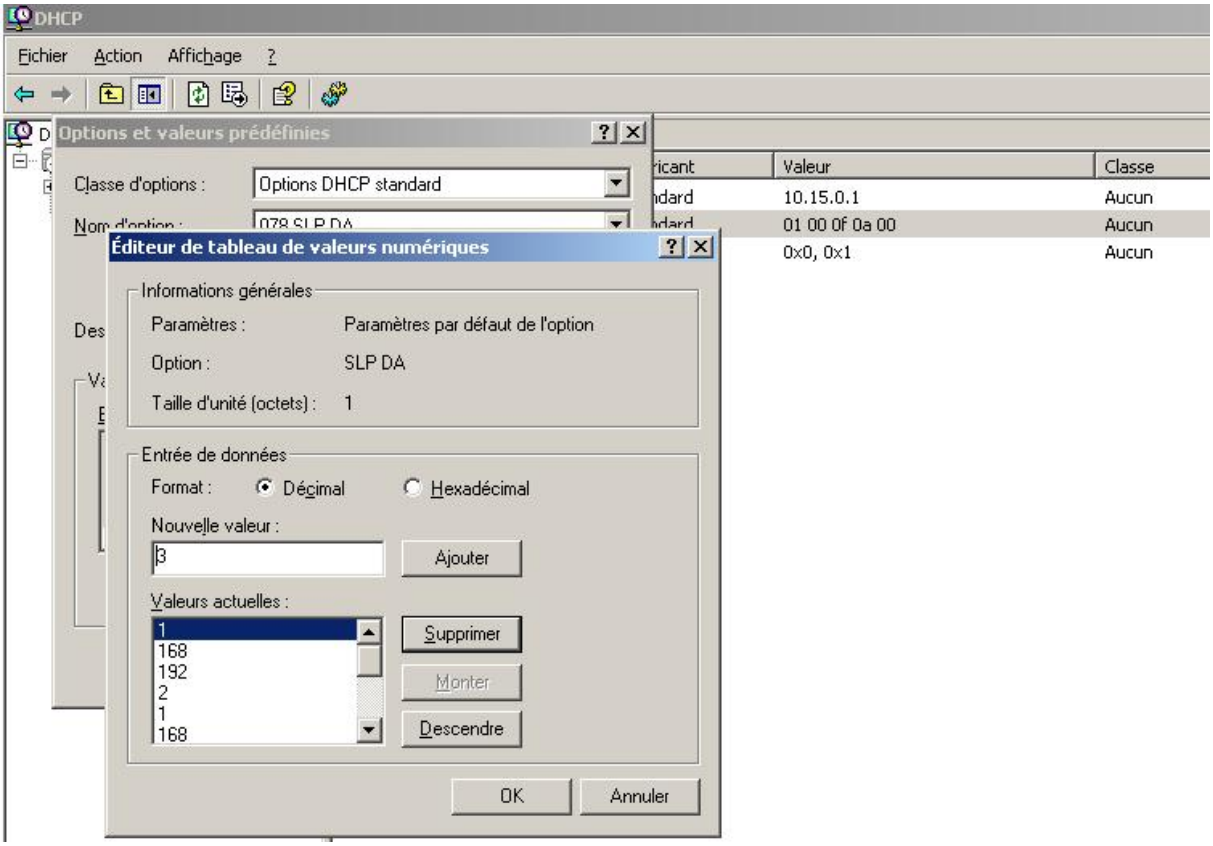
6. Cliquer sur **option 78** et entrer les données appropriées.
7. Dans la zone **obligatoire**, taper **0** ou **1** puis cliquer sur le bouton ajouter.

   Ce paramètre est important pour l'octet obligatoire. Si vous tapez **0**, une configuration statique est substitué, si vous tapez **1**, la configuration de protocole DHCP substitue les paramètres statique.

8. Taper toute les adresses IP. Dans ce cas il faut ajouter séparément chaque octet.

   Prenant l'exemple de l'adresse 192.168.1.2, taper le premier chiffre 192 ensuite cliquer sur le bouton ajouter. Cela signifie, d'ajouter un deuxième chiffre qui est 168.

Cliquer sur le bouton ajouter. Pour les deux autres chiffres (1 et 2), il faut suivre les mêmes étapes.



9. Revenir au logiciel DHCP.
10. Cliquer sur le bouton droit, ensuite sur le nœud du serveur puis sur **définir les options prédéfinies**.
11. Cliquer sur le bouton **ajouter** pour ajouter l'option 79
12. Suivre les mêmes étapes que pour **l'option 78**

On suivant toutes ces étapes, on dit qu'on a fait la configuration **du serveur DHCP**

II- Configuration du Scalence :

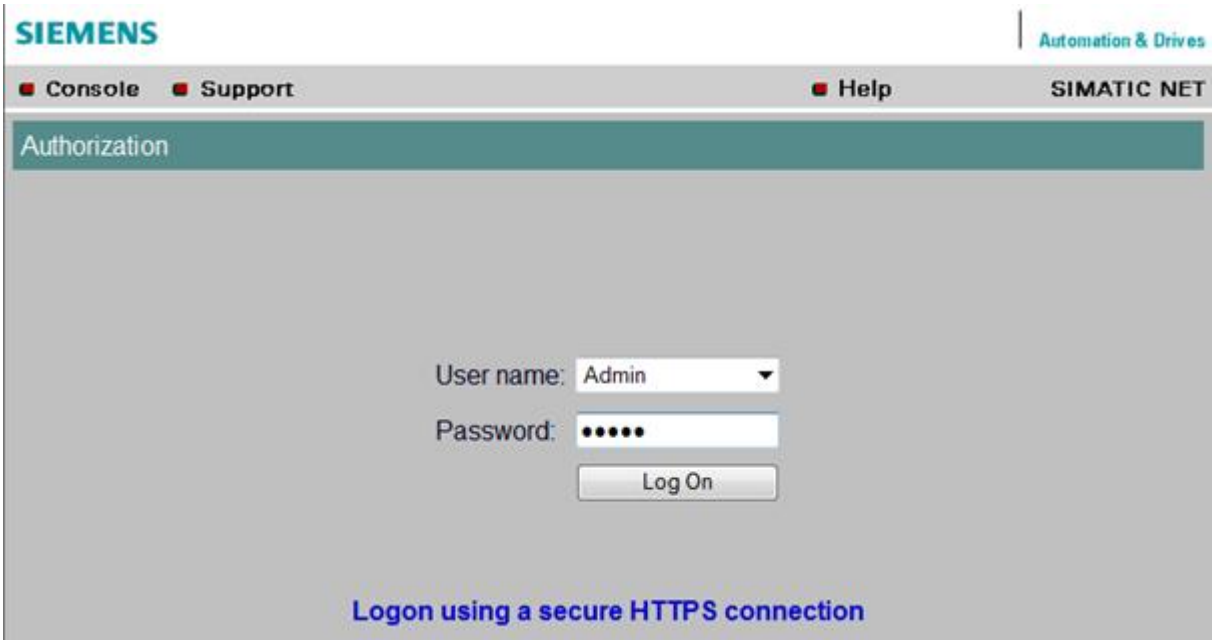
Pour accéder au scalence, il faut procéder comme suite **:**

- Un double clique sur le navigateur **Web (Internet explorer)** et on saisi l'adresse IP par défaut 0.0.0.0

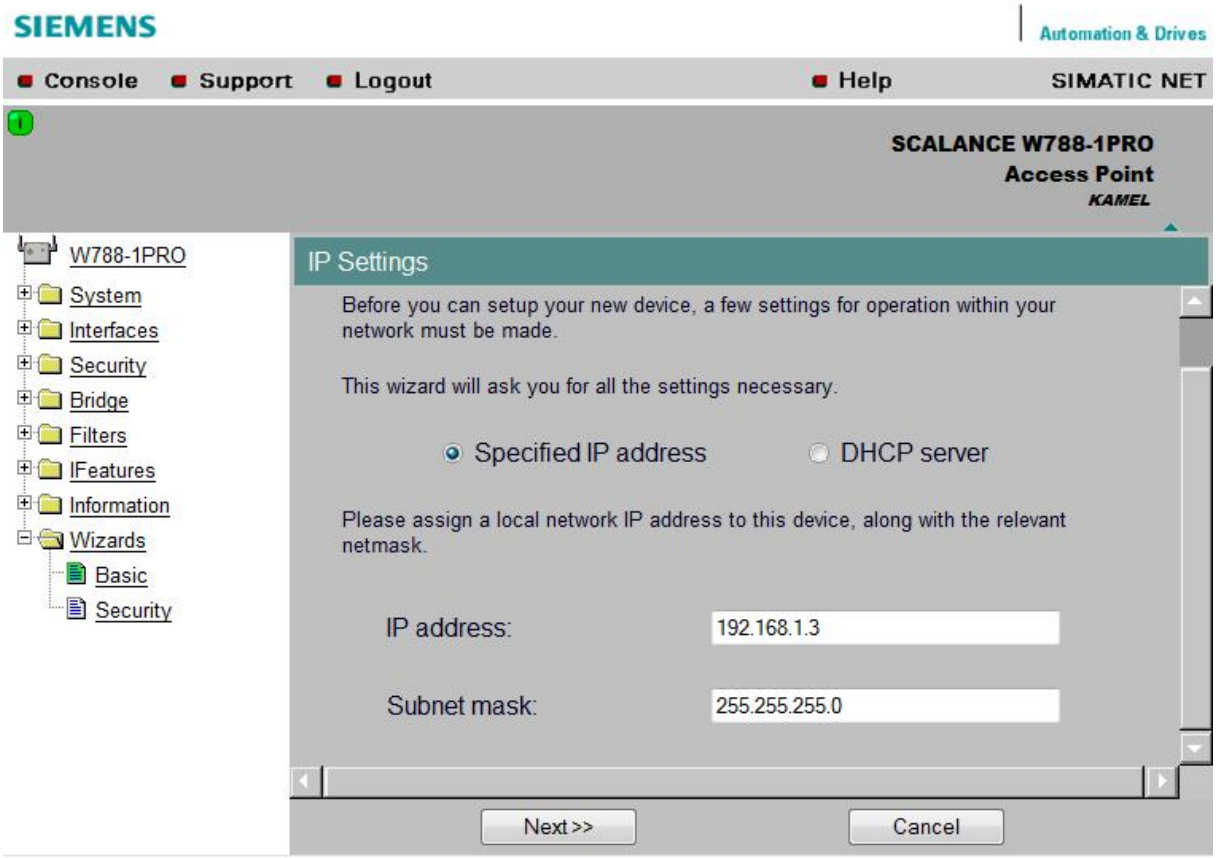
- Une boite de dialogue s'ouvre automatiquement et nous demande un login pour accéder au scalence.

ü la configuration se fait comme suit :

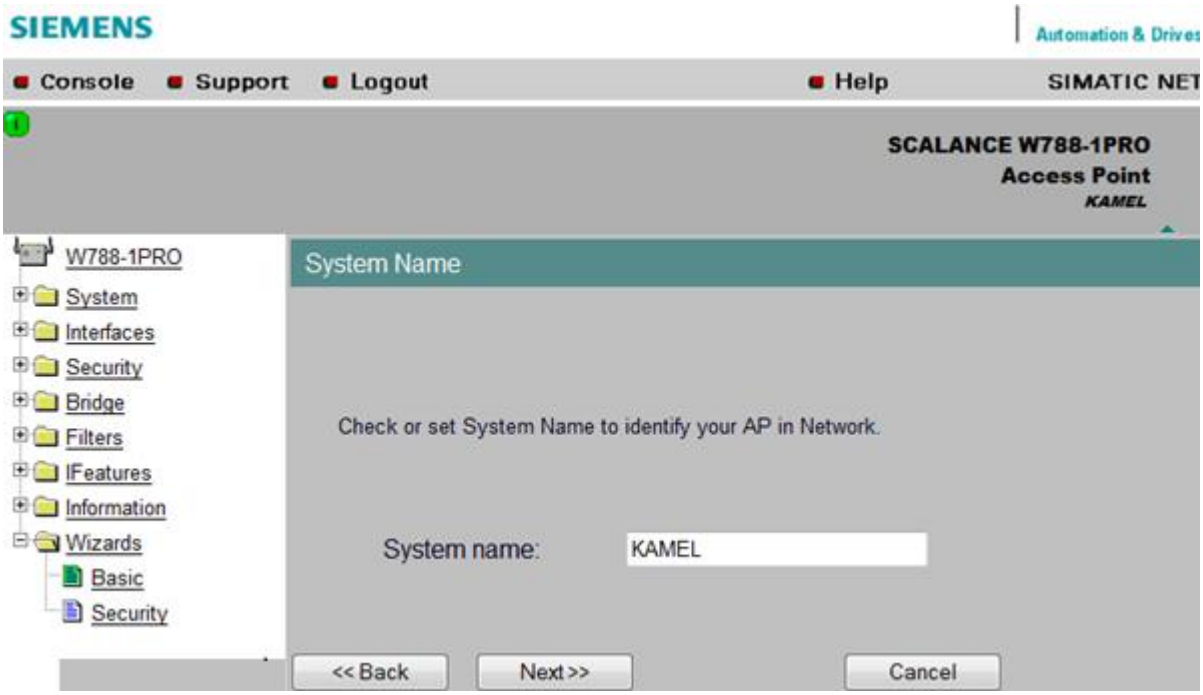
Lorsque nous nous connectons pour la première fois sur le scalence, il nous demande d'entrer le nom d'utilisateur "Admin" et le mot de passe par défaut est "admin".



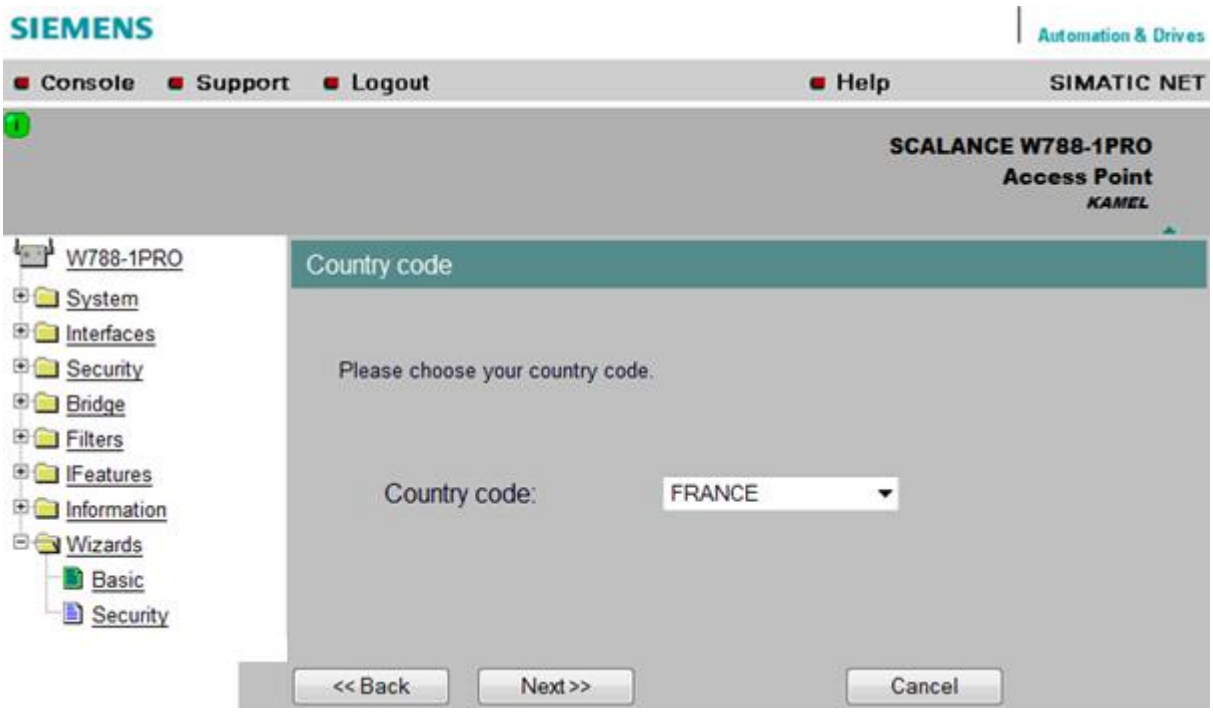
- Cliquer sur la touche **wizards** puis **basic,** ensuite écrire l'adresse IP du scalence. Remplir la case **masque sous réseau** ensuite appuyer sur le bouton **next**.



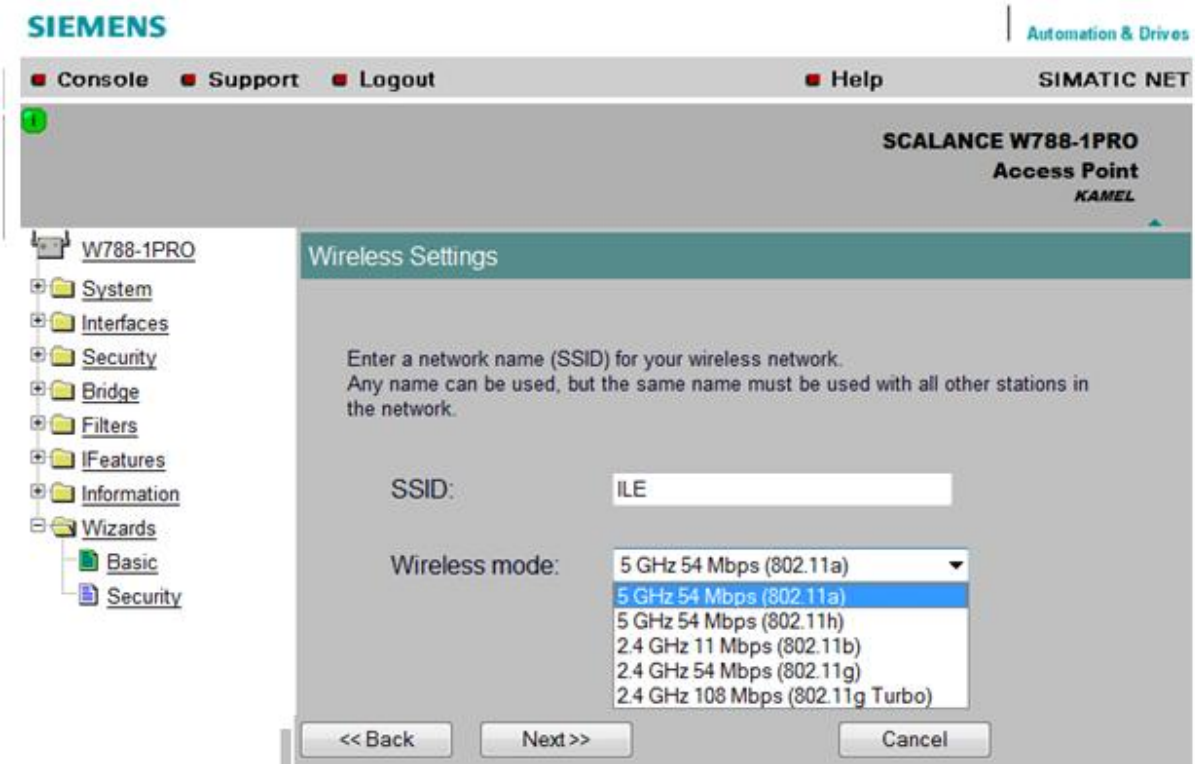
- Donner un nom au scalence. Dans ce cas, on a proposé le prénom « kamel ». Cliquer sur le bouton **next**.



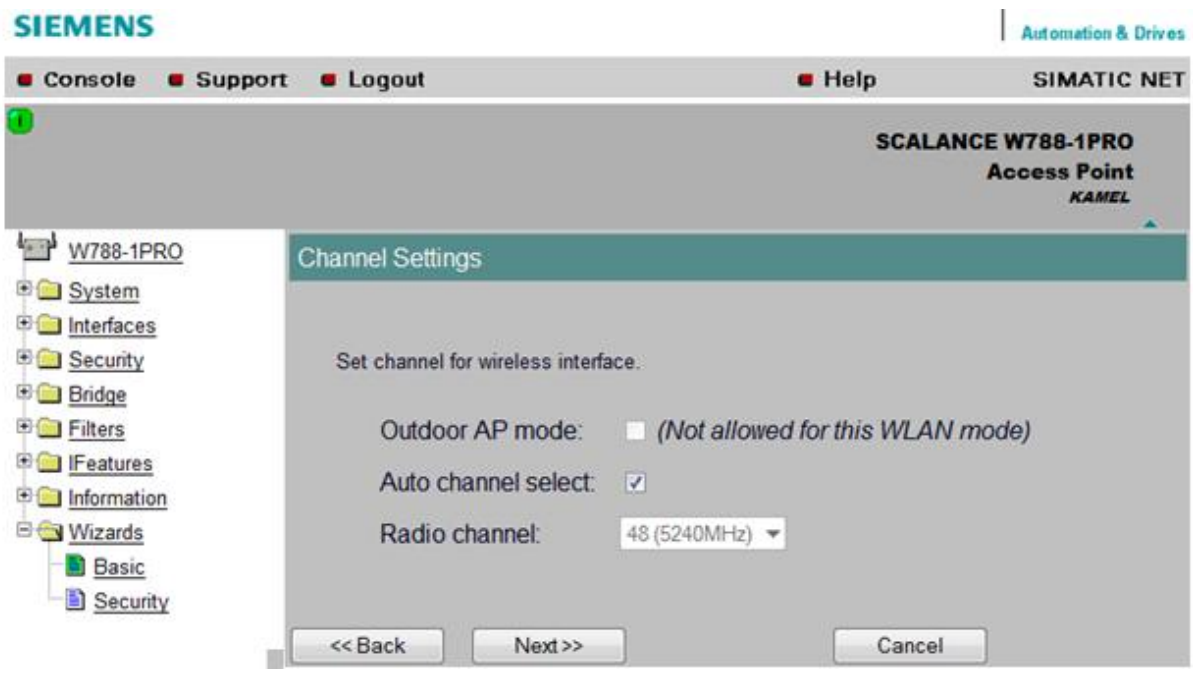
- Pour country code on a choisit le payé « France » : Ce choix est fait parce que le code de notre payé l'Algérie ne figure pas sur la liste. Cliquer sur **next**.



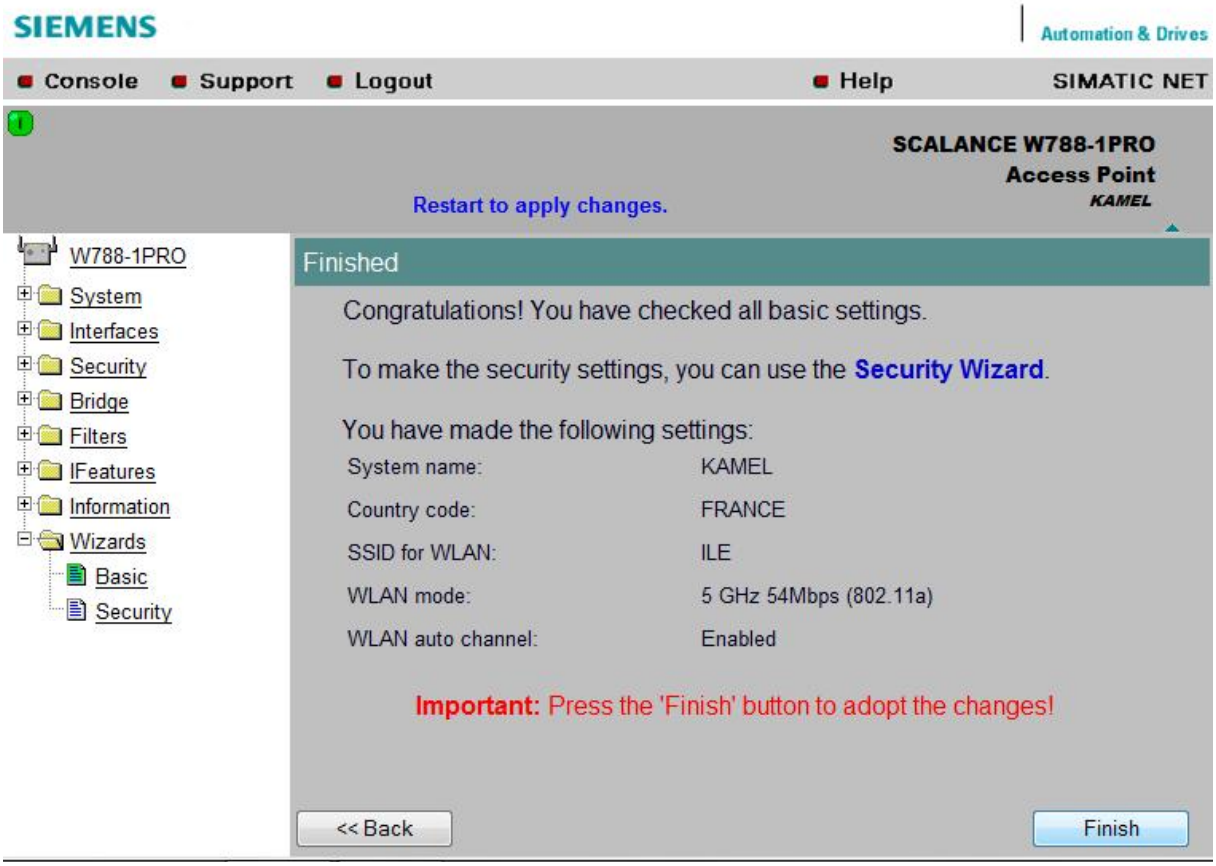
- Donner un nom au réseau SSID, on a proposé dans notre cas « I L E ».
- Choisir les références du câble utilisé (5 GHz 54 Mbps (802.11a)). Ceci défini la norme des wireless setting, taper sur le bouton **next**.



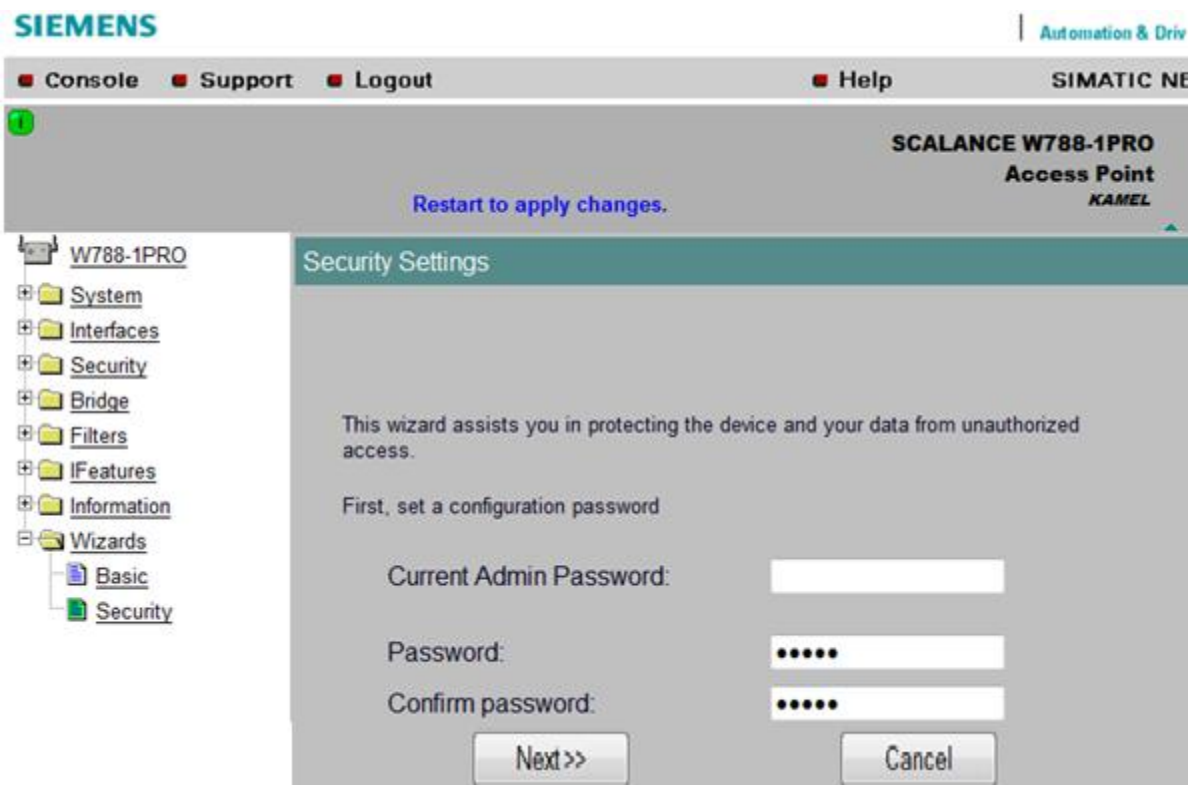
- Sur la fenêtre **« Channel setting »,** cocher la case **auto channel select**, pour rendre le choix de la fréquence RADIO automatique.



- Appuyer sur la case finish pour terminer la première étape de la configuration.



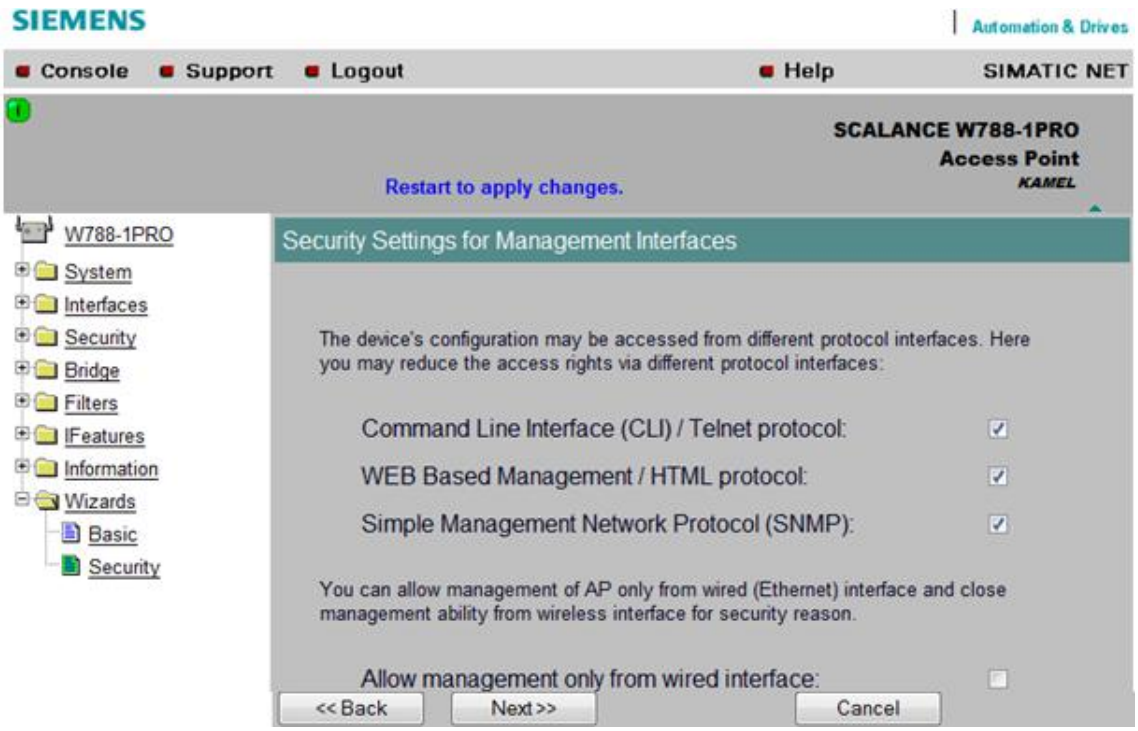
- Concernant la sécurité, cliquer sur le bouton **security**, écrire le mot de passe et confirmer ce choix, ensuite activer la case **next**.



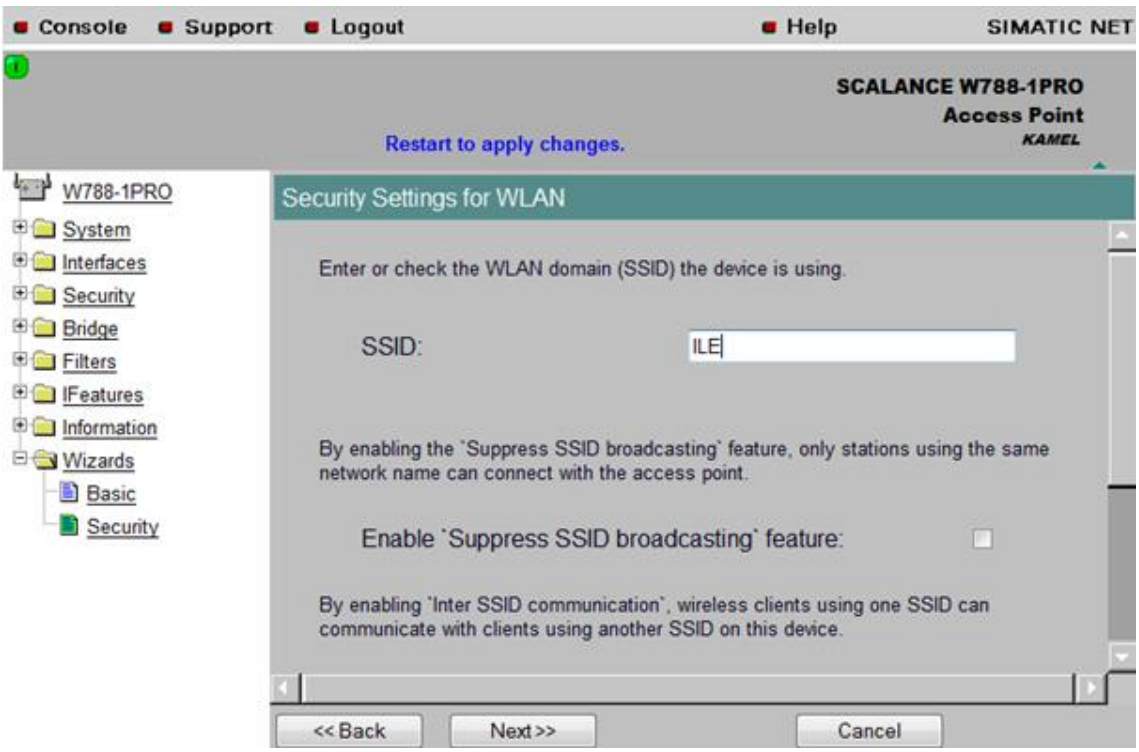
Pour accéder à l'interface graphique du scalence il y'a trois méthodes :

- Telnet Protocol (CLI) : l'invité de commande.
- HTLM Protocol : internet explorer.
- SNMP Protocol : un service de messagerie.

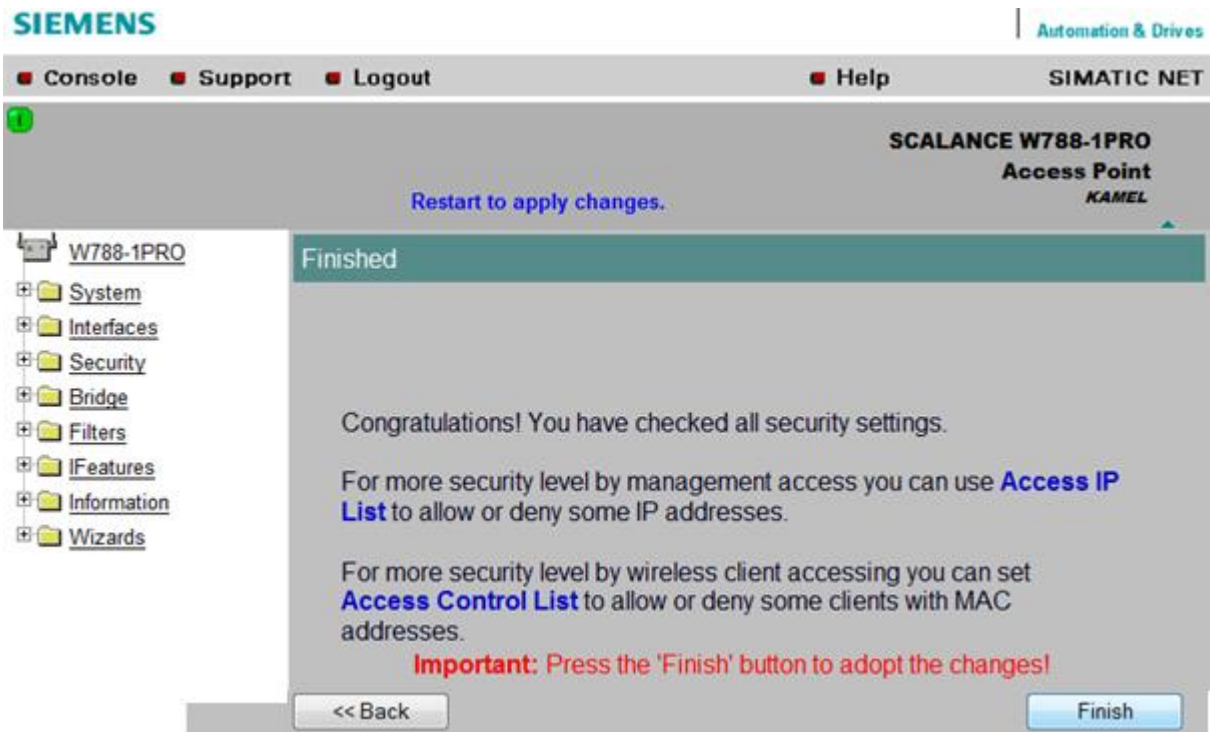
Pour activer ou désactiver l'une des trois méthodes il suffit de cocher ou décocher sa case.



- Entrer le mot choisi pour le domaine SSID. Ici, notre choit est porté sur ILE.



- Cliquer sur la case Finish.



De cette façon on a terminé la configuration du scalence.

III- La configuration du contrôleur :

A fin d'assurer l'enregistrement des points d'accès sur le contrôleur, on doit commencer par la configuration du contrôleur avant de configurer les points d'accès :

III.1- L'accès au contrôleur :

Pour accéder au contrôleur, il faut emprunter le chemin suivant :

- Un double clique sur le navigateur **Web (Internet explorer)** et on saisi l'adresse IP du contrôleur par défaut.
- Une boite de dialogue s'ouvre automatiquement. Elle va nous demander un login pour l'accès au contrôleur. **Fig. II.4.**

Fig. II.4 : L'accès au contrôleur par (Login).

Pour l'accès, taper le nom et le mot de passe, ensuite, cliquer sur Login, le menu principal de l'assistant Hipath Wireless est affiché sur l'écran. **Fig. II.5**

Fig. II.5 : Menu principal du HWC.

III.2 Les étapes de la configuration du contrôleur :

Pour commencer la configuration du contrôleur dans le Menu principal. On clique sur le bouton **Wireless Controller configuration**. La fenêtre de l'assistant de *Wireless Controller configuration* est affichée sur l'écran

a) IP Adresses: cette commande permet de configurer l'identifiant du contrôleur (les adresses IP, le nom, les interfaces **(esa1** et **esa0)…etc**). **Fig. II.6.**

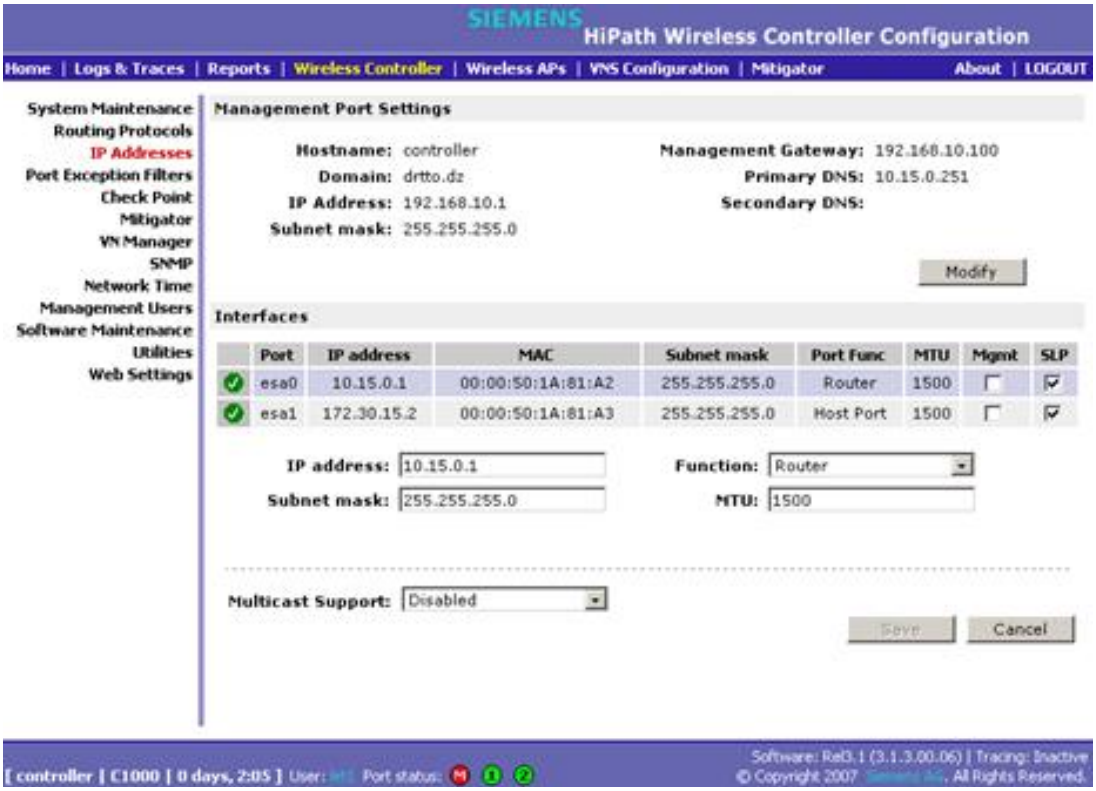


Fig. II.6: Les commandes de « IP Adresses ».

On clique sur le bouton **Modify** afin de modifier l'identification du contrôleur, comme suit :

- **Hostname** : le nom de contrôleur (Controller).
- **Domain:** le nom de domaine d'entreprise, on choisi le domaine de Direction Regionale des Télécommunication de Tizi–ouzou (drtto.dz).
- **Management IP Address:** représente l'adresse de contrôleur (192.168.10.1).
- **Subnet mask** : défini le masque sous réseau (255.255.255.0).
- **Management Gateway** : c'est une passerelle pour le réseau (192.168.10.100).
- **Primary DNS:** c'est l'adresse du serveur DNS principale (10.15.0.251).
- **Secondary DNS:** représente le serveur DNS secondaire.

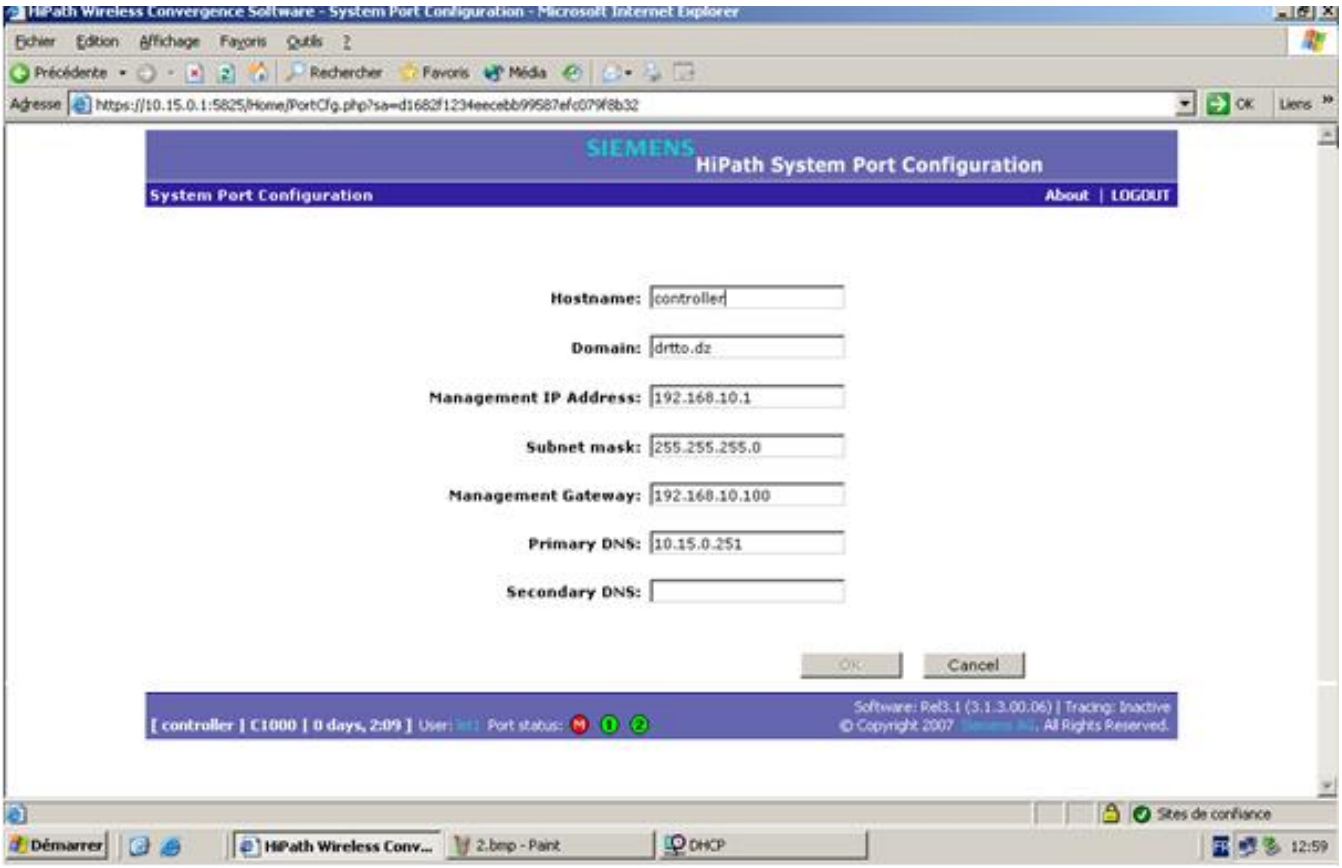


Fig. II .7: Fenêtre Modify.

Interfaces optique :

C'est la partie intérieure de la fenêtre, on doit configurer les paramètres des deux interfaces (Esa1 et Esa0), come suit:

- **IP Address**: représente l'adresse IP du port de l'interface (10.15.0.1).
- **Subnet mask** : c'est le masque sous réseau de port par default (255.255.255.0).
- **MTU (**Maximum Transmission Unit): la taille maximale de paquet pour la transmission, par default est 1500 kb/s.
- **Function** : elle est définie par l'une des trois paramètres suivants :

– **Host Port:** spécifie le port pour relier les APs sans chemine dynamique.

– **Third-Party AP Port** : dans le cas ou on a utilisé d'autre marques des point d'accès.

– **Router** : Spécifié le port, si on veut relier ce port avec un autre port d'un routeur.

– Dans notre cas on a choisit **Router**

a) Routing Protocol :

On utilise cette commande pour le routage de réseau. Il permet de tracer la route du paquet de données, soit avec un chemin statique ou en employant le protocole de routage dynamiques (OSPF). Dans notre cas on utilise le chemin statique, car on a besoin d'accès à internet. La configuration de **Static Routes** se fait comme suit **Fig. II.8**:

Fig. II.8 : Les commandes de « Static Routes ».

- **Destination Address :** l'adresse de groupe des clients (l'adresse de VNS) définie l'adresse de destination des paquets. Comme adresse on a choisi (0.0.0.0).
- **Subnet Mask:** cette commande est le masque sous réseau (0.0.0.0).
- **Gateway :** cette case est réservé pour l'adresse de passerelle soit (routeur, Firewall, modem...etc.) pour l'accès à un réseau extérieur.
- **Un** click sur **Add**: cette commande sert à modifier les paramètres de la liste.

Remarque :

OSPF Routing: Cette commande est utilisée pour le routage dynamique, car l'OSPF est un Protocol de routages dynamiques**.**

e) Port Exception Filtring :

Cette commande permet de filtrer les paquets qui sont arrivés de l'extérieur du réseau, généralement elle est utilisée pour la sécurité. En choisissant les protocoles des paquets à filtrer (TCP, UDP, IP…). Dans notre cas on garde la configuration de cette commande par défaut. **Fig. II.9**

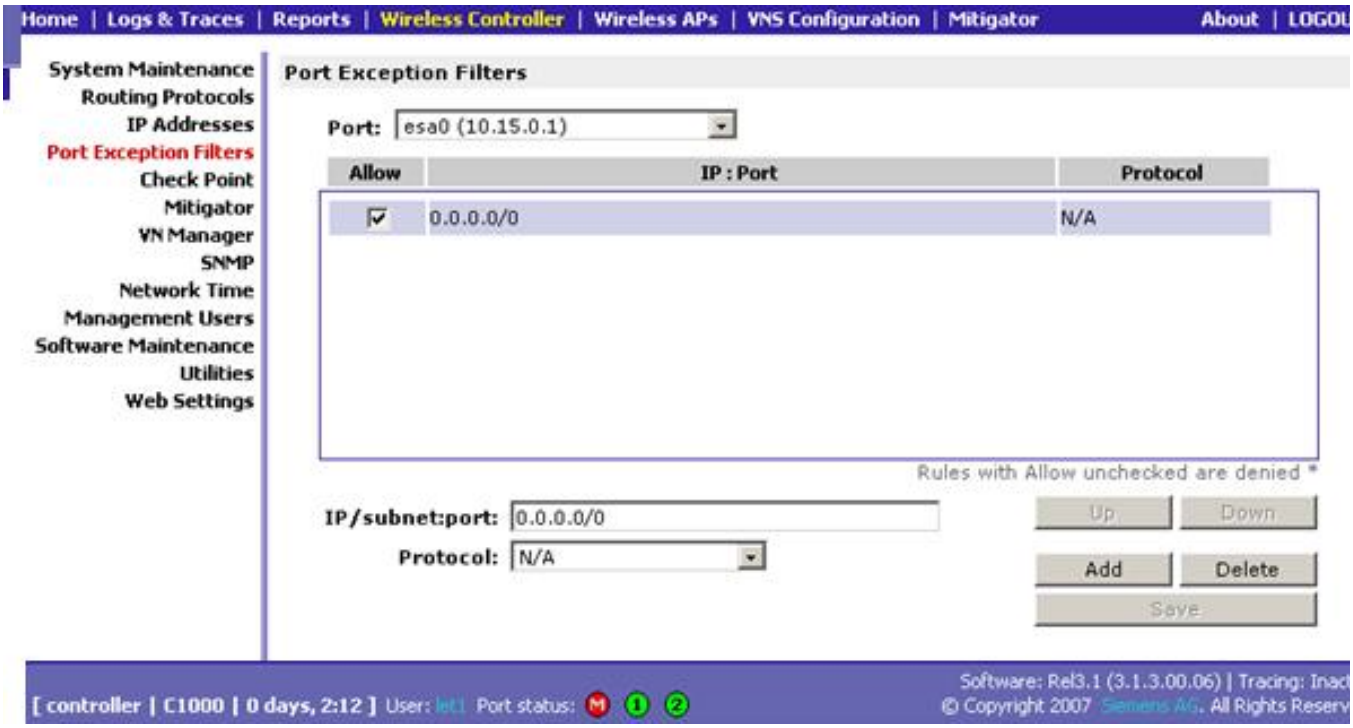


Fig. II. 9 : Les commandes de « Port Exception Flirting ».

d) Check point:

Il est aussi appelé firewall, il est certifié par ***OPSEC*** société de programmation spécialisée en systèmes intelligents. Il permet de sécuriser et de sauvegarder des données sur internet. La configuration de cette étape n'a pas été faite. **Fig. II.10**

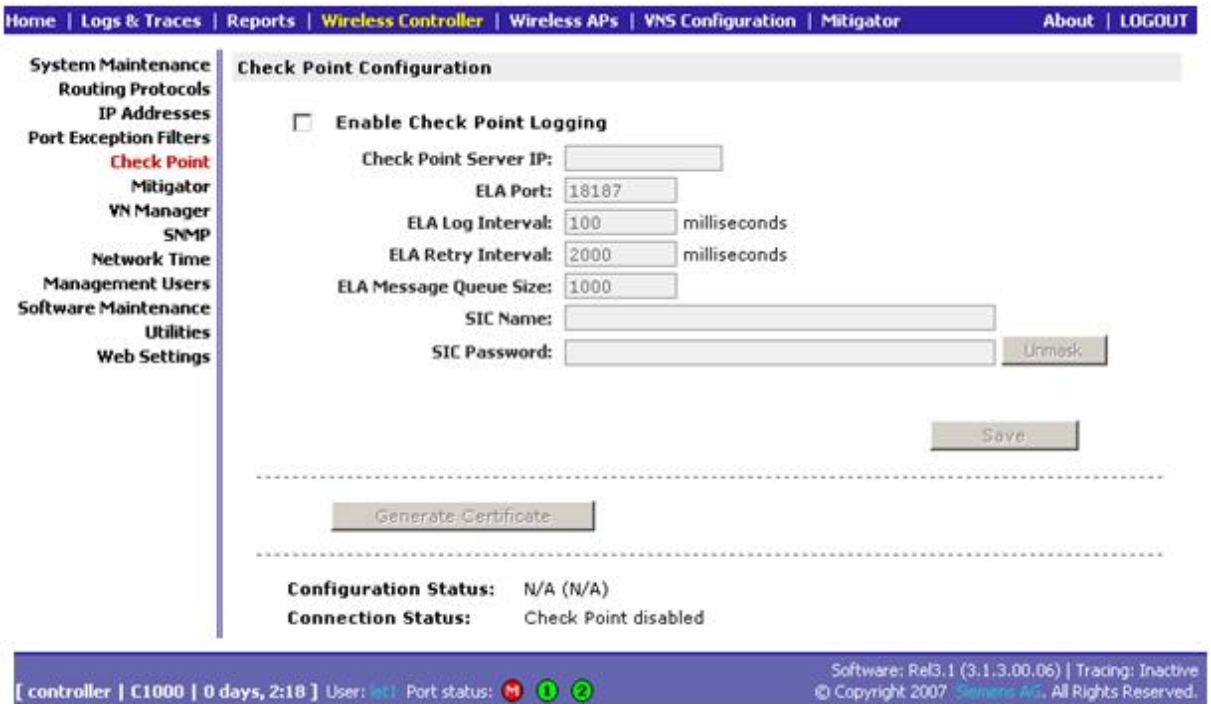


Fig. II.10: Les commandes de « Check point »

e) **Network Time**:

Cette commande sert pour la synchronisation des éléments du réseau par une horloge universelle, ou bien par l'utilisation de Protocol NTP (Network Time Protocol). C'est une commande standard utilisée par des serveurs d'horloges atomique pour ajuster périodiquement l'horloge des ordinateurs clients. **Fig. II.11**

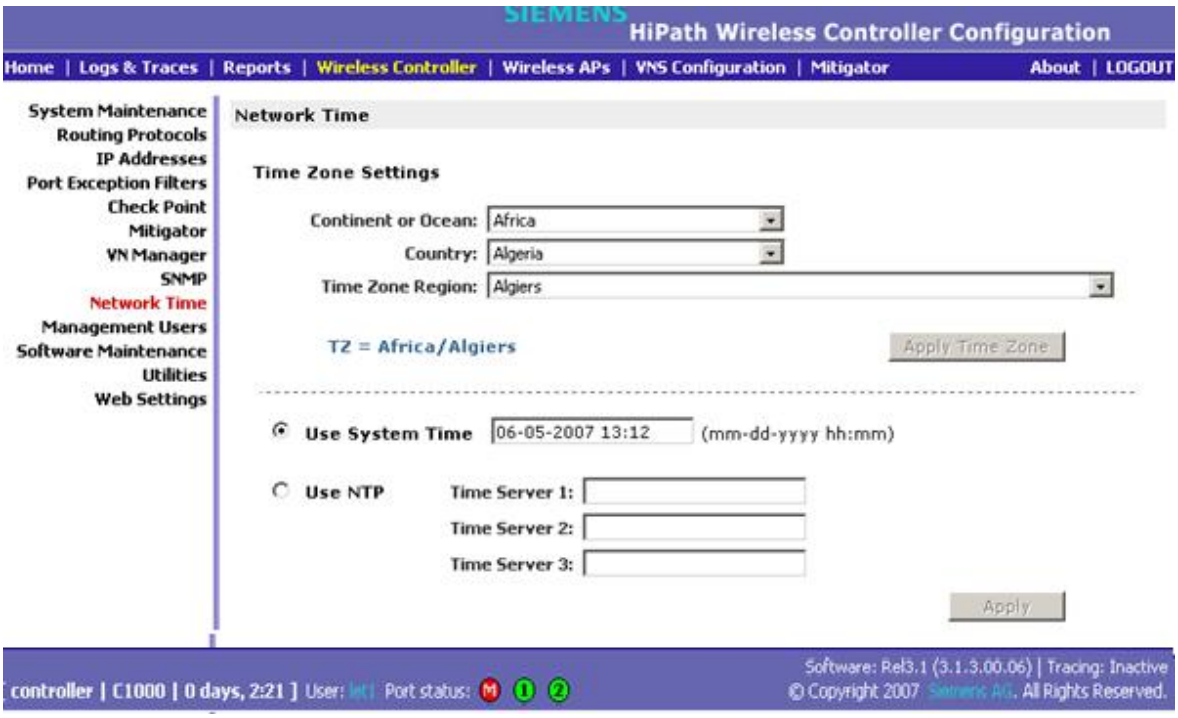


Fig. II.11 : Les commandes de « Network Time ».

f) Management User:

Cette commande nous permet de modifier le contenu par le bouton ajouter ou supprimer. Les utilisateurs des sessions soit administrateur, qui ont le privilège administrateur (Read /write) ou utilisateur avec le privilège (Read), comme montre la figure ci-dessous :

Fig. II.12 : Les commandes de « Management Users ».

g) Software Maintenance :

Cette commande permet d'améliorer le fonctionnement du contrôleur. A partir des options qui sont présentées sur la figure ci dessous, nous pouvons télécharger les mises à jour et la licence, ainsi que les nouvelles versions pour le système d'exploitation du contrôleur.

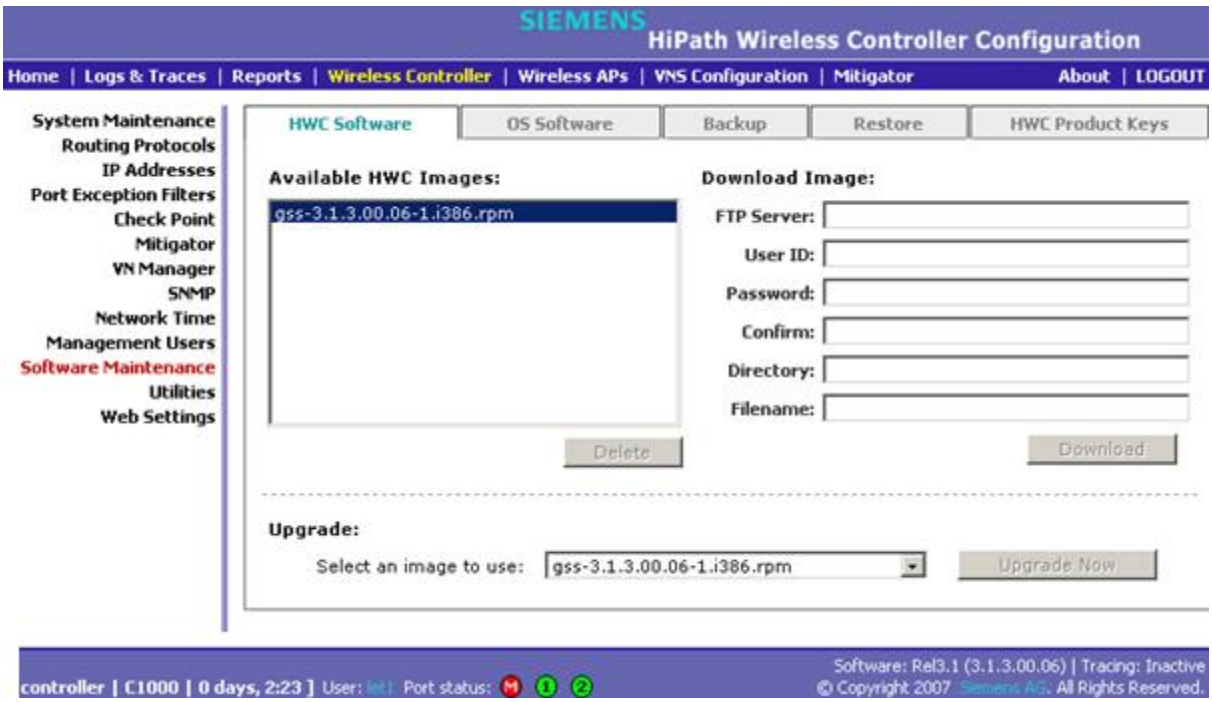


Fig. II.13 : les commandes de « Software Maintenance ».

h) Utilities :

Ce paramètre est composé de deux commandes :

Ping : Pour tester la continuité de la liaison.
Trace route : Pour déterminer l'itinéraire de la liaison.

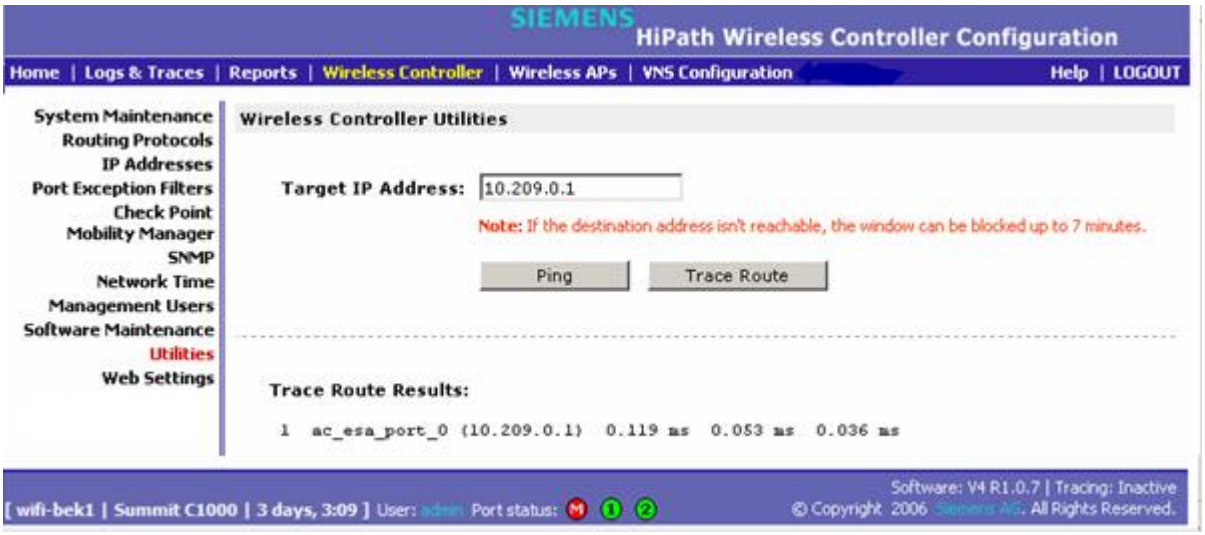


Fig. II.14 : La fenêtre d'Utilities.

i) Web Settings :

Cette commande limite la période de temps pour mettre la session en veille. **Fig. II.15.**

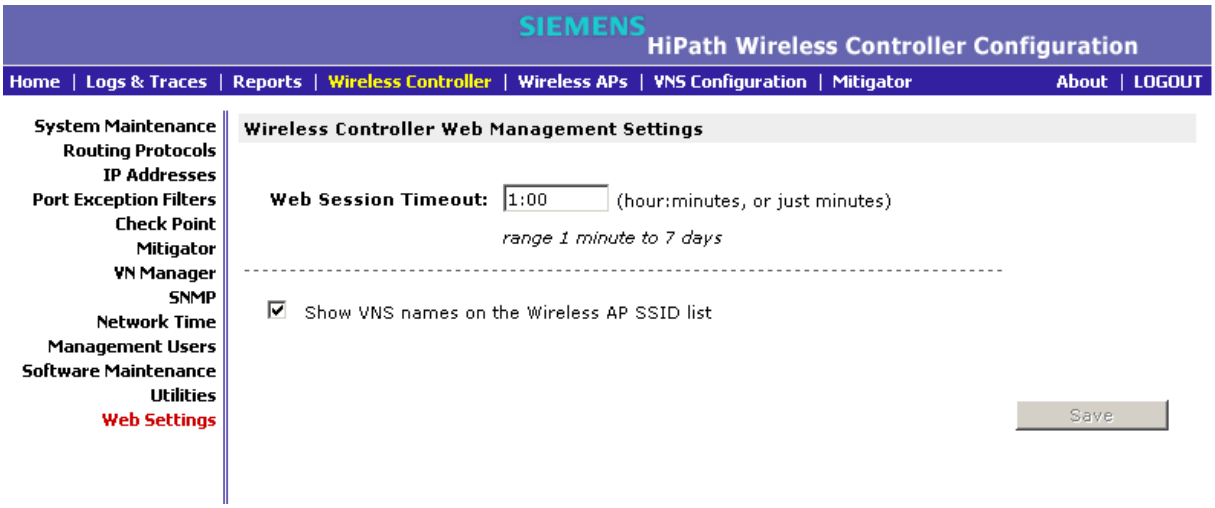


Fig. II. 15 : la fenêtre de Web Setting.

III.3 Configuration des APs :

Avant de commencer la configuration des APs (points d'accès), Il faut s'assurer de plusieurs points:

- L'ensemble des points d'accès sont reliés et branchés physiquement avec le contrôleur.

- Le contrôleur est installé et configuré.

- L'installation d'un serveur DHCP (sous Windows 2003 Server) permet d'assurer l'attribution des adresses IP aux différents APs.

a) Wireless AP configuration:

La configuration se fait en suivant plusieurs étapes:

Cliquer sur le bouton « menu principal » ensuite sur le bouton **Wireless AP configuration**. Une fenêtre s'affiche, elle indique la liste de tous les APs qui sont enregistrés sur le contrôleur par leur numéro de série. Sur la fenêtre principale « ***AP propriety***», on peut modifier les propriétés de chaque point d'accès (AP) manuellement, comme le montre la **Figure II. 16**. Dans cette étape, nous avons modifié les noms et le rôle des points d'accès, à partir du contrôleur.

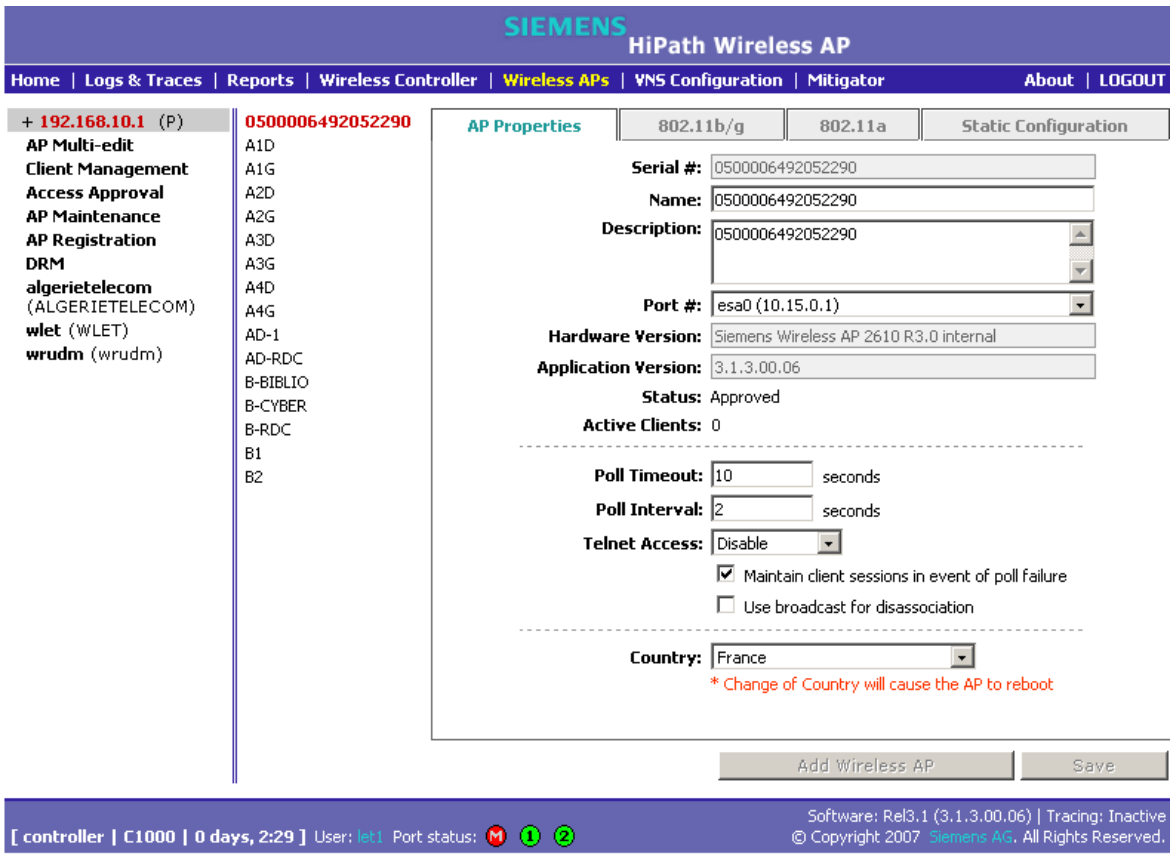


Fig. II.16 : Les commandes de « AP propriety ».

b) 802.11b/g et 802.11a :

Cette commande modifié les paramètres radio pour chaque point d'accès (AP), on choisi l'AP à configuré et on sélectionne la norme, par exemple (802.11b/g, au 802.11a).

Remarque :

Cette étape n'est pas configurée car nous allons utiliser le service **DRM.** Nous allons détailler ce service par la suite.

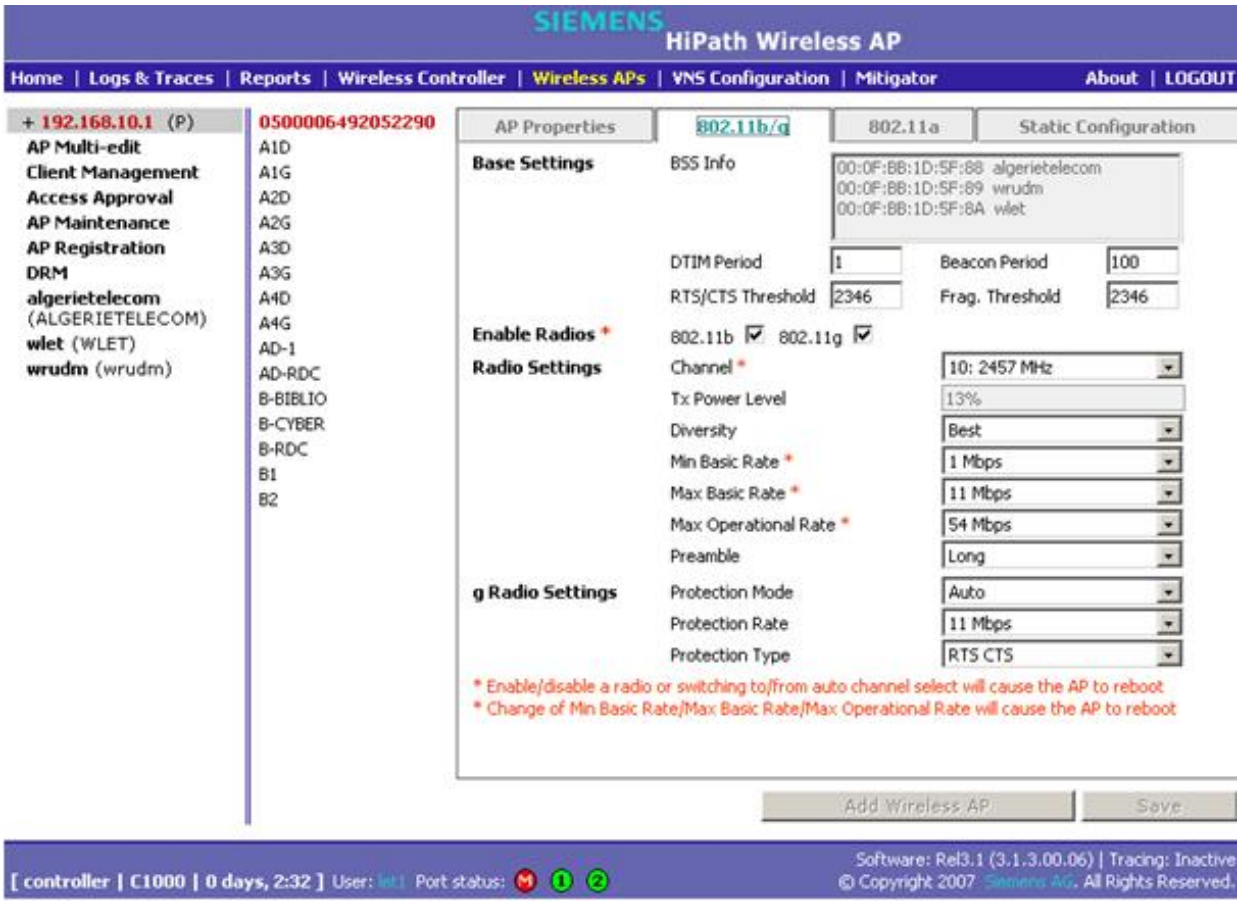


Fig. II.17 : les commandes de « Normes 802.11b/g et 802.11a **».**

b) Statice Configuration :

Cette commande est utilisée pour identifier l'AP. Dans ce cas nous avons activé la commande **VLAN Setting**. Ensuite, choisir la fonction **Untagged.** Ceci pour désactiver l'utilisation de VLAN. Sur **IP Address Assignment** on coche la commande **Use DHCP,** pour que l'AP reçoive une adresse IP automatiques.

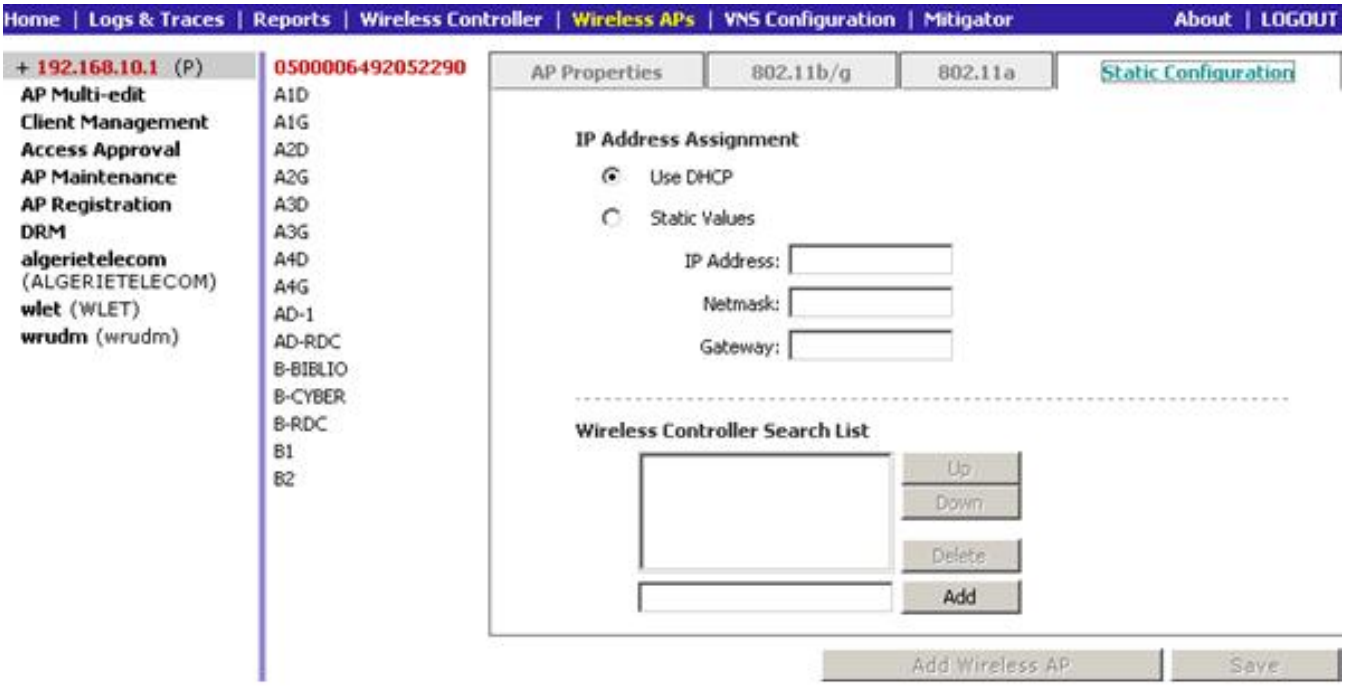


Fig. II. 18 : Les commandes de « **Statice Configuration** ».

c) AP Multi-Edit:

Cette commande permet de configurer plusieurs APs de marques différentes que Siemens au même temps. Dans notre cas cette commande n'est pas prise en considération car on utilise le même cas d'APS (siemens).

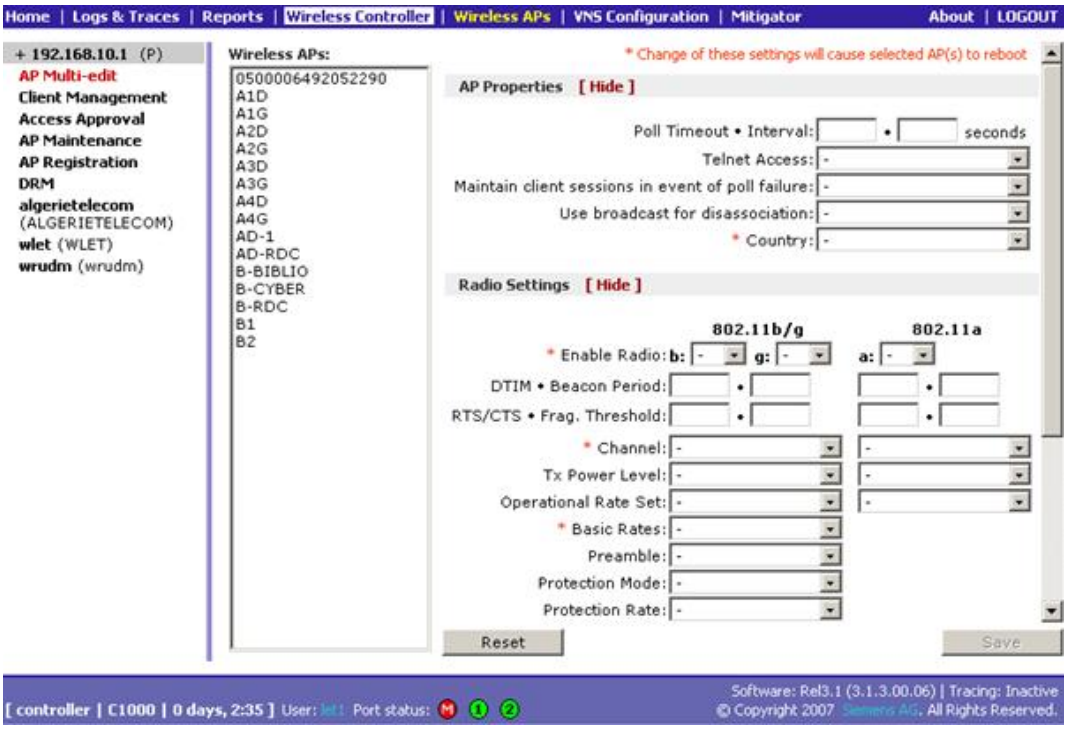


Fig. II.19 : Les commandes de « **AP Multi-edit ».**

e) Client Management :

Cette commande sert à sécuriser notre réseau dans le cas ou un utilisateur inconnu veut accéder au réseau. On l'ajoute à la liste noire ou le désactiver.

Disassociate: cliquez sur un point d'accès et choisir les clients à déconnecter.

Blacklist : cette commande ajoute un client à la liste noire.

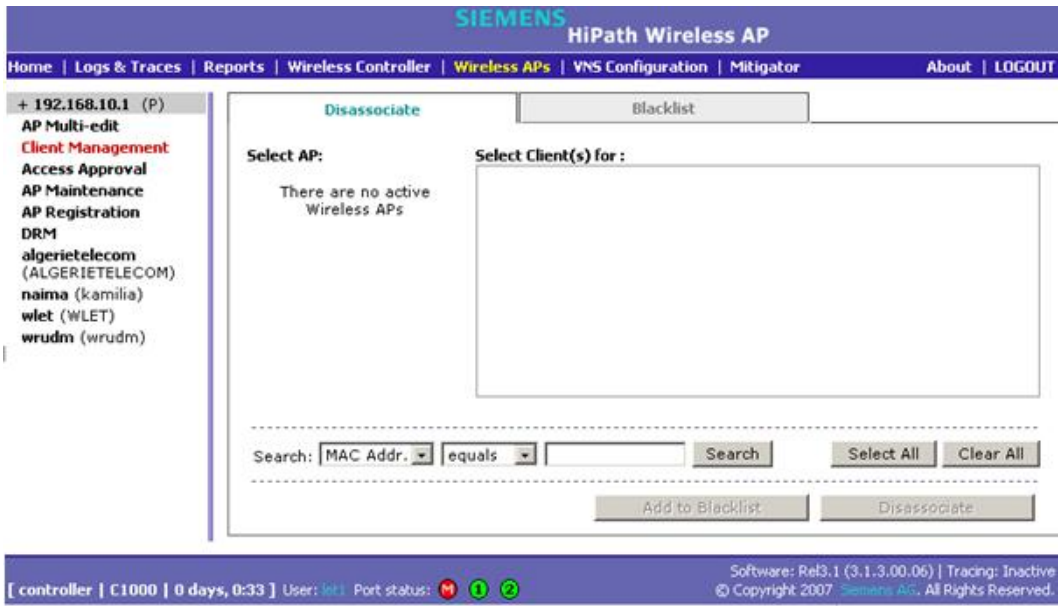


Fig. II.20 : les commandes de la « Disassociate & Blacklist ».

f) AP Registration:

Cette commande permet de configurer les paramètres d'enregistrement du point d'accès sur le contrôleur. **Fig. II.21.**

Fig. II.21 : Les commandes de « Wireless AP Registration ».

g) DRM (Dynamic Radio Management) :

Cette application est intégrée dans le contrôleur. Son objectif est basé sur le réglage automatique de la zone radio pour chaque point d'accès et la puissance de l'émission des APs. Il assure aussi la mobilité des clients entre les APs et la distribution automatique des canaux pour chaque point d'accès. **Fig. II.22.**

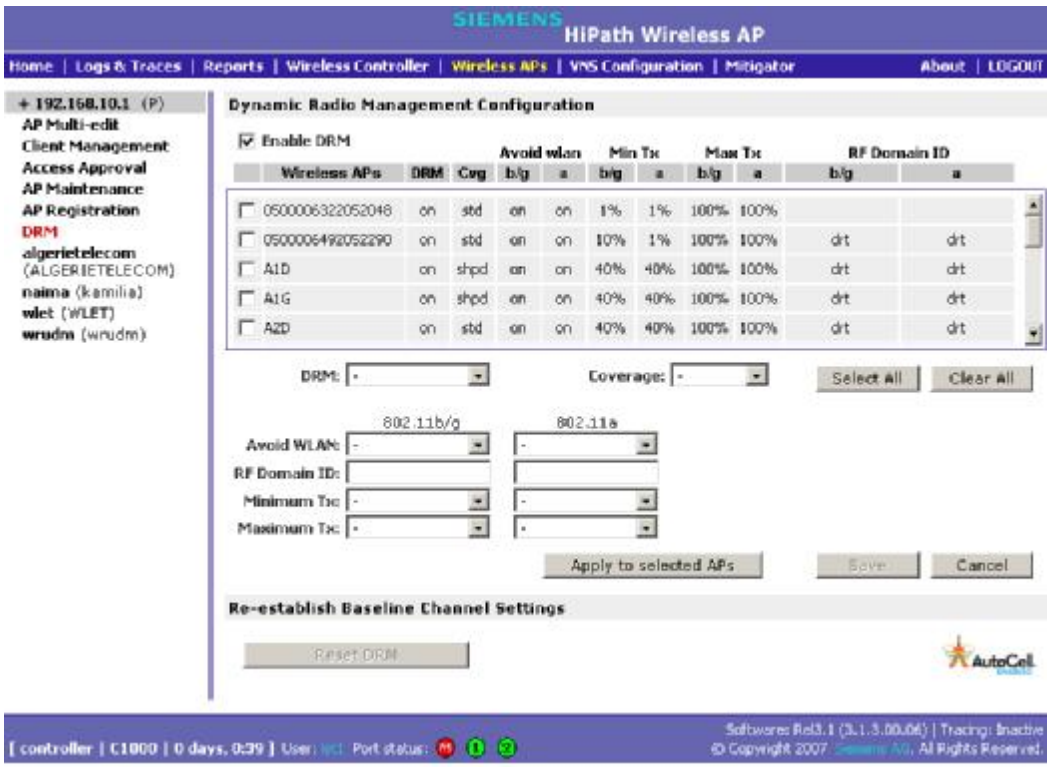


Fig. II.22. : Les commandes de **« DRM ».**

- **DRM :** dans la liste de cette commande on choisi la commande **DST.** Elle permet d'ajuster la gamme sur le client qui est plus éloigné. Ceci est indiqué par la puissance d'un signal. Par contre la commande **SHPD** ajuste la gamme basée sur la radio voisine APs.

- **WLAN :** sur la liste de cette commande on choisi le bouton **ON** pour activer l'utilisation du réseau.

- **RF Domain ID :** la commande d'identification de domaine RF permet de contrôler les canaux et les niveaux de la puissance d'un signale. Ceci, pour partager les canaux des AP, d'une manier intelligente pour évité les interférences.

- **Sur Minimum TX:** choisir le niveau de puissance minimum et celle-ci ne peut pas être réduite par le DRM.

- **Sur Maximum TX**: choisir le niveau de puissance maximum et celle-ci ne peut pas être augmentée par le DRM.

III.4. Configuration de VNC :

1) **Virtual Network configuration :** cette commande définie la configuration du réseau sans fil virtuel (VNS).

Le VNS ***« Virtual Network Services » :*** Définit un sous réseau IP virtuel, ou bien une passerelle (Gateway) pour router le flux de données d'un groupe d'utilisateur.

Remarque :

Chaque AP peut supporter 16 VNSs dont 8 pour le bouton standard 802.11a et 8 VNS pour le bouton standard 802.11b/g. Chaque contrôleur support 50 VNS. Chaque VNS est définie par sa topologie, L'authentification, la Sécurité … La configuration d'un VNS nécessite deux étapes:

- Étape 1 : donner un nom au sous réseau VNS (le SSID) et définir la topologie de VNS.
- Étape 2 : configurer les paramètres du VNS.

a) Topology :

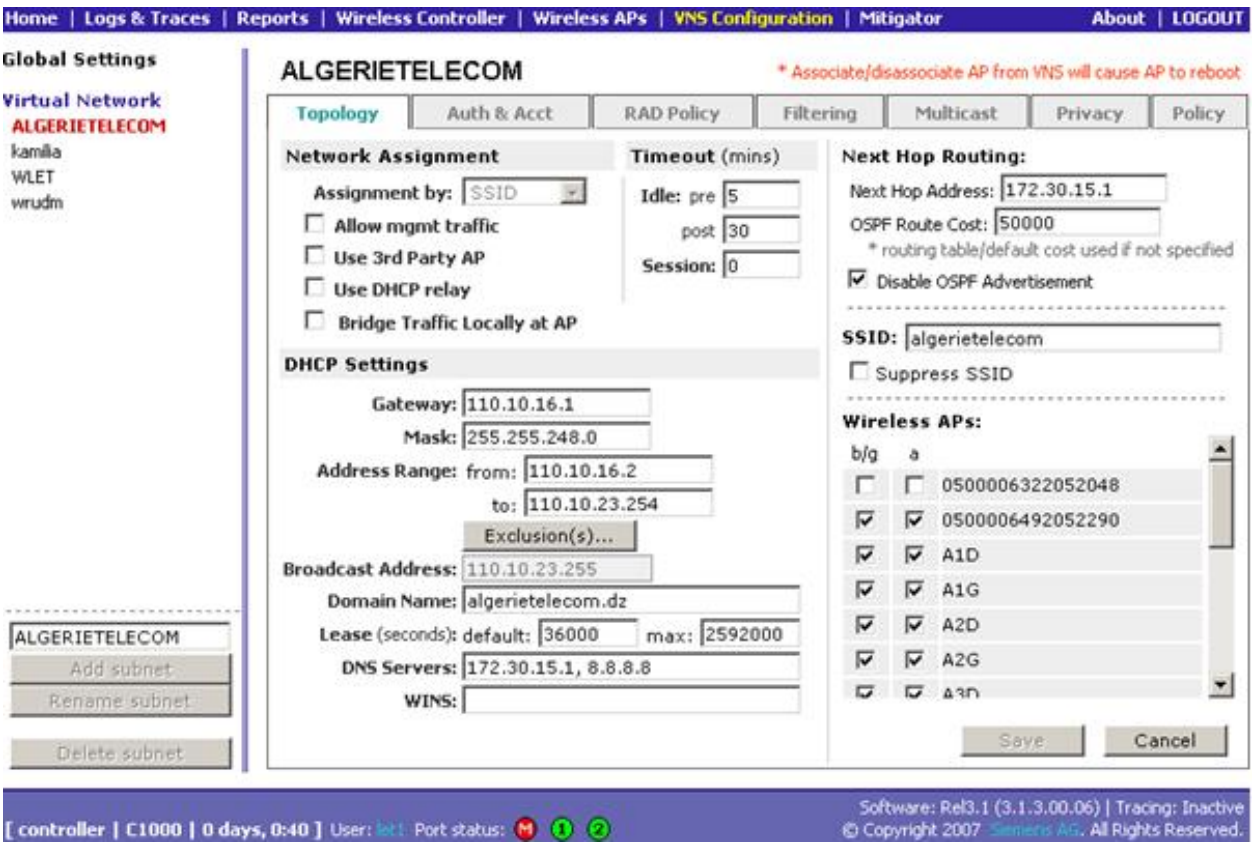


Fig. II.23 : Les commandes de la « Topology VNS ».

d) Auth et accet :

RADIUS est un Protocole d'authentification de sécurité basé sur les clients et les serveurs. Il est largement utilisé par les fournisseurs de services Internet sur des serveurs distants, c'est le protocole le plus connu pour l'authentification et l'autorisation des utilisateurs de réseaux d'accès à distance. Dans notre cas on n'a pas configuré cette partie car le serveur radius ce trouve au niveau du site centrale à Alger.

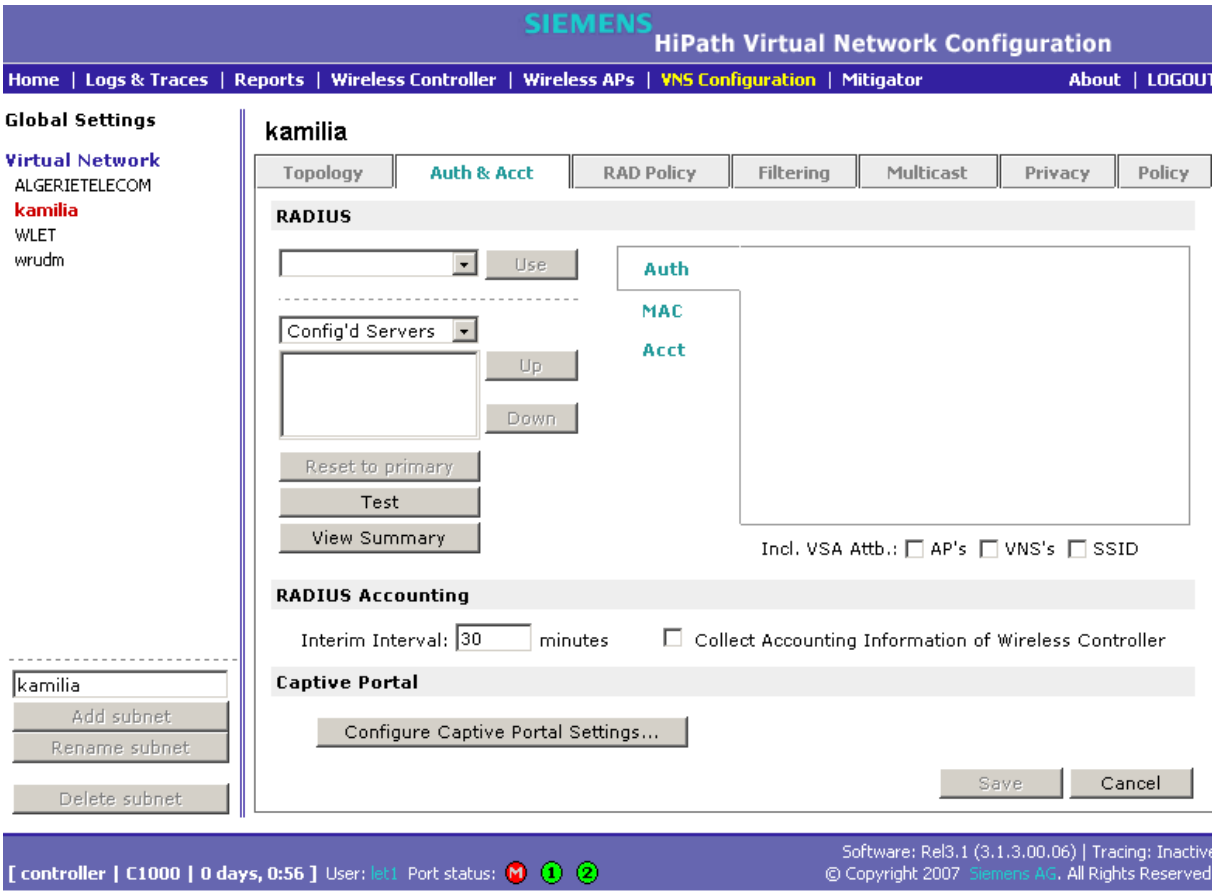


Fig. II. 24 : Les commandes de « l'Authentification ».

b) Filtering:

C'est un ensemble de règles qui utilise le contrôleur pour filtrer les paquets qui sont arrivés d'un réseau extérieur. Cette commande autorise l'accès de sortie des données, pour cela on coche la case « Allow ».

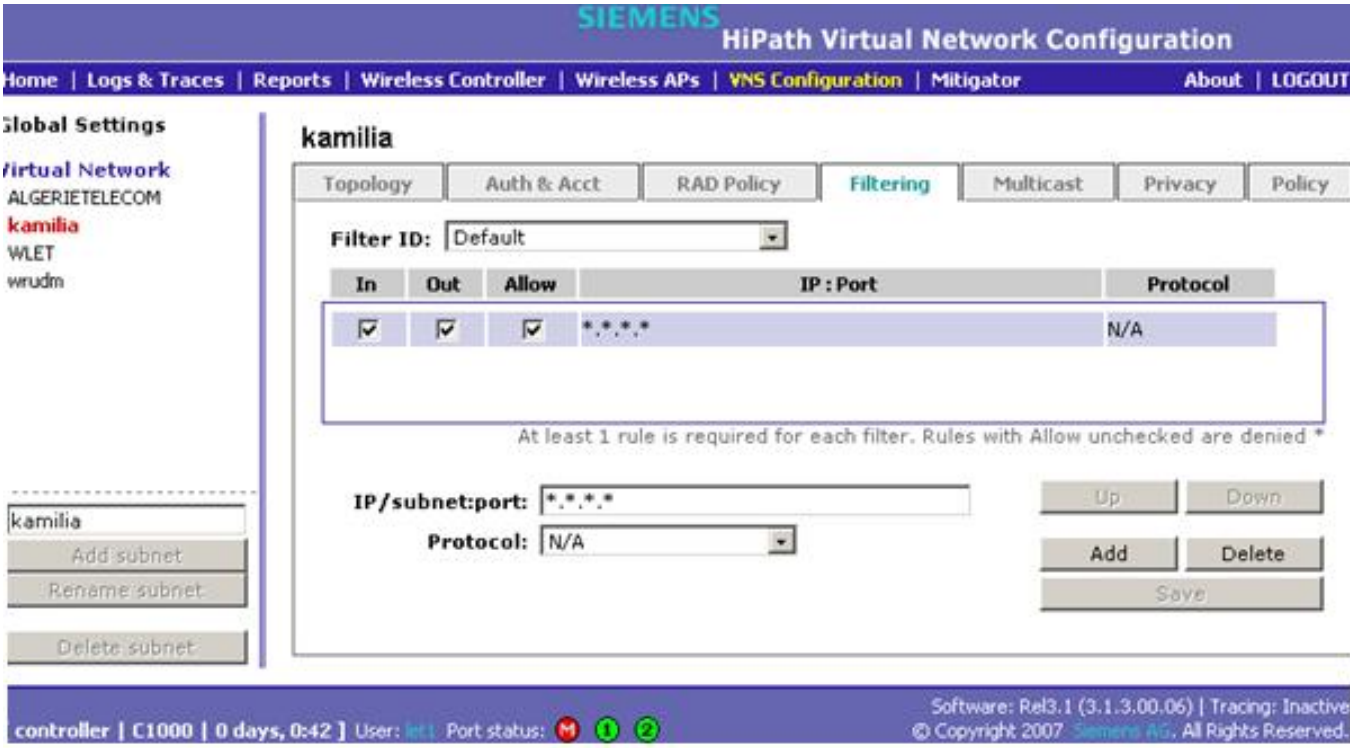


Fig. II.25 : les commandes de « Filtring ».

d) Privacy:

Cette commande permet de configurer les paramètres de cryptage. Cette configuration se fait comme suit :

- **None :** aucune protection ne peut être utilisée**.**
- **Static Keys WEP** (**W**ired **E**quivalent **P**rivacy**) :** c'est un protocole de sécurité des réseaux sans fil qui sont les réseaux 802.11(WiFi). Il fournit un niveau de sécurité minimal.
- **WPA-PSK :** c'est une solution de sécurité qui ajoute une authentification améliorée par rapport au protocole WEP.

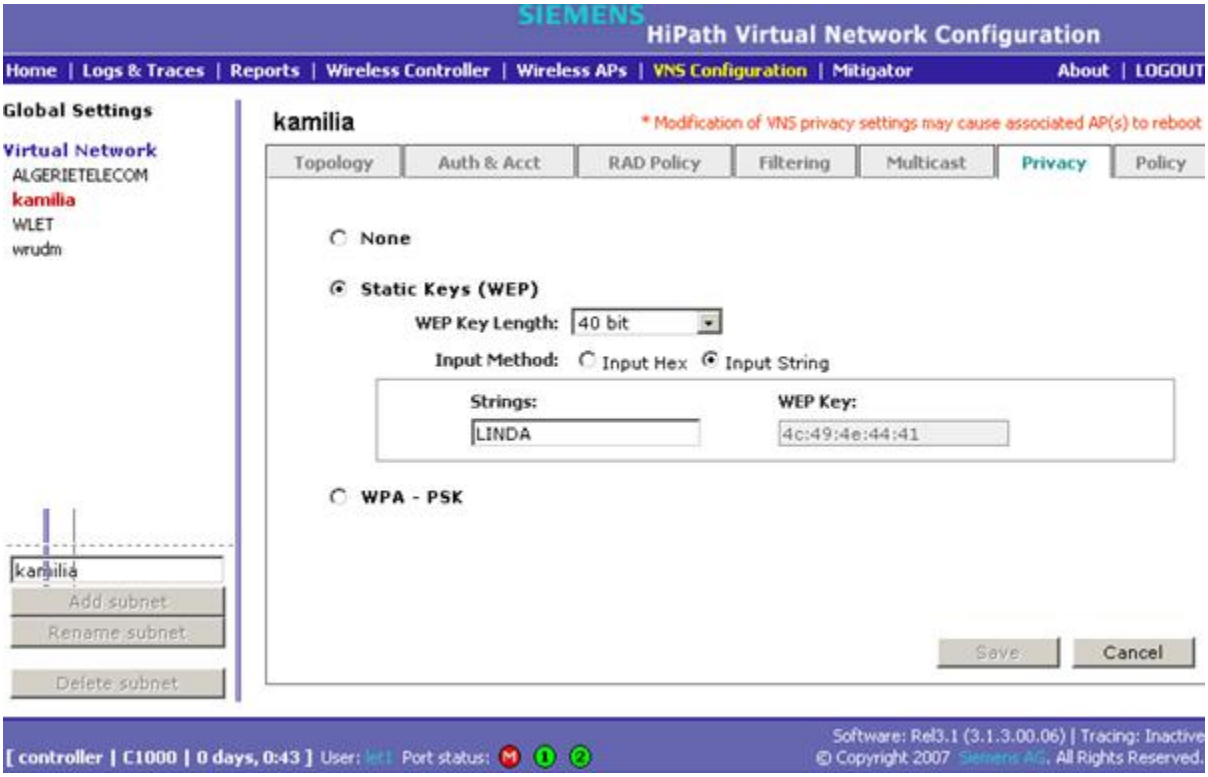


Fig. II.26 : Etape de paramètre de sécurité.

IV. La supervision.

On peut superviser les APs et les clients dans le contrôleur à partir des commandes suivantes :

Reports & Displays :

Une fenêtre affiche les étapes de la supervision sur le contrôleur, comme le montre la **figure II.27**.

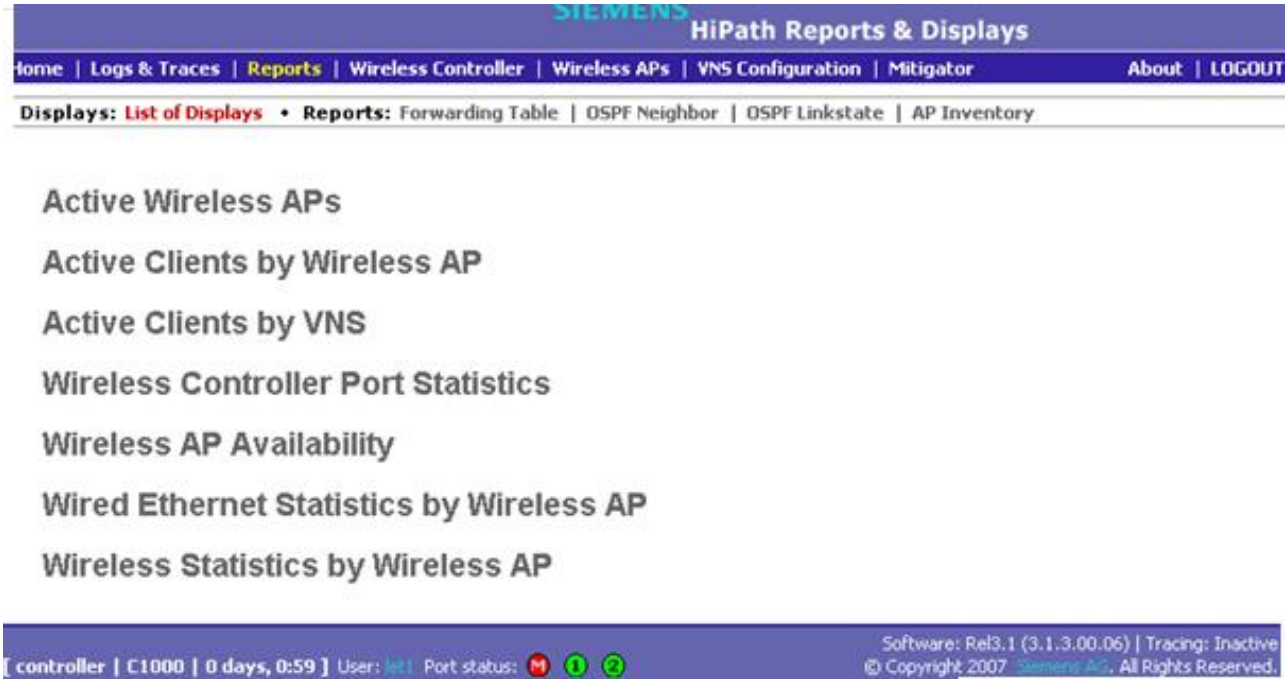


Fig.II.27 : La Fenêtre de « rapports et Display ».

a) Sur Active Wireless APs :

Cette fenêtre permet d'afficher un journal détaillé des informations sur les APs. Elles sont Activées sur le réseau sans fil. Comme exemples de ces information citons : l'adresse, le canal, le nombre de client connectés et le numéro de série de chaque AP ainsi que la duré de connexion de l'utilisateur sur le réseau. **Fig. II.28**

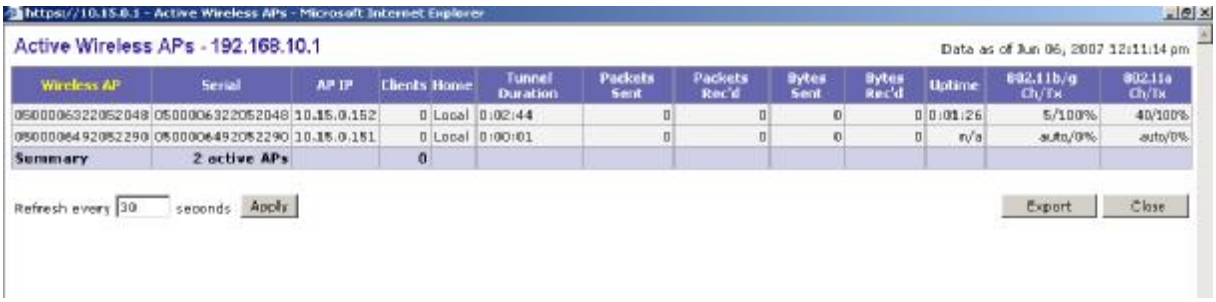


Fig. II.28 : La Fenêtre de « Active Wireless APs ».

a) Active Client by Wireless APs:

Cette fenêtre représente un journal d'informations détaillé sur les clients qui sont associé à chaque AP activé. Par exemples citons: l'adresse IP, le canal, la duré de connexion sur le réseau, le SSID ,l'authentification (WPA) de chaque client, le nombre de bite transmit

et reçu ainsi que l'état de client si il est activé au non, En cliquant sur la fenêtre AP, qu'est identifier par son numéro de série, une fenêtre montre tous les clients qui sont actif et associé sur l'AP, cette fenêtre permet à l'administrateur de contrôler l'état actuelle des clients connectés sur le réseau. Nous pouvons aussi désactiver des clients en les ajouter à la liste noire (Black List) (**figure II. 29**).

Fig. II.29 : La Fenêtre de « Active Client by Wireless APs».

- **Add to Blacklist:** ajouter un client à la liste noire.

- **Dissociations**: désactiver un client, c'est-à-dire vous pouvez déconnecter un client qui est associé sur n'importe quel AP d'un réseau sans fil.

- **Export** : enregistrer le rapport sur un disque amovible.

b) Active Client by VNS (Virtuel Network Service) :

En cliquant sur le bouton **Active Client by VNS,** une fenêtre affiche un journal d'informations détaillé sur les clients qui sont connectés sur chaque VNS. Le type d'information est: l'adresse et le canal de client sur le VNS, la durée de connexion sur le réseau, l'authentification (WPA). **Fig. II.30**

Remarque *:*

A partir de cette fenêtre l'administrateur peut contrôler l'état actuel des clients sur son réseau. Il peut aussi dissocier ou ajouter des clients à la liste noire(Blacklist) comme la fenêtre précédente.

Fig. II.30 : La Fenêtre de « Active Client by VNS ».

c) Wireless Controller port statistics:

A partir de cette fenêtre, l'administrateur peut avoir des détails sur les statistiques de flux de données transmis et reçus sur les deux interfaces, Esa1, Esa0.

Esa1 : représente le flux des données et le nombre des trames qui sont entrées à partir de l'internet.
Esa0 : définit le flux des données et le nombre des trames qui sont sorties à partir du contrôleur vers les clients.

Fig. II.31: Wireless Controller port statistics

d) Wireless AP availability:

C'est l'interface graphique de l'état des points d'accès actifs (en vert) et non actifs (en rouge), qui sont connectés avec le contrôleur comme le montre la figure suivante:

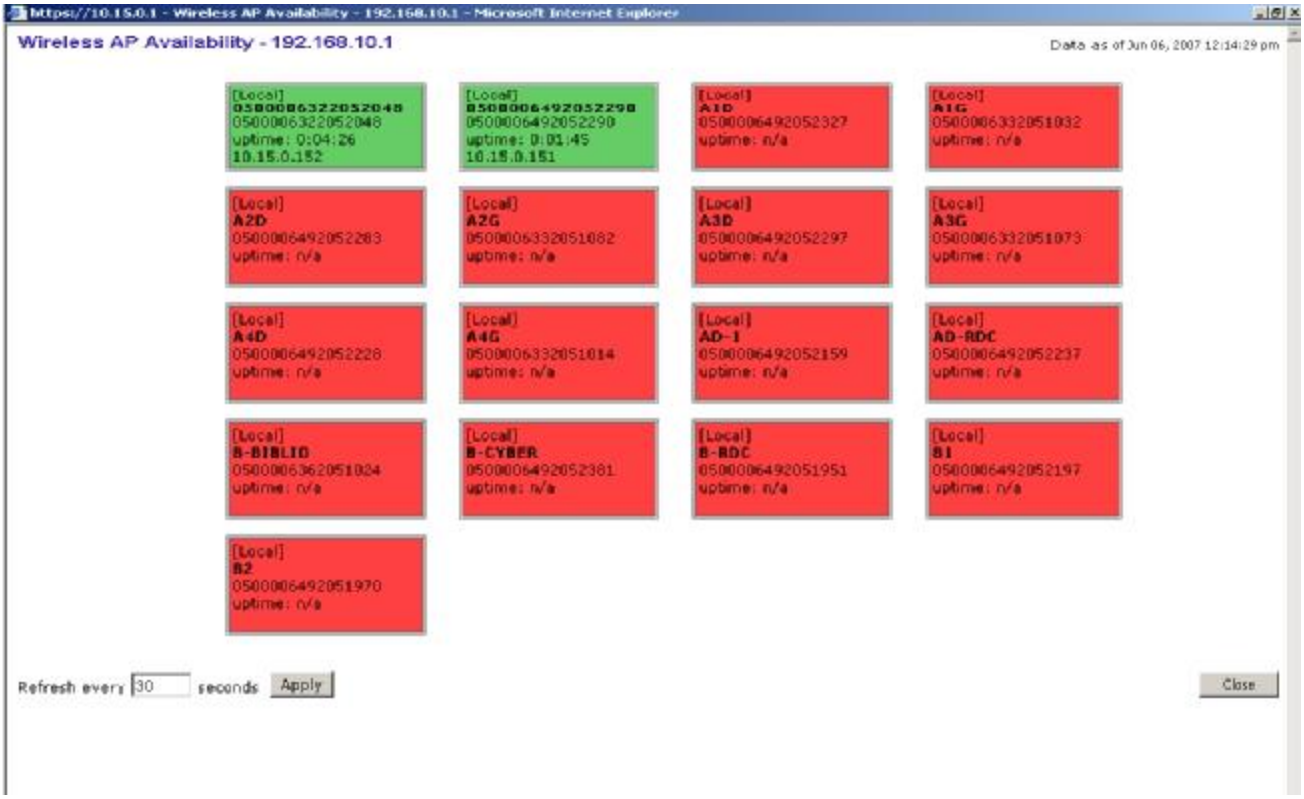


Fig. II.32 : La Fenêtre de « Wireless AP availability ».

Remarque :

Lorsqu'on branche un nouveau point d'accès (AP), le contrôleur va détecter et enregistrer une image de l'AP automatiquement, grâce au serveur DHCP qui donne des adresses IP à tous les points d'accès qui sont branchés sur le réseau. Si le serveur DHCP n'est pas installé dans ce cas, le contrôleur ne peut pas détecter les APs, car ils ne sont pas identifiés.

V. Conclusion :

La technologie du réseau informatique se développe chaque jour. Dans ce chapitre nous avons donné un aperçu sur la méthode d'installation et la configuration d'un réseau Wi-Fi plus évalué. Cette méthode est basée sur un système centralisé. Simplifier les taches administratives. La sécurité du réseau sans fil évite tous les conflits lors d'une infrastructure et d'une configuration réseau Wi-Fi.

Abréviations

AAA: Authentification, Authorization, Accounting

AP: Access Point

BLR: Boucle Locale Radio

BSS: Basic Service Set

BOOTP: Bootstrap Protocol

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

ESS: Extended Service Set

FTP: File Transfer Protocol

IEEE: Institute of Electrical and Electronic Engineers

GSM: Global System for Mobile Communication

GPRS: General Packet Radio Service

IP: Internet Protocol

LLC: Logical Link Control

MAC: Media Access Control

NAS: Network Access Server

NTP: Network Time Protocol.

OPSEC : société de programmation spécialisée en systèmes intelligents.

OSI: Open System Interconnection

PLCP : Physical Layer Convergence Protocol

PMD : Physical Medium Dependant

RADIUS: Remote Authentication Dial-In User Service

SSID: Service Set Identifier

TCP: transmission control protocol

UDP: User Datagram Protocol

UMTS: Universal Mobile Telecommunication System

WEP: Wired Encryption Protocol

Wi-Fi: Wireless Fidelity

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WPAN: wireless Personal Area Network

Conclusion générale

Le travail qu'on a élaboré consiste sur l'implémentation d'un réseau sans fil sécurisé au niveau de la résidence universitaire DIDOUCHE Mourad de Tizi-Ouzou (ILE).

Le stage pratique qu'on a effectué au sein de l'entreprise Algérie Télécom de Tizi-Ouzou nous a favorablement aidées en concrétisant la théorie qu'on a acquise durant notre cursus. Cette étude nous a permis de découvrir des nouveaux équipements, qui vont assurer la sécurité et la bonne gestion des adresses IP.

Ce travail est basé particulièrement sur la configuration du contrôleur c1000, qui gère de façon centralisée les différents points d'accès quelque soient les sous-réseaux IP de réseau LAN. Outre les fonctions de redondance, comme les alimentations redondantes et la présence de plusieurs ports de données, les contrôleurs peuvent être déployés par paires, de sorte que les fonctions du contrôleur primaire puissent être reprises par un contrôleur secondaire en cas de défaillance pour cela ont été dans l'obligation d'étudier profondément les différents protocoles de sécurisation tel que Radius, AAA, DNS… et le protocole de gestion des adresse IP DHCP.

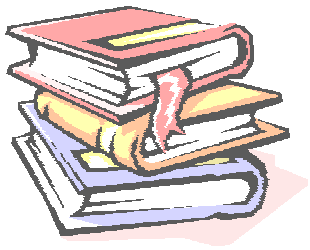
Comme nous avons pu le voir, il existe plusieurs niveaux de sécurité. Le WEP étant la sécurité la plus répandue, c'est aussi la plus facile à contourner. Pour un réseau fiable, il vaut mieux donc opter pour une sécurité WPA, qui nécessite un réseau en mode infrastructure. Par soucis de confidentialité, il est préférable d'avoir un réseau sécurisé. En effet, le pirate pourrait obtenir des informations telles que les identifiants de connexion internet, ou bien d'autres informations importantes, mais rien n'empêche la sécurisation d'un réseau sans fil est possible par de nombreux moyens matériels et/ou logiciels. Son choix dépend de l'utilisation que vous voulez faire de votre réseau et des moyens dont vous disposez.

Dans notre cas la sécurité est réalisée à différents niveaux : configuration des équipements et choix des protocoles.

Nous tenons également à dire que l'implémentation que nous avons réalisée avec l'équipe d'Algérie Telecom nous a permis de découvrir la bonne méthode pour une installation réseau sans fil, l'étude du site ainsi que le bon emplacement des équipements.

Nous espérons que nous avons été au bout de la tâche qui nous a été confiée et que nous avons réussi à présenter un document capable d'offrir aux gens du domaine les informations nécessaires sur l'implémentation d'un réseau sans fil et les configurations des équipements utilisés et que ce travail puisse servir de support pour les prochaines promotions.

Bibliographie



[1] : http://www.ietf.org/html.charters/aaa-charter.html

[2] : http://www.efort.com

[3] : http://fr.wikipedia.org/wiki/Radius_(informatique)

[4] : http://en.wikipedia.org/wiki/Diameter_(protocol)

[5] : http://www.freeradius.org

[6] : http://www.wiki-pc.fr/Le_protocole_DHCP

[7] : http://www.art-telecom.fr

[8] : http://www.wi-fi.org

[9] :http://www.livre-wi-fi .com

[10] : DI GALLO Frédéric « WI-fi l'essentiel qu'il faut savoir » 2003

[11] : AURELIEN Geron « WI-fi professionnel la norme 802.11, le déploiement, la sécurité »

[12] : GUY Pujolle « Les réseaux »

[1 3] : Emmanuel LEBEL Geron «Réseaux locaux haut débit » 2001

[11] :CYBER NETWORK « Livre blanc, sécurité des réseaux » 2004