République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et Recherche Scientifique
Université Saad Dahlab de Blida 1

Faculté des sciences
Département d'Informatique

En vue d'obtenir le diplôme de master

Domaine : Mathématique et informatique

Filière : Informatique

Spécialité : Informatique

Option : Réseaux et systèmes informatiques

Étude comparative des méthodes d'authentification avec le standard 802.1x dans les réseaux WLAN

Présenté par :

-M Abdelhaq Kassaa

-M Saadeddine Baziz

Encadreur :

-M Abderrazak Bachir Bouidjra

Promoteur :

-M Nacim Fateh Chikhi

Soutenu le : 14/09/2020

Devant le jury :

-M. Mohamed Ould Khaoua	(Université de BLIDA 1)	Président
-Mme. Bachira Boutoumi	(Université de BLIDA 1)	Examinatrice
-M. Abderrazak Bachir Bouidjra	(Université de Sidi-Bel-Abbès)	Encadreur
-M. Nacim Fateh Chikhi	(Université de BLIDA 1)	Promoteur

Année universitaire : 2019 / 2020

Remerciements

Au nom du dieu le clément et le miséricordieux, louange à ALLAH le tout puissant sans lui rien de tout cela n'aurait pu être.

Nos vifs remerciements accompagnés de toute nos gratitudes vont ensuite à notre encadreur Monsieur CHIKHI NACIM d'avoir accepté de nous encadrer, pour ses conseils et ses corrections qui nous ont permis d'améliorer le document final.

Nos remerciements à Monsieur BOUIDJRA ABDEREZAK pour ses remarques et conseils, pour d'avoir accepté de nous encadrer, qui nous a aidé à organiser ce stage au sein de l'entreprise ICT-TOWERS et de nous avoir fait travailler sur un sujet très intéressant qui nous a beaucoup apporté.

Nous remercions également les membres de Jury qui ont accepté d'évaluer ce travail.

Enfin, Nous remercions nos familles et nos amis pour leur aide et leur soutien précieux durant cette année.

Dédicaces

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

Nous dédions ce modeste travail :

A nos parents Que dieu leurs procure bonne santé et longue vie ;
A toute la famille,
A nos amies et collègues
Et à tous ceux qui nous ont aidé.

Résumé

La transmission radio rend les réseaux sans fil commodes d'usage, faciles à déployer, et économiques, mais soulèvent par contre des problèmes de sécurité, dus à la nature ouverte des supports de transmission utilisés. La norme IEEE 802.11 est l'un des mécanismes les plus largement adoptés pour les WLAN ; elle fournit des directives complètes pour leur fluidité opérationnelle. Le 802.11 souffrait d'une confidentialité limitée des données et d'une procédure lourde d'échange des paramètres de sécurité. En réponse aux contraintes de sécurité du 802.11, IEEE a introduit le 802.1x pour l'authentification et la gestion des clés.

Le 802.1x est un protocole de contrôle d'accès réseau basé sur les ports qui utilise le protocole d'authentification extensible (EAP) au niveau de la couche de transport qui prend en charge une variété des méthodes d'authentification telles que MD5, TLS, TTLS, PEAP, LEAP, FAST etc. Le 802.1x définit uniquement le mécanisme d'authentification et ne recommande aucune méthode d'authentification qui rend l'authentification plus flexible mais conduit en revanche à la question de savoir comment sélectionner la méthode d'authentification appropriée.

Notre projet vise à l'étude et la mise en œuvre les différentes méthodes d'authentification et aussi à mesurer les performances réseaux tels que le débit et le délai (RTT Round Time Trip). Afin de fournir une visibilité cohérente pour le choix de la méthode d'authentification en considérant le niveau de sécurité approprié par rapport aux performances du réseau à aboutir.

Mots-clés : - Authentification, EAP, réseaux WLAN, 802.1x

Abstract

Radio transmission makes wireless networks convenient to practical use, easy to be spread, and economic. However, it raises security problems because of the open nature of the used transmission supports. The IEEE 802.11 standard is one of the most widely adopted mechanisms for WLANs, it provides comprehensive guidelines for their operational smoothness. 802.11 suffered from limited data confidentiality and cumbersome procedure for exchange of security parameters. In response to security limitations in 802.11, IEEE introduced 802.1x for authentication and key management.

The 802.1x is a port based network access control protocol that uses Extensible Authentication Protocol (EAP) at the transport layer which supports a lot of authentication methods such as MD5, TLS, TTLS, PEAP, LEAP, FAST etc. The 802.1x only defines authentication mechanism and does not recommend any appropriate authentication method that makes the authentication more flexible but on the other hand leads to the question of how to select the appropriate authentication method.

Our project aims at studying and implementing different authentication methods and also at measuring network performance such as throughput and RTT (Round Time Trip). In order to provide consistent visibility for the choice of authentication method considering the appropriate level of security in relation to the performance of the network to be achieved.

Key-Words: - Authentication, EAP, Wireless LANs, 802.1x

ملخص

ان نظام الارسال عبر موجات الراديو يجعل الشبكات اللاسلكية سهلة الاستعمال، سهلة الانتشارواقتصادية. ومع ذلك ، فإنه يثير مشاكل أمنية ناتجة عن طبيعة النواقل المستعملة. يعد معيار IEEE802.11 أحد أكثر الآليات المعتمدة على نطاق واسع للشبكات اللاسلكية المحلية WLAN ، فهو يوفر إرشادات شاملة لسلاسة تشغيلها. لكنه في المقابل عانى من عدة ثغرات أمنية كخصوصية البيانات والإجراءات المرهقة لحماية المعلومات . استجابة للقيود الأمنية في 802.11 ، قدمت IEEE بروتوكول 802 .1x للتعرف و ادارة المفاتيح.

802.1X هو بروتوكول تحكم في الوصول إلى الشبكة قائم على المنفذ الذي يستخدم بروتوكول للتعرف EAP في طبقة النقل الذي يدعم مختلف طرق التعرف مثل MD5، TLS، TTLS، PEAP، LEAP و FAST وما إلى ذلك. يعرّف 802.1x آلية التعرف فقط ولا يوصي بأي طريقة تعرف التي تجعل عملية التعرف اكثر مرونة لكنه في المقابل يقود الى التساؤل عن كيفية اختيار طرقة التعرف المناسبة .

يهدف مشروعنا إلى دراسة مختلف طرق التعرف وتطبيقها مع القيام بقياس مستويات أداء الشبكة مثل سرعة التدفق والوقت المستغرق RTT من أجل توفير رؤية متسقة لاختيار طريقة التعرف ، مع مراعاة المستوى المناسب من الأمان فيما يتعلق بأداء الشبكة المطلوب تحقيقه.

الكلمات المفتاحية: - التعرف، EAP، الشبكات اللاسلكية المحلية، 802.1x

Table des matières

Table des figures

Liste des tableaux

Liste des Abréviations

A

AAA : Autorisation, Authentification, Accounting
AES : Advanced Encryption Standard.
AP : Access Point

B

BLR : Boucle Locale Radio.
BSS : Basic Service Set.
BSSID : Basic Service Set Identifier.

C

CCK : Complementary Code Keying.
CFP : Contention Free Period.
CSMA/CA : Carrier Sense Multiple Access/Collision Avoidance.
CTS : Clear To Send.
CW : Contention Window.
CCX : Cisco Compatible eXtension.

D

DCF : Distributed Coordination Function.
DoS : Deny of Service.
DS : Distribution System.
DSSS : Direct Sequence Spread Spectrum.

E

EAP : Extensible Authentication Protocol.
EAPoL : EAP over LAN.
ESS : Extended Service Set.
ESSID : Extended Service Set Identifier.
ETSI : European Telecommunications Standards Institute.

F

FAST : Flexible Authentication via Secure Tunneling.
FHSS : Frequency Hopping Spread Spectrum.
FTP : File Transfert Protocol

G

GPRS : General Packet Radio Service.
GSM : Global System for Mobile Communication.

H

HR-DSSS : High Rate -Direct Sequence Spread Spectrum.

I

IBSS : Independent Basic Service Set.
IEEE : Institute of Electrical and Electronics Engineers.
IETF : Internet Engineering Task Force.
IGCInfrastructure à Gestion de Clé **IGC :** Infrastructure à Gestion de Clé.
ISO : International Organization for Standardization.
ITU – International Telecommunication Union.

L

LAN : Local Area Network.
LLC : Logical Link Control.
LEAP : Lightweight Extensible Authentication Protocol)

M

MAC : Media Access Control.
MAN : Metropolitan Area Network.
MD5 : Message Digest 5.
MIC : Message Integrity Code.
MiM : Man in the Middle.

N

NAS : Network access Server

O

OFDM : Orthogonal Frequency Division Multiplexing.
OSI : Open Systems Interconnection.

P

PAE : Port Access Entity.
PAN : Personal Area Network.
PCF : Point Coordination Function.
PEAP : Protected EAP.
PKI : Public Key Infrastructure.
PSK : Pre Shared Key.

R

RADIUS : Remote Authentication Dial In User Service.
RC4 : Rivest Cipher 4.
RSN : Robust Security Network.
RTS/CTS : Request to Send/Clear to Send.

S

SSID : Service Set Identifier.

T

TKIP : Temporal Key Integrity Protocol.
TLS : Transport Layer Security.
TTLS : Tunneled TLS.

W

WAN : Wide Area Network.
WEP : Wired Equivalent Privacy.
Wi-Fi : Wireless-Fidelity.
Wimax : Technologie de WMAN définie par le Wimax Forum à partir des normes IEEE 802.16 et ETSI HiperMAN.
WLAN : Wireless LAN.
WMAN : Wireless MAN.
WPA : Wireless Protected Access.
WPAN : Wireless PAN.
WWAN : Wireless WAN.

Introduction générale

Depuis quelques années, les réseaux sans fil ne cessent de se développer. Ils rencontrent aujourd'hui un succès important car ils permettent de déployer des moyens de transmission sans contrainte d'immobilité liée aux câblages et aux prises réseaux. La promotion actuelle de ce type de solution est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, coût inférieur à un système filaire, mobilité, accès partagé à des services de haut débit.

Contrairement à un réseau filaire, le sans-fil ne permet pas d'avoir un périmètre géographique circonscrit puisque son signal est diffusé bien au-delà des limitations physiques des lieux de travail (bureaux et bâtiments). Par conséquent, La nature ouverte du support de transmission des réseaux sans fil les rend bien plus vulnérables que les réseaux conventionnels. En effet, ce mode de transmission a pour conséquence la possibilité d'interception des données envoyées et/ou reçues sur le support et par la suite de pouvoir modifier et rejouer les données. L'intrus peut également injecter, saturer ou endommager les équipements du réseau.

Tout comme le réseau filaire, l'infrastructure des réseaux sans fil doit être adéquatement protégée afin d'empêcher des accès non autorisés. La gestion des accès au réseau est devenue très importante, d'une part pour la protection contre les tentatives d'intrusions, et d'autre part pour assurer la **mobilité**.

Le standard d'authentification IEEE 802.1X a été conçu à l'origine pour les réseaux filaires [3], mais en raison des grands défauts et vulnérabilités dans les réseaux WLAN (norme IEEE 802.11), IEEE 802.1X a été révisé pour l'adapter aux réseaux sans fil WLAN. IEEE 802.1X est très simple dans son concept. Son but est de mettre en oeuvre le contrôle d'accès au moment où un utilisateur se connecte au réseau. Le standard 802.1X s'appuie sur l'encapsulation EAP (Extensible Authentification Protocol) pour mettre en relation le serveur d'authentification et le système à authentifier par l'intermédiaire d'un point d'accès dans le cas des réseaux 802.11. Le protocole EAP réalise une enveloppe générique pour de multiples méthodes d'au-

thentification. Plusieurs méthodes d'authentification pour les réseaux WLAN ont été proposées, chacune ayant des avantages et des inconvénients.

Problématique :

Pour atteindre ses objectifs, IEEE 802.1X utilise des protocoles bien connus tels qu'EAP et RADIUS. En raison de la diversité des applications WLAN, une méthode d'authentification unique ne pouvait pas convenir dans tous les cas. Il existe par conséquent de nombreuses méthodes telles que LEAP, MD5, PEAP, TLS, TTLS, etc. Compte tenu du nombre de ces différentes méthodes d'authentification qui pourraient être prises en charge par EAP, se pose alors la question quelle est la meilleure à utiliser ? Ben évidemment il n'y a pas de réponse simple, chaque méthode peut être un choix idéal pour un environnement réseau spécifique. Il existe plusieurs facteurs sur lesquels la décision de la sélection de la méthode d'authentification dépendra. En fonction de ces facteurs, la bonne étude de ces facteurs nous guidera vers le choix de la méthode d'authentification EAP la plus appropriée pour les réseaux WLAN.

Objectif :

L'objectif de ce travail est l'étude comparative avec la mise en oeuvre des différentes méthodes d'authentifications en considérant plusieurs facteurs possibles tel que :

— Le niveau de sécurité à garantir.

— La performance réseau (débit, le délai (RTTround time trip)).

Et ce afin nous a fournir une visibilité cohérente pour le choix de la méthode d'authentification en considérant le niveau de sécurité approprié par rapport aux performances du réseau à aboutir.

Organisation du mémoire :

Dans le présent mémoire, nous mettrons en évidence les étapes que nous avons suivies pour réaliser notre travail. Le mémoire s'articule en quatre chapitres organisés comme suit :

Chapitre I : où nous présenterons quelques concepts de base sur les réseaux informatiques ainsi que des notions de base sur la sécurité informatique.

Chapitre II : ce chapitre présente des généralités sur les réseaux sans fils, décrit en détail les réseaux Wi-Fi (architecture, techniques d'accès au support, mobilité/-

Roaming...). Il traite aussi la sécurité des réseaux Wi-Fi et les différentes attaques susceptibles d'atteindre un réseau Wi-Fi.

Chapitre III : nous étudions dans ce chapitre les différentes solutions d'authentification dans les réseaux WLAN ainsi que les principes des protocoles Radius et 802.1X. Il se termine par la description des méthodes d'authentification avec leurs avantages et inconvénients.

Chapitre IV : ce dernier chapitre est consacré à la partie " Implémentation et test " dans lequel nous avons introduit l'organisme du stage, les outils ainsi que les équipements ayant servi pour réaliser notre travail. Il se termine par une démonstration des résultats obtenus.

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

Chapitre I

Notions de base sur les réseaux informatiques

I.1 Introduction

Les réseaux informatiques ont aujourd'hui autant d'importance que les ordinateurs eux-mêmes, au point que la plupart de nos activités ne pourraient plus être envisagées sans la mise en place de ces réseaux. Ils permettent ainsi d'élargir les horizons des individus et de créer les conditions permettant de réaliser en l'espace d'une décennie des progrès qui, par le passé, posaient des difficultés. Dans ce chapitre, nous allons expliquer plusieurs termes et définitions relatifs à notre travail que nous avons jugés nécessaire de connaître pour une bonne compréhension du sujet. Dans la deuxième partie nous allons présenter les notions de base en sécurité informatique, les objectifs et nous finirons par l'importance du contrôle d'accès.

I.2 Généralités sur les réseaux informatiques

I.2.1 Définition d'un réseau informatique

Le terme " réseau " se définit comme un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Il permet de faire circuler des éléments matériels ou immatériels entre chacune de ces entités. En informatique un réseau est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et permet aux utilisateurs de partager des ressources matérielles et logicielles (applications métier), des données, et d'échanger des informations au format numérique [25].

I.2.2 Rôles des réseaux

Il y a deux types principaux des objectifs des réseaux :

1. Les objectifs techniques
   - Partage des ressources logicielles(compilateur, système de gestion de base de données) et matérielles (imprimantes, traceurs, scanners,...), ce qui permet de diminuer les coûts.
   - La fiabilité (un réseau permet une duplication des données et limite ainsi les pertes de ces données).
2. Les objectifs des utilisateurs
   - La communication entre personnes (messagerie électronique, conférence électronique , téléphonie mobile, etc.)
   - L'accès distant à l'information (banques, bourses, bibliothèque en ligne, etc.).

I.2.3 Les supports réseaux

Les réseaux modernes utilisent principalement trois types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises. Ces supports sont les suivants [26] :

1. Fils métalliques dans des câbles (coaxial, paire torsadée).
2. Fibres de verre ou optiques de plastique (câbles en fibre optique).
3. Transmission sans fil (les ondes électromagnétiques).

I.2.4 Architecture des réseaux informatiques

Pour que les données arrivent correctement au destinataire, il faut une architecture logicielle chargée du contrôle des paquets dans le réseau. Les trois (03) grandes architectures suivantes se disputent le marché mondial des réseaux : [26] :

1. L'architecture OSI (Open Systems Interconnection).
2. L'architecture TCP/IP (Transmission Control Protocol / Internet Protocol) utilisée dans le réseau internet.
3. L'architecture introduite par l'UIT-T (Union International des Télécommunication-section Télécommunication) pour l'environnement ATM (Asynchronous Transfer Mode).

I.2.4.1 Architecture OSI (Open System Interconnexion) :

Le modèle OSI constitue le modèle de référence inter-réseau le plus connu. Le modèle OSI est un modèle à sept couches qui décrit le fonctionnement d'un réseau de communication de paquets. Chacune des couches de ce modèle représente une catégorie de problèmes que l'on rencontre dans un réseau. Découper les problèmes en couches présente des avantages tels que :

— Mettre un réseau en place revient à trouver une solution pour chacune des couches.

— Changer de solution pour une couche sans pour autant être obligé de tout repenser.

les couches de model OSI sont :

1. **Couche 1 (physique) :** Elle décrit les caractéristiques électriques, logiques et physiques de la connexion de la station au réseau : câbles, connecteurs, cartes réseau.
2. **Couche 2 (liaison) :** Son rôle est de définir des règles pour l'émission et la réception de données à travers la connexion physique de 2 systèmes : transmettre les données sans erreur, déterminer la méthode d'accès au support. Les données sont structurées en trames qui contiennent des informations de détection et correction d'erreurs.
3. **Couche 3 (réseau) :** permettre d'acheminer correctement les paquets d'information jusqu'à l'utilisateur final. Pour effectuer ce transport de bout en bout, la couche 3 utilise quatre processus de base : L'adressage , l'encapsulation , le routage , la dés-encapsulation L'unité d'information de la couche réseau est le paquet.
4. **Couche 4 (transport) :** Cette couche est responsable du bon acheminement des messages complets au destinataire. Elle segmente les messages de données en paquets et permet de reconstituer les paquets dans le bon ordre
5. **Couche 5 (session) :**elle permet l'ouverture et la fermeture d'une session de travail entre 2 systèmes distants. Elle assure la synchronisation du dialogue. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.
6. **Couche 6 (présentation) :** définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.

7. **Couche 7 (application) :** Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie....

I.2.4.2 Architecture TCP/IP (TCP/IP : Transmission Control Protocole / Internet Protocol) :

C'est une suite de protocoles utilisés sur Internet. Cette architecture est conçue dans le but de faire communiquer plusieurs machines différentes et incompatibles. Cette architecture est composée de 4 couches qui regroupent certaines couches du modèle OSI dans des couches plus générales :

— La couche accès au réseau (couche physique + couche liaison)

— La couche Internet (couche réseau)

— La couche Transport (couche transport)

— La couche application (couche session + couche présentation + couche application).

La figure I.1 résume les couches des modèles OSI et TCP/IP.

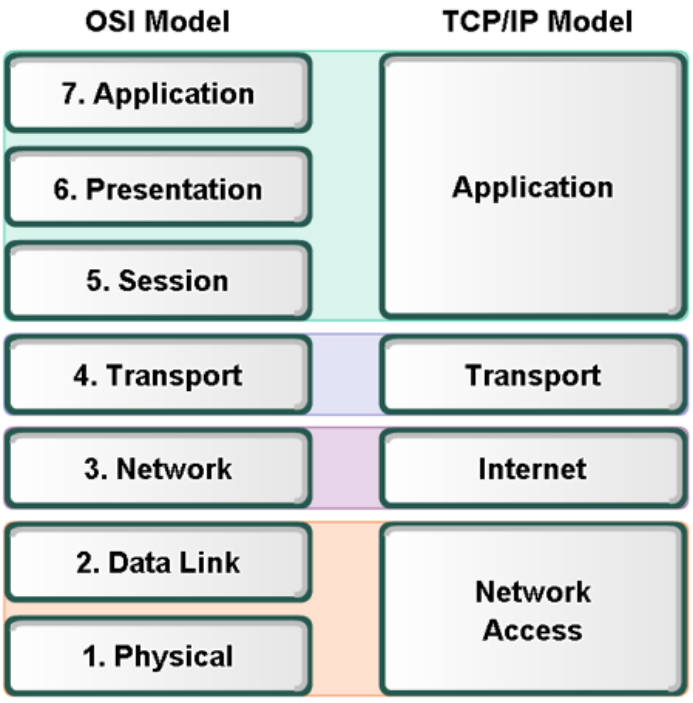


Figure I.1 – architecture OSI et TCP/IP

I.2.5 Topologies réseaux

Généralement, la topologie décrit l'arrangement spatial et la façon dont les données transitent dans les équipements. Les différents types de topologie sont la topologie physique et la topologie logique.[25]

I.2.5.1 La topologie physique :

Elle décrit le plan du réseau (la manière dont les équipements réseaux sont connectés entre eux). On distingue généralement les topologies suivantes :

— La topologie en bus.

— La topologie en étoile.

— La topologie en anneau.

— La topologie en arbre.

— La topologie maillée.

la topologie en bus : Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont relies à une même ligne de transmission par l'intermédiaire de câble, généralement de type coaxial. Le mot " bus " désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté .[25]

La topologie en étoile : Dans un réseau en étoile, chaque équipement est relié par une liaison point à point à un point central. Chaque point central est appelé "hub" ou concentrateur. Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible[25]. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub ou switch).

La topologie en anneau : Dans cette architecture, les ordinateurs sont reliés sur une seule boucle de câble.Les signaux se déplacent le long de la boucle dans une direction et passent par chacun des ordinateurs. A un instant donné, un seul noeud peut émettre sur le réseau. Il ne peut donc pas se produire de collision entre

deux messages contrairement au cas du réseau de type bus. Un jeton circule en permanence le long de la boucle. Lorsqu' aucun noeud n'émet de message, le jeton est dans un état libre (trame vide). Seul le noeud qui a envoyé le message est en attente d'un accusé de réception. Les autres noeuds n'étant pas en alerte, se contentent de retransmettre l'accusé de réception sans le lire. Lorsque le jeton arrive à la station émettrice celle-ci vérifie l'accusé de réception, retire son message et rend le jeton libre et ainsi de suite... Cette topologie est utilisée par les réseaux Token Ring et FDDI .[1]

Topologie maillée : Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres . L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est : s'il y a N terminaux, le nombres de liaisons nécessaires est de N.(N-1)/2. Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. L'Armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée.[1]

Topologie en arbre : : le réseau est divisé en niveaux. Le sommet, de haut niveau, est connectée à plusieurs noeuds de niveau inférieur dans la hiérarchie. Ces noeuds peuvent être eux-mêmes connectés à plusieurs noeuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence. Le point faible de ce type de topologie réside dans l'ordinateur "père" de la hiérarchie qui, s'il tombe en panne, paralyse la moitié du réseau. [1]

I.2.5.2 La topologie logique :

par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication . Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI. [25]

I.2.6 classification des réseaux

Le langage courant distingue les réseaux selon différents critères (la taille, leur vitesse de transfert de données ainsi que leur étendue...). La classification tradition-

1. https ://www.supinfo.com/articles/single/5709-classification-reseaux-informatiques. consulter le 19/04/2020

nelle, fondée sur la notion d'étendue géographique, correspond à un ensemble de contraintes que le concepteur devra prendre en compte lors de la réalisation de son réseau. Généralement, on adopte quatre catégories de réseaux informatiques : [26] :

I.2.6.1 PAN (Personal Area Network) :

Un PAN désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Les bus utilisés les plus courants sont l'USB, les technologies sans fil telles que Bluetooth ou l'infrarouge.

I.2.6.2 LAN (Local Area Network) :

Un réseau local d'étendue limitée à une circonscription géographique réduite (bâtiment...). Ces réseaux destinés au partage local de ressources informatiques (matérielles ou logicielles) offrent des débits élevés de 10 à 100 Mbit/s. Un réseau local relie des ordinateurs et des périphériques tels que des unités de stockage ou des imprimantes à l'aide de support de transmission par câble (coaxial ou paire torsadée) ou par radiofréquences sans fil sur une circonférence d'une centaine de mètres (voir Figure).

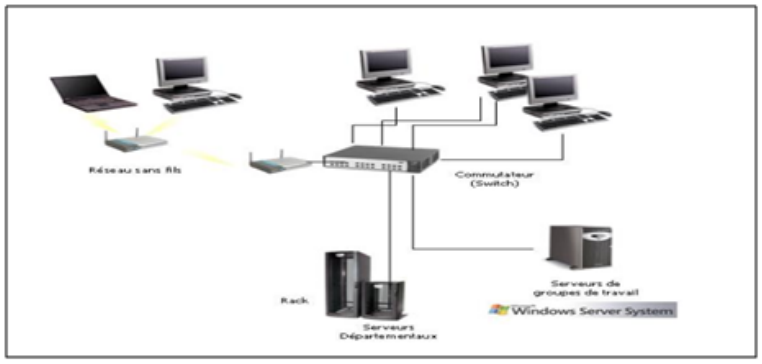


Figure I.2 – Un réseau LAN (Local Area Network)

I.2.6.3 MAN (Metropolitan Area Network) :

Avec une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux (connecter plusieurs LAN proches entre eux) ou assurer la desserte informatique de circonscriptions géographiques importantes (réseau de campus). Pour les relier entre elles, on fait appel à des routeurs et des câbles de fibre optique permettant des accès à très haut débit.

I.2.6.4 RAN (Regional Area Network) :

Ces réseaux ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir 50 km de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs.

I.2.6.5 WAN (Wide Area Network) :

Ces réseaux assurent généralement le transport d'information sur de grandes distances à l'échelle d'un pays. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance. Les débits offerts sont très variables de quelques kbit/s à quelques Mbit/s. Ces réseaux peuvent être terrestres (Utilisation d'infrastructure au niveau : câble, fibre, . . .) ou hertziens, comme les réseaux satellite. Internet est un regroupement de WAN. La Figure I.3 illustre sommairement ces grandes catégories de réseaux informatiques.

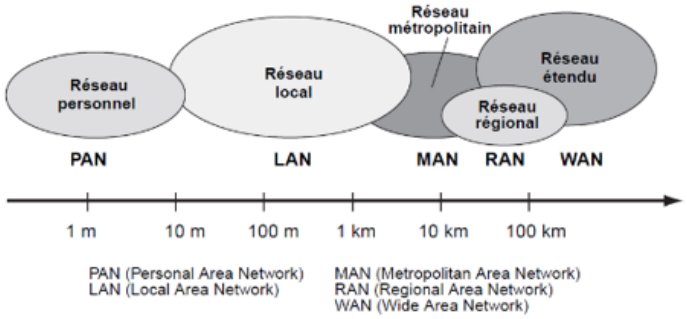


Figure I.3 – Les grandes catégories de réseaux informatiques.[26]

I.2.7 Catégories des réseaux :

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement :

I.2.7.1 L'architecture d'égal à égal (en anglais peer to peer) :

C'est une architecture dans laquelle les participants partagent une partie de leurs propres ressources matérielles (puissance de traitement, capacité de stockage, capacité de liaison réseau, imprimantes, ...). Ces ressources partagées sont nécessaires pour fournir le service et le contenu offerts par le réseau. Donc les participants à un tel réseau sont des fournisseurs de ressources (service et contenu) ainsi que des ressources.[31]

I.2.7.2 L'architecture client- serveur :

C'est un réseau distribué qui se compose d'un système plus performant, le Serveur, et plusieurs systèmes pour la plupart moins performants, les Clients. Le serveur est l'unité centrale d'enregistrement ainsi que le seul fournisseur de contenu et de service. Un client ne demande que du contenu ou l'exécution de services, sans partager aucune de ses propres ressources.[31]

I.2.8 les Equipements d'interconnexion :

les équipement d'interconnexion entre les réseaux sont [25] :

- **répéteur :** permet de régénérer un signal. Il opère au niveau 1 du modèle OSI.
- **concentrateur (hubs) :**permet de connecter plusieurs hôtes entre eux. Il récupère les données binaires parvenant sur un port les diffuse sur l'ensemble des ports. Le hub opère au niveau 1 du modèle OSI.
- **Pont(bridge) :** C'est une sorte de hub, mais en plus intelligent. Il crée plusieurs domaines de collisions, permet le passage de paquets entre plusieurs segments LAN, maintient à jour une table d'adresses MAC. Il opère au niveau 2 du modèle OSI.
- **Switch :** permet de relier divers éléments tout en segmentant le réseau. Il agit dans la couche liaison de données.
- **routeur :**permet de relier de nombreux réseaux locaux de telles façons à permettre la circulation de données d'un réseau à un autre de façon optimale.
- **B-routeurs :** qui associent les fonctionnalités d'un routeur et d'un pont.
- **modem :** qui permet la relation avec internet. De nos jours, les "boxes" des fournisseurs d'accès cumulent les fonctions de modem, de routeur et souvent de point d'accès Wi-Fi.

I.3 Sécurité des réseaux informatiques

I.3.1 Définition de sécurité informatique :

C'est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information, du système d'information et des systèmes et ressources informatiques. Elle consiste, aussi, à s'assurer : l'intégrité, la confidentialité de l'information et la disponibilité des systèmes .[18]

I.3.2 objectifs de la sécurité :

Les trois principaux objectifs de la sécurité informatique, appelées CID (d'après leurs initiales) sont : [27, 15]

1. **Confidentialité :** garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources de l'entreprise.
2. **Intégrité :** garantir que les données échangées sont exactes et complètes
3. **Disponibilité :** garantir l'accès aux ressources, au moment voulu, aux personnes habilitées d'accéder à ces ressources.

.

I.3.3 L'importance du contrôle d'accès réseau

Au sein d'un réseau d'ordinateurs, des systèmes individuels permettent de partager des informations. Les accès non autorisés représentent un risque pour la sécurité. Dans la mesure où un grand nombre de personnes ont accès à un réseau, la probabilité d'accès non autorisé est accrue, en particulier suite à une erreur d'utilisateur. Une utilisation inappropriée des mots de passe peut également conduire à des accès non autorisés. Le contrôle d'accès consiste à définir les accès au réseau et les services disponibles après identification. Le terme AAA est souvent utilisé pour désigner les facettes suivantes de la sécurité : [24]

— **Authentification** (Authentication) : il s'agit de la vérification de l'identité d'un utilisateur.

— **Autorisation** (Authorization) : il s'agit des droits accordés à un utilisateur, tels que l'accès à une partie d'un réseau, à des fichiers, le droit d'écriture, etc.

— **Comptabilité** (Accounting) : : il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

Pour cela, trois techniques ont été utilisées [22] :

1. **Mot de passe :** La protection par mot de passe est bien connue. Une station cherchant à se connecter au réseau doit envoyer un mot de passe à la requête de ce réseau, ou plus généralement d'un point d'accès de celui-ci. Si le mot de passe est correct, l'accès est autorisé, sinon il est interdit. Cette protection est extrêmement simpliste, car il est facile de capturer le mot de passe par écoute passive.
2. **Filtrage sur adresse MAC :** Cette protection consiste à n'autoriser l'accès au réseau qu'à des stations présentant une adresse MAC prédéfinie est connue

du réseau. Cette protection n'est pas non plus très difficile à contourner, car l'écoute passive du réseau permet de récupérer les adresses MAC autorisées. Ensuite, de nombreuses cartes radio permettent de modifier par logiciel leur adresse MAC.

3. **Identificateur de réseau(SSID) :** Cet identificateur inclus dans la norme IEEE 802.11, permet de filtrer le trafic. Un trafic ne portant pas le même identificateur que le réseau que l'on souhaite pénétrer est ignoré par ce dernier. Il est donc nécessaire de connaître le nom du réseau qui est partagé secrètement, pour y pénétrer. Cette protection est en fait très sommaire, car le point d'accès envoie périodiquement en clair des trames indiquant l'identité du réseau, et une écoute de celui-ci permet de récupérer le SSID.

I.4 conclusion

Tout au long de ce chapitre nous avons présenté les notions de base des réseaux informatiques filaires, leur définition, leur architecture et leur classification selon des critères différents (topologie, couverture géographique, fonctionnement). Puis, nous avons abordé les notions de base de la sécurité informatique. Le chapitre suivant est consacré aux réseaux sans fil.

Chapitre II

les réseaux sans fils

II.1 Introduction

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires, ce qui a valu un développement rapide de ce type de technologies.
Dans ce deuxième chapitre, nous allons présenter les réseaux sans fil avec leurs différentes architectures et normes existantes ainsi que leurs faiblesses et limites en termes de sécurité.

II.2 Définition d'un réseau sans fil

Un réseau sans fil (en anglais wireless network) est un réseau dans lequel au moins deux terminaux peuvent communiquer 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 radioélectriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.[25]

II.3 Intérêt des réseaux sans-fils

L'utilisation des réseaux sans fil procure plusieurs avantages, notamment : :

— La mobilité

— L'usage facile dans les endroits à câblage difficile ;

— La réduction du temps de déploiement et d'installation ;

— La réduction des coûts d'entretien ;

— L'augmentation de la connectivité (évolutivité) ;

D'autres part les réseaux sans fils soufrent de problèmes tel que :

— la sécurité

— les interférences des ondes électromagnétiques.

— sensibilité à l'environnement : les obstac, les zones mortes , les phénomènes naturelles (vent, pluie...)

— Débit et portée faibles

— détection des collisions.

— La consommation d'énergie

II.4 Classification des réseaux sans fil

On peut classifier les réseaux sans fil suivant les distances qui séparent les terminaux tout en permettant à ces derniers de rester connectés. Ces distances forment des zones géographiques offrant une connectivité aux terminaux, plus communément appelées zones de couverture ou cellules. La figure II.1 décrit les différentes catégories de réseaux définies en fonction de la taille de la zone de couverture. La figure (II.2) décrit les principales normes existantes.

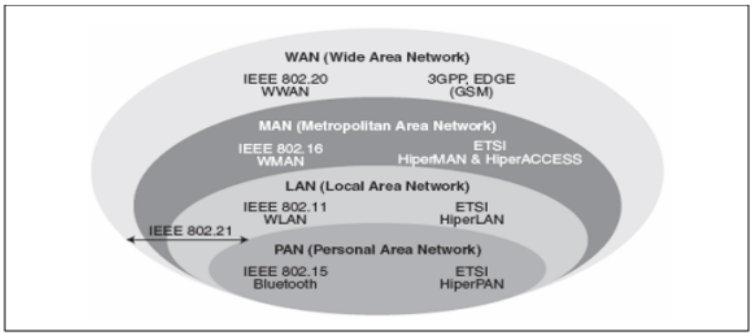


Figure II.1 – Catégories de réseaux sans fil [26]

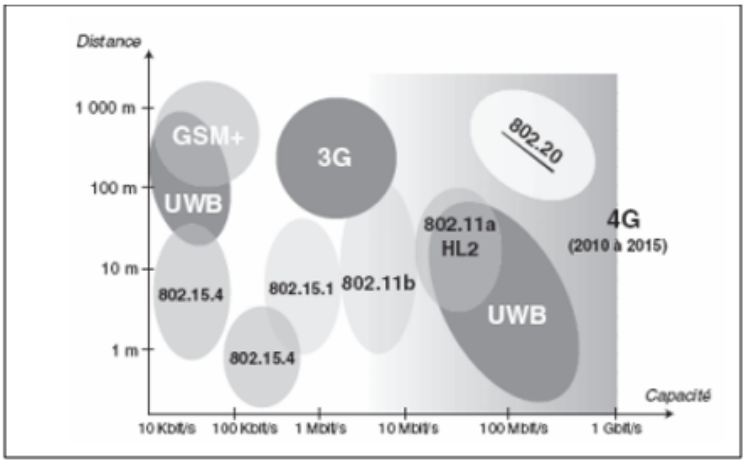


Figure II.2 – Principales normes des réseaux sans fil [26]

II.4.1 Les réseaux personnels sans fil (WPAN : Wireless Personal Area Network) :

Dans cette catégorie on retrouve les réseaux sans fil à l'échelle humaine dont la portée maximale est limitée à quelques dizaines de mètres autour de l'usager (bureaux, salles de conférence, etc.). On y trouve les standards suivants :

— **Bluetooth :** nom commercial de la norme IEEE 802.15.1. Il est aujourd'hui présent dans de nombreux dispositifs (ordinateurs, appareils photo, téléphones portables, ...) car il est peu gourmand en énergie. Il propose un débit théorique de 1 Mb/s pour une portée d'environ 30 mètres. La norme IEEE 802.15.3 (Bluetooth2 ou UWB) est une évolution de la norme Bluetooth permettant des débits plus rapides. Aujourd'hui la dernière génération (Bluetooth5) élargit encore plus la portée jusqu'à 200 mètres [25, 26, 11].

— **ZigBee :** aussi connu sous le nom IEEE 802.15.4, est une technologie un peu similaire au Bluetooth ; il repose sur les ondes radio de 2,4 GHz, et son rôle est également de connecter des équipements entre eux à faible distance (100 m). Il offre un débit assez faible : 250 Kbps. Son intérêt réside dans sa grande simplicité, son faible coût et sa consommation électrique extrêmement basse. Ceci le rend tout à fait adapté pour un grand nombre d'applications, telles que la connexion d'un clavier sans fil à un ordinateur ou l'ouverture d'une porte de garage [25, 15]

— **Infrarouge :** l'infrarouge est utilisé depuis de nombreuses années pour la communication direct entre deux équipements proches l'un de l'autre, tel que la télécommande et la télévision. Cependant, ces ondes ne sont pas capables

de traverser les obstacles, et la puissance du signal se dissipe rapidement : la portée est donc faible. A courte distance, les débits peuvent toutefois être assez élevés : l'organisme IrDA a développé une série de standards, dont le plus rapide à ce jour, le Very Fast Infrared (VFIR) permet d'atteindre un débit de 16 Mb/s [15].

II.4.2 Les réseaux locaux sans fil (WLAN : Wireless Local Area Network)

C'est la catégorie des réseaux locaux sans fil dont la portée va jusqu'à 500 m, pour les applications assurant la couverture d'un campus, un bâtiment, un aéroport, un hôpital, etc. Plusieurs normes de WLAN ont été développées, nous citons dans ce qui suit les deux principales : IEEE 802.11 (Wi-Fi) et Hiperlan2 (High performance radio LAN 2.0).

— **WiFi :**Le nom Wi-Fi (contraction de Wireless Fidelity), correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance) ; cet organisme était chargé de définir un ensemble de contrôles de qualité et des tests d'interopérabilité permettant de garantir qu'un produit respecte bien les normes de l'IEEE et qu'il peut s'interconnecter avec des produits d'autres fournisseurs. Un produit passant ces tests avec succès reçoit le label Wi-Fi qui est un gage de qualité et d'interopérabilité (voir figure II.3). Ainsi un réseau Wi-Fi est en réalité un réseau répondant à la norme 802.11. Wi-Fi utilise deux bandes de fréquences : la bande ISM (Industrial, Scientific and Medical), située dans les 2,4 GHz pour les versions 802.11b et 802.11g, et la bande U-NII (Unlicensed-National Information Infrastructure), située dans les 5 GHz pour la version 802.11a. Aujourd'hui la dernière version du Wi-Fi (WiFi 6 :802.11ax) dépasse la vitesse remarquable de 10 Gbit/s . [25, 26, 15, 17]

Figure II.3 – Le logo de certification de la WiFi Alliance

— **Hiperlan (High Performance Radio LAN) :** C'est une norme Européenne élaboré par l'ETSI (European Telecommunications Standards Institute). Il existe deux types : **HiperLAN1** offre un débit théorique de 23.5 Mbp/s et est basé sur une architecture réseau ad hoc. **HiperLAN2** permet d'obtenir un débit théorique de 54 Mb/s sur une zone d'une centaine de mètres et est basé sur le mode infrastructure. Les deux types fonctionnent dans la bande 5Ghz.[5, 19]

II.4.3 Les réseaux métropolitains sans fil (WMAN : Wireless Metropolitan Network)

Les WMAN, connus aussi sous le nom de Boucle Locale Radio (BLR), visent à remplacer les modems ADSL que l'on trouve sur les réseaux téléphoniques fixes, pour donner à l'utilisateur final des débits du même ordre de grandeur que l'ADSL. Les WMAN sont basés sur la norme IEE 802.16 et offrent un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 km, ce qui oriente principalement cette technologie aux opérateurs de télécommunications. La norme IEEE 802.16, plus connue sous son nom commercial WiMax, permet d'obtenir un débit théorique de 70 Mb/s sur une portée de 50 km [25, 26].

II.4.4 Les réseaux étendus sans fil (WWAN : Wireless Wide Area Network)

WWAN est également connu sous le nom de réseau cellulaire mobile. C'est l'interconnexion des réseaux précédents qui les supporte. Il s'agit des réseaux sans fil

les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Dans cette catégorie, on peut citer le réseau GSM et ses extensions (GPRS/EDGE), le CDMA, UMTS et LTE[25, 26].

II.5 Les réseaux WIFI

Comme il a été précisé plus haut dans le document, les réseaux Wi-Fi proviennent de la norme IEEE 802.11.

II.5.1 Présentation du standard IEEE 802.11

La norme IEEE 802.11 est le standard qui décrit les caractéristiques des réseaux sans fil et elle est l'équivalente de la norme IEEE 802.3 (Ethernet) pour les réseaux filaires. La première version de la norme IEEE 802.11 a été ratifiée en 1997. Le standard IEEE 802.11 et ses différentes extensions ont été conçus à l'origine, afin d'offrir un support de communication fiable, robuste et flexible pour bâtir des réseaux locaux sans fil WLAN, administrés par une ou plusieurs stations de base. Grâce à son large déploiement et son faible coût, ce standard est devenu une solution incontournable dans le monde des réseaux locaux sans fil[26, 15, 33].
La norme 802.11 offre deux modes de fonctionnement : le mode infrastructure et le mode sans infrastructure (mode Ad Hoc) [26].

II.5.1.1 Mode Infrastructure :

Dans ce mode, chaque station se connecte via une liaison sans fil à un Point d'accès (AP) qui joue le rôle de station de base. On dit que la station est le client et l'AP est le maître. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé **BSS** (Basic Service Set) qui couvre un espace appelé cellule ou une **BSA**(Basic Set Area). Chaque SS est identifié par un **BSSID** (BSS IDentifier), un identifiant de 6 octets (48 bits) correspondant à l'adresse du point d'accès.

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution **DS** (Distribution System) afin de constituer un ensemble de services étendu **ESS** (Extended Service Set) qui couvre un espace appelé **ESA** (Extended Service Area), composé de plusieurs cellules. Le DS peut être un réseau filaire Ethernet (cas le plus fréquent), un

câble de point à point, ou encore une liaison sans fil.

Un ESS est identifié par un nom **ESSID** (ou simplement le SSID) de 32 octets correspondant au nom du réseau et représente en quelque sorte un premier niveau de sécurité : la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu[26, 25, 15].

II.5.1.2 Mode sans Infrastructure (Ad Hoc)

Dans les réseaux de type Ad Hoc, chaque station communique directement avec les stations situées à sa portée, sans passer par un point d'accès afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès. L'ensemble formé par les différentes stations est appelé IBSS (Independant Basic Service Set). L'IBSS constitue donc un réseau provisoire permettant à des personnes géographiquement proches d'échanger des données. Il est identifié par un SSID (Service Set Identifier) comme l'infrastructure. Comme il n'y a pas de point d'accès, les stations n'intègrent qu'un certain st un ESS en mode nombre de fonctionnalités, telles les trames utilisées pour la synchronisation[26, 25, 15].
Une vue complète des éléments architecturaux proposés par l'IEEE 802.11 peut se résumer par le schéma de la figure II.4

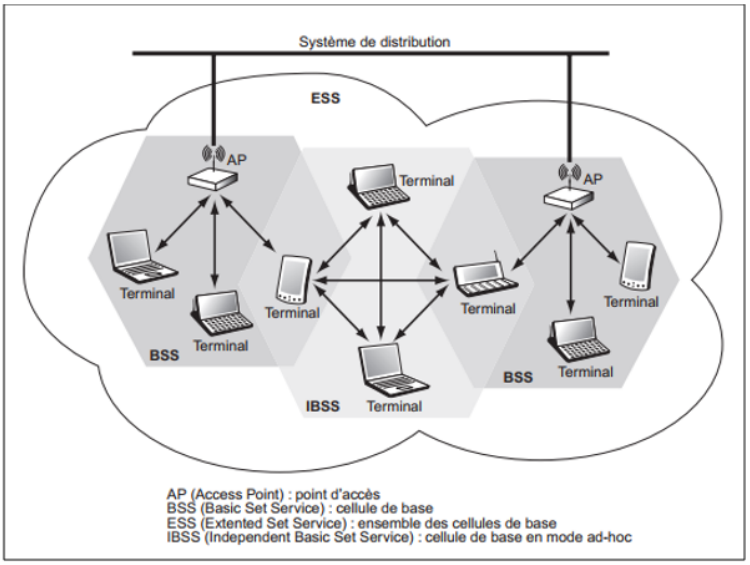


Figure II.4 – Architecture type d'un WLAN 802.11[26]

II.5.2 Les évolutions de 802.11

Au fil des années, des améliorations importantes ont été apportées au standard 802.11. Certaines concernent la couche physique, d'autres concernent la couche MAC :

— **802.11 (802.11 legacy) :** est la première norme 802.11 sortie en 1997 et qui permettait d'atteindre des débits de 1 ou 2 Mbps en utilisant des méthodes de codage basées sur Direct-Sequence Spread Spectrum (DSSS) et Frequency Hopping Spread Spectrum (FHSS) dans la bande des 2.4 GHz[15].

— **802.11a (wifi) :**propose 8 canaux dans la bande des 5 GHz au lieu de 2,4 GHz, modulation radio de type OFDM, débit maximal théorique de 54 Mb/s sur une portée d'environ 20 m. la norme IEEE-802.11a possède un avantage dans la mesure où elle subit moins d'interférence. Cependant, cette fréquence élevée pénètre plus difficilement les murs et réduit la zone de couverture des appareils. [15, 33, 12]

— **802.11b (wifi 2) :** fréquence radio à 2,4 GHz, modulation DSSS ou HR-DSSS (High Rate DSSS), débit maximal théorique de 11 Mb/s. Ratifiée en septembre 1999, 802.11b est l'amendement de 802.11 qui a donné sa popularité au WiFi. Bien que 802.11b soit encore largement utilisé, il est maintenant supplanté par 802.11g [15, 33, 12].

— **802.11g (wifi 3) :** constitue une amélioration directe de 802.11b en proposant un débit maximum théorique de 54 Mb/s sur la bande des 2,4 GHz. Il utilise la modulation radio de type OFDM. Toutefois, 802.11g garde une compatibilité avec 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b[33].

— **802.11n (wifi 4) :** propose un débit bande de base de 540 Mbits/s sur une portée de 50 mètres environ grâce à l'utilisation conjointe des techniques MIMO (Multiple Input Multiple Output) et OFDM. Il propose l'utilisation des deux bandes de fréquences 2,4 GHz et 5 GHz. Comme 802.11g, cette norme reste compatible avec 802.11. De plus, elle reprend les concepts de 802.11e pour la gestion de la Qualité de Service, de 802.11i pour la sécurité et de 802.11f pour la gestion des handovers. Cette norme a été ratifiée le 11 septembre 2009[2]

— **802.11ac (wifi 5) :** cette norme exploite la fréquence radio à 5 GHz avec une largeur de canal allant jusqu'à 160 MHz ainsi que la modulation radio de type OFDM et offre un débit maximal théorique de 7Gbps. La norme 802.11ac introduit un nouveau procédé avec le Beamforming qui est une technologie qui permet d'orienter le signal vers les appareils connectés assurant ainsi une

meilleure connexion, une meilleure portée tout en ne gaspillant pas autant d'énergie et aussi utilise la technologie Mu-MIMO (Multi-user MIMO) qui permet de communiquer avec plusieurs appareils simultanément. Cette norme a été ratifiée le 8 janvier 2014 [25, 17].

— **802.11ax (wifi 6) :** également connue sous la dénomination High-Efficiency WLAN (HEW) cette norme est combiné les technologies**OFDMA**(Orthogonal Frequency Division Multiple Access) et **Mu-MIMO** ce qui permet d'augmenter le début théorique jusqu'à 9,6 Gbps, qui est 37% plus élevé que celui du 802.11ac . OFDMA permet au Wi-Fi de communiquer avec plusieurs appareils simultanément en divisant le canal Wi-Fi. ainsi que cette norme utilise la technologie TWT (Target Wake Time) qui permet au routeur d'indiquer aux appareils connectés quand mettre leur Wi-Fi en veille et ainsi d'économiser leur batterie[17, 8].

II.5.3 Architecture en couches du standard 802.11

Comme tous les standards de l'IEEE La norme 802.11, couvre les deux premières couches du modèle OSI [26] : la couche physique (niveau 1) et la couche liaison de données (niveau 2).

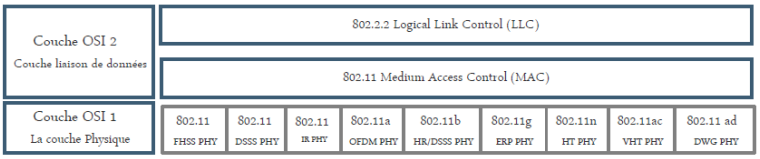


FIGURE II.5 – modèle en couches de l'IEEE 802.11

II.5.3.1 La couche physique :

La couche physique a pour rôle de transporter correctement la suite de signaux 0 ou 1 que l'émetteur souhaite envoyer au récepteur. Elle est divisée en deux sous-couches [26] :

— **la sous-couche PMD(Physical Medium Dependent) :**qui gère l'encodage des données et effectue la modulation.

— **la sous-couche PLCP** (Physical Layer Convergence Protocol) qui s'occupe de l'écoute du support et fournit un CCA (Clear Channel Assessment) à la couche MAC pour lui signaler que le canal est libre.

On distingue les techniques d'étalement (transmission ou modulation) utilisé dans la norme 802.11 :

— **FHSS (Frequency Hopping Spread Spectrum) :** Ce mode utilise une modulation par déplacement de phase gaussienne "Gaussian Frequecy Shift Keying" (GFSK) avec un étalement de spectre par saut de fréquences dans la bande 2,4 GHz. Le principe consiste à diviser la bande de fréquences 2.4 GHZ en sous-canaux de 1 MHz de largeur et les communications se font en sautant successivement d'un canal à un autre, selon une séquence et un rythme convenus à l'avance entre l'emetteur et le récepteur. Cette technique de modulation permet un débit physique de 1 ou de 2 Mbit/s. Le FHSS n'est utilisé que dans la première version du standard 802.11 [15].

— **DSSS (Direct Sequence Spread Spectrum) :** Est une technique d'étalement de spectre, mais contrairement au FHSS, aucun saut de fréquence n'a lieu : la modulation DSSS provoque des transitions d'état très rapides (chipping) qui tendent à étaler le spectre du signal et ceci en provoquant artificiellement un débit très élevé. Pour ce faire, l'émetteur envoie une séquence de plusieurs bits, appelés des "chips", pour chaque bit d'information à transmettre. Le 802.11 a divise la bande des 2.4 GHz en 14 canaux de 22 MHz chacun. Pour communiquer, l'émetteur et le récepteur doivent se mettre d'accord sur un canal fixe à utiliser. Cette technique permet un débit physique de 1 Mbit/s ou 2 Mbit/s. .[15]

— **HR-DSSS(High-Rate DSSS) :** Pour atteindre des débits de 5,5 Mb/s ou 11 Mb/s, le 802.11b a amélioré encore le procédé de chipping en utilisant la modulation CCK (Complementary Code Keying) pour atteindre ce qu'on appelle le HR-DSSS. Celle-ci repose toujours sur le même principe de base d'étalement par chipping avec la modulation 4DPSK. Toutefois, au lieu d'utiliser toujours le même code d'étalement pour étaler le signal, elle utilise jusqu'à 64 codes différents, ce qui permet de transporter 6 bits d'information (car $2^6 = 64$) en plus des deux bits autorisés par la modulation 4DPSK[15].

— **OFDM (Orthogonal Frequency-Division Multiplexing) :** Cette technique est considérée la plus puissante des modulations précédentes car elle permet à la fois les débits les plus importants (54Mbs), la meilleure résistance au multipath, et une grande capacité de partage du spectre. L'OFDM repose sur le principe du multiplexage : permettre la transmission simultanée de plusieurs communications sur une même bande de fréquences. Il existe deux types de multiplexage :

1. **TDM (Time Division Multiplexing) :** chaque communication dispose de sa tranche de temps pour émettre des données et peut utiliser l'ensemble du spectre.

2. **FDM (Frequency Division Multiplexing) :** en partageant les différentes communications par fréquences, un spectre assez large est divisé en de multiples sous-porteuses (sub-carriers) et les données sont émises simultanément sur chaque sous-porteuse [15].

Pour résoudre les problèmesd'interférences entre les sous-porteuses, l'OFDM utilise une fonction mathématique assez complexe pour rendre les sous-porteuses orthogonales, les porteuses sont placées dans le spectre de fréquences de telle sorte que les pics de puissance d'une porteuse donnée correspondent aux zéros des autres porteuses.

— **IR(infra red) :** Travaille avec des ondes infrarouges et n'est utilisé que dans les cas où les distances entre les différentes stations sont faibles. La couche physique 802.11 reposant sur l'infrarouge n'a jamais connu le succès parce que de meilleurs produits, basés sur l'infrarouge et standardisés par IrDA, existaient déjà [15]

En plus des technique de modulation la norme 802.11 utilise les technique multi-antennes suivantes :

— **MIMO (Multiple Input Multiple Output)**[26, 17] : MIMO est une technologie permettant grâce aux propriétés du multipath de transporter plusieurs flux en parallèle sur des antennes différentes mais en utilisant la même fréquence. Elle a pour objectif d'améliorer considérablement le débit, la portée et la fiabilité du WiFi. On distingue aussi 2 variantes de MIMO selon le nombre d'utilisateurs recevant simultanément des données sur les même porteuses :

- **Le SU-MIMO (Single User) :** permet d'envoyer des données via les différentes antennes vers un seul utilisateur à un instant donné. Il a été inauguré avec le standard 802.11n.
- **Le MU-MIMO (Multi User)** permet aux stations ayant plusieurs antennes de transmettre plusieurs flux de données à plusieurs utilisateurs simultanément sur le même canal de fréquence. Il a été inauguré avec le standard 802.11ac.

— **Beamforming :**Il permet à l'émetteur de focaliser automatiquement le signal qu'il émet en direction du récepteur au lieu d'envoyer toute la puissance dans toutes les directions afin d'en augmenter la portée et de limiter les interférences avec les réseaux voisins. Cette technique est utilisée par le 802.11ac[15].

II.5.3.2 La couche liaison de données

La couche liaison de données est composée essentiellement de deux sous-couches, LLC (Logical Link Control) et MAC. La couche LLC utilise les mêmes propriétés que la couche LLC 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique au 802.11. Le rôle de la couche MAC 802.11 est comparable à la couche Ethernet 802.3, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente.
Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version classique telles que la sécurité des communications, l'économie d'énergie, la fragmentation, le réassemblage, le contrôle d'erreur ou encore comment assurer une bonne qualité de service, en particulier pour les communications multimédia. La couche MAC est donc en quelque sorte le "cerveau " du 802.11[26, 15].

Le format des trames MAC 802.11 : La figure II.6, représente le format standard d'une trame MAC 802.11. Les données sont placées dans le champ Données, d'une longueur variable. Les stations source et destination ainsi que les points d'accès utilisés pour relayer la trame sont identifiées par leurs adresses physiques, sur 6 octets, dans les champs de type @ [34].

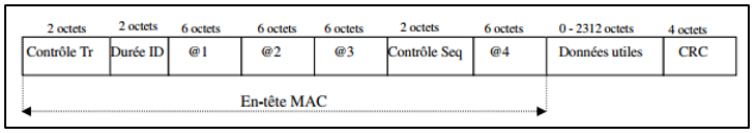


Figure II.6 – La structure d'une trame MAC 802.11

Il existe trois types de trames qui sont envoyées parmi les stations d'un réseau sans fil 802.11. Ce type, codé dans le champ Contrôle Tr, catégorise les trames en : [34] :

1. **Trames de données** ;
2. **Trames de contrôle** , utilisées pour coordonner l'accès au médium. Dans cette catégorie entrent les trames d'acquittement - ACK (Acknowledgement) - ou les trames RTS (Request toSend) et CTS (Clear to Send), dont le rôle est d'éviter les collisions avec des stations plus éloignées. À cause de leur caractère de contrôle, cette catégorie de trames est prioritaire pour l'accès au medium.
3. **Trames de management**. Celles-ci ont la même priorité d'accès au medium que les trames de données. Leur rôle est l'échange des informations relatives

strictement au protocole 802.11 (synchronisation, scanning, authentification, association) entre les stations du réseau sans-fil.

La couche MAC 802.11 assure les fonctionnalités suivantes :

- Accès au support
- Mobilité : roaming, association désassociassions
- Le contrôle d'erreur
- L'économie d'énergie

Les techniques d'accès au support : Il existe deux méthodes d'accès fondamentalement différentes au niveau de la couche MAC : [26, 28, 13] :

1. **le mode DCF** (Distributed Coordination Function) : Un mode d'accès au canal dit à compétition qui propose un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). Ce mode peut aussi bien être utilisé en mode ad-hoc qu'en mode infrastructure.
2. **le mode PCF** (Point Coordination Function) : Fondée sur l'interrogation à tour de rôle des terminaux, ou polling, sous le contrôle du point d'accès, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui demandent une gestion du délai utilisé pour les applications temps réel, telles que la voix ou la vidéo. Il ne peut être utilisé pour des réseaux ad-hoc multi-sauts puisqu'il n'y a pas de nœud fixe qui puisse prendre en charge la coordination du réseau.

Description du mode d'accès DCF : Le DCF est la technique d'accès générale utilisée pour permettre des transferts de données asynchrones en best-effort. D'après le standard, toutes les stations doivent la supporter. Le DCF s'appuie sur le CSMA/CA. Dans les réseaux sans-fil la détection des collisions n'est pas possible ; la transmission couvre la réception de signaux sur la même fréquence et ne permet pas à la station d'entendre la collision : les liaisons radio ne sont jamais full-duplex. La technique d'accès de Wi-Fi doit tenir compte de ce phénomène [25]. Pour pallier ces problèmes, 802.11 utilise un mécanisme d'évitement de collision associé à un système d'accusé de réception : le CSMA/CA. Les autres éléments importants sont les espaces inter-trames IFS (Inter Frame Spacing) qui correspondent à un intervalle de temps entre la transmission de deux trames et le temporisateur d'émission. Il en existe trois types selon 802.11 : [26] :

— **SIFS** (Short Initial inter-Frame Spacing), représente le plus cours des IFS et permet de séparer deux trames d'un même dialogue (envoie de données, Ack, etc.)

— **PIFS** (PCF IFS), utilisé par le point d'accès pour bénéficier d'une priorité supérieur, dans le cas de réseaux à accès au support mixte DCF/PCF.

— **DIFS** (DCF IFS), utilisé en DCF (c'est à dire en CSMA/CA) lorsqu'une station veut initier une communication.

SIFS < PIFS < DIFS

La temporisation d'émission, appelé NAV (Network Allocation Vector) est un timer qui détermine l'instant auquel la trame peut être transmise avec succès,il permet d'éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé[26].

L'algorithme de CSMA/CA [26, 13] : Les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations qui s'y trouvent.

— Lorsqu'une station envoie une trame, les autres stations l'entendent et, pour éviter une collision, mettent à jour un timer, appelé NAV (Network Allocation Vector), permettant de retarder toutes les transmissions prévues. Le NAV est calculé par rapport à l'information située dans le champ durée de vie, ou TTL, contenu dans les différentes trames (données, ACK, etc.).

— Quand une station veut émettre, elle écoute le support : -Si le support est libre durant un temps spécifique (DIFS), la station attendre une période de durée aléatoire supplémentaire appelée backoff puis transmet ses données immédiatement. -Si le support est encore occupé, elle continue de l'écouter jusqu'à ce qu'il soit libre. Quand le support devient disponible durant un temps spécifique (DIFS) elle retarde encore sa transmission en utilisant l'algorithme de back-off puis transmettre ses données.

— Si les données envoyées sont bien reçues, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer leur bonne réception.

— Si la station émettrice reçoit l'acquittement alors la trame est correctement reçue et aucune collision n'a eu lieu.

— Sinon doit retransmettre la trame.

— Lorsque la station source transmet ses données, les autres stations mettent à jour leur NAV, en incluant le temps de transmission de la trame de données, le SIFS et l'ACK.

L'algorithme de Backoff (Backoff process)[26, 13] : Cette algorithme permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent

transmettre des données en même temps. Dans Wi-Fi, le temps est découpé en tranches (SlotTime) qui sont un peu plus petit que la durée de transmission minimale d'une trame. Grâce à cet algorithme, les stations ont la même probabilité d'accéder au support. Son seul inconvénient est de ne pas garantir un délai minimal et donc de compliquer la prise en charge d'applications temps réel telles que la voix ou la vidéo.

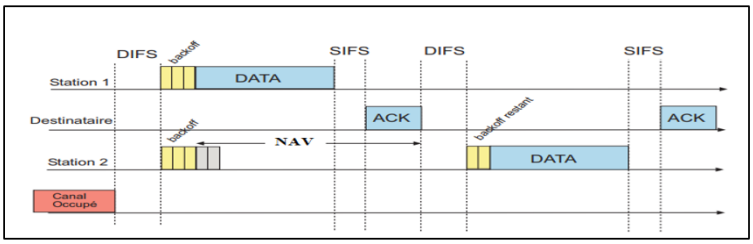


FIGURE II.7 – Transmission des trames suivant CSMA/CA

Le mécanisme RTS/CTS : Un des problèmes des réseaux sans fil est celui de la station cachée *(hidden node problem)* . Deux stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station peuvent entendre l'activité de cet AP mais ne pas s'entendre l'une l'autre du fait que la distance entre les deux est trop grande ou qu'un obstacle les empêche de communiquer entre elles [26].

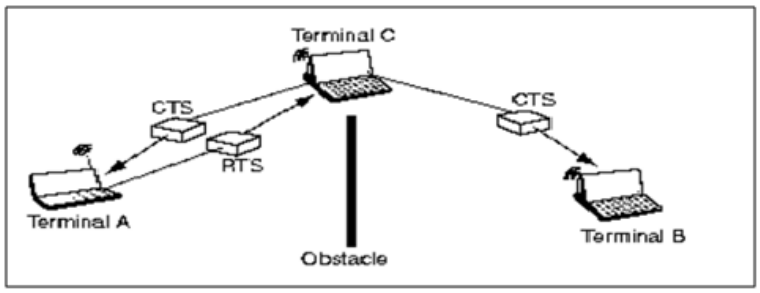


FIGURE II.8 – Problème de la station cachée (hidden node problem)[26]

La figure II.8 montre une station A cachée de la station B mais pas de la station C. Si A transmet des informations à C et que B désire faire de même, il y aura une collision car B n'a pas détecter la transmission entre A et C. [26] Le mécanisme de réservation fondé sur l'envoi de trames RTS/CTS (Request to Send/Clear to Send) entre une station source et une station destination avant tout envoi de données. Ce mécanisme de réservation RTS/CTS permet de résoudre le problème de la station cachée : [26, 13]

— Une station source qui veut transmettre des données envoie un petit paquet RTS contenant la durée de la transmission (combien de temps le canal sera

réservé) après avoir attendu un temps DIFS et un temps aléatoire.

— Toutes les stations du BSS entendant le RTS lisent le champ TTL du RTS et mettent à jour leur NAV.

— La station destination ayant reçu le RTS répond, après avoir attendu pendant un SIFS, en envoyant un petit paquet CTS.

— Les autres stations entendant le CTS lisent le champ TTL du CTS et mettent à nouveau à jour leur NAV.

— Après réception du CTS par la station source, cette dernière est assurée que le support est stable et réservé pour sa transmission de données.

Cela permet à la station source de transmettre ses données ainsi que de recevoir l'ACK sans collision.

Lorsque les trames à envoyer sont petites c'est CSMA/CA qui est utilisé (car utilisation du RTS/CTS nécessite l'envoi de deux trames avant de pouvoir émettre de l'information). Dans le cas où les trames sont plus grandes qu'un certain seuil (RTS Threshold), c'est alors RTS/CTS qui est utilisé (Comme les trames RTS/CTS réservent le support donc il est habituellement utilisé pour envoyer de grosses trames).[26]

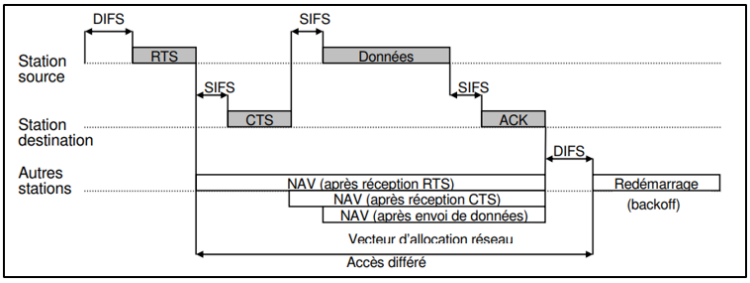


Figure II.9 – Transmission en utilisant les trames RTS/CTS [26]

En conclusion, le CSMA/CA permet de partager l'accès. Le mécanisme de réservation RTS/CTS évite les problèmes de la station cachée. Tous ces mécanismes entraînent toutefois l'ajout aux trames Wi-Fi d'en-têtes, que les trames Ethernet ne possèdent pas. C'est pourquoi les réseaux Wi-Fi montrent toujours des performances plus faibles que les réseaux locaux Ethernet.[26]

Description du mode d'accès PCF : Le mode DCF introduit un mode d'accès à compétition, l'acquisition du support n'est pas bornée et, par conséquent, ce mode de transmission ne convient pas aux données ayant des exigences temporelles strictes comme les flux multimédias. Le principe de base de la PCF est de centraliser la gestion de l'accès au médium d'une cellule. C'est le point d'accès qui

indiquera à chacun des stations qui lui sont rattachées quand elles doivent émettre leurs paquets. Le back-off aléatoire devient ainsi en partie inutile.

La méthode du Polling est une méthode PCF (Point Coordination Function), elle nécessite un point de coordination (PC, Point Coordination). Le point de coordination est un point d'accès, le Polling ne fonctionne donc pas dans un réseau ad hoc. Le Polling, contrairement à CSMA/CA et RTS/CTS, permet de garantir la qualité de Service, de ce fait il est utilisé pour la transmission des donnés temps réel, telles que la voix ou la vidéo[13, 34].

PCF	**DCF**
Mode infrastructure	Mode ad hoc et mode infrastructure
Données synchrone (Données sensibles)	Données asynchrone
Peu Implémenté	C'est la plus utilisé
Optionnelle	Techniques par défaut (obligatoire)
Priorité d'accès supérieure	Priorité d'accès basse
Sans collision	Possibilités de collision
Contrôle par le point d'accès	Possibilité broadcast et multicast
Interrogatoire (polling)	Chance égale aux utilisateurs

Tableau II.1 – La différence PCF et DCF

II.5.4 La mobilité & Le Roaming :

Les réseaux sans fils offrent l'avantage majeur de la mobilité qui est le fait qu'un terminal doit pouvoir se déplacer et donc passer d'une cellule. Cela est rendu grâce à une technique appelée handover (Roaming). Le Roaming est le processus de mouvement d'une cellule vers une autre sans perdre la connexion au réseau (sans interruption de la communication).(voir Figure II.10).

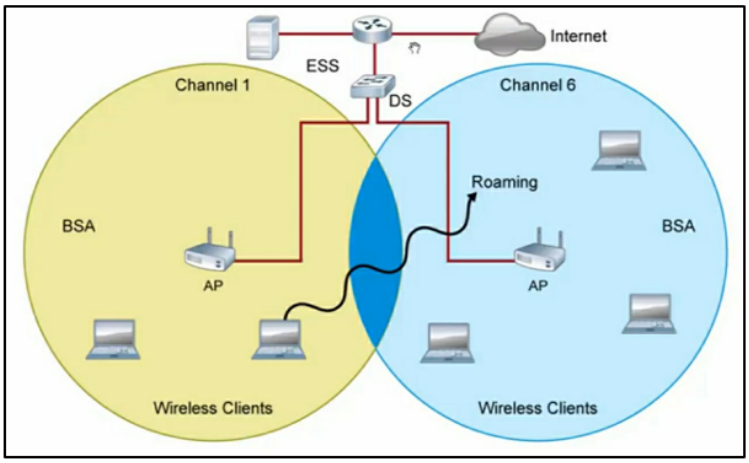


Figure II.10 – handover (Roaming) dans les WLAN

Le standard définit certaines règles, telles que la synchronisation, l'écoute passive

et active ou encore l'association et la réassociation, qui permettent aux stations de choisir le point d'accès auquel elles veulent s'associer [26]

II.5.4.1 Synchronisation

Lorsque les terminaux se déplacent, c'est-à-dire lorsqu'ils changent de cellule ou qu'ils sont en mode d'économie d'énergie, ils doivent rester synchronisés pour pouvoir communiquer. Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès. Pour conserver la synchronisation, le point d'accès envoie périodiquement des trames balises, ou Beacon Frames, qui contiennent la valeur d'horloge du point d'accès. Lors de la réception de ces trames, les stations mettent à jour leurs horloges pour rester synchronisées avec le point d'accès [26].

II.5.4.2 Association

Quand un terminal veut accéder à un BSS ou ESS, une station doit s'associer auprès d'un point d'accès, selon un certain nombre de critères (la puissance du signal, le taux d'erreur des paquets ou la charge du réseau). Si la puissance du signal du point d'accès est trop faible, la station cherche un autre point d'accès plus approprié.
L'association, tout comme la réassociation, comporte les différentes étapes suivantes : [26]

1. La station écoute le support ou Le scan
2. Après avoir trouvé le meilleur point d'accès, elle s'authentifie.
3. Si cette phase réussit, la station s'associe avec le point d'accès et transmet ses données.

II.5.4.3 L'écoute du support (scan)

Cette écoute peut se faire de deux manières différentes, actives ou passives selon des critères tels que les performances ou la consommation d'énergie :

— **Écoute passive :** La station attend de recevoir une trame balise (Beacon) qui sont envoyées périodiquement par les points d'accès.

— **Écoute active :** la station envoie une trame de requête (Probe Request Frame) et attend une réponse (Probe Response). Dès qu'un ou plusieurs points d'accès lui répond, elle enregistre les caractéristiques de ce dernier.

Une fois l'écoute terminée, la station trie les informations récupérées sur les points d'accès et choisit le plus approprié, essentiellement en fonction de la qualité du lien (rapport signal sur bruit). [26, 23]

II.5.4.4 Authentification et association

Après le choix d'un point d'accès pour s'associer avec, la station va initier la procédure d'authentification qui sera détaillée dans le prochain chapitre. Après que la station est authentifiée auprès du point d'accès, elle envoie une trame Association Request et le point d'accès répond avec une trame Association Response. Si la réponse est positive, la station et le point d'accès peuvent commencer à s'échanger entre eux des trames de données.[26, 23]

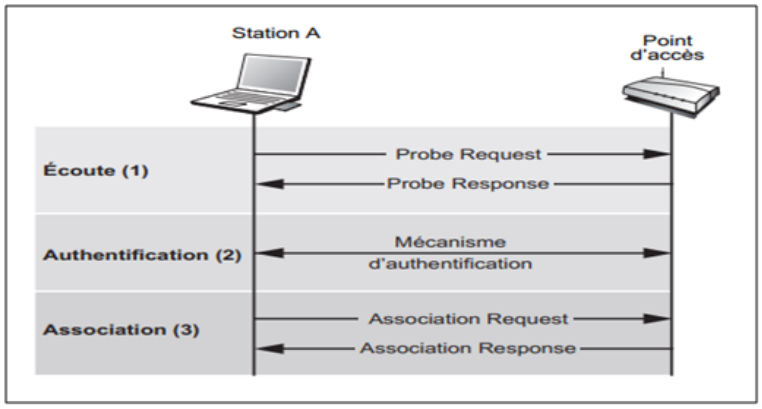


Figure II.11 – Mécanisme d'association d'une station avec un point d'accès [26]

II.5.4.5 Réassociation

Les réassociations s'effectuent lorsqu'une station se déplace physiquement par rapport à son point d'accès d'origine, entraînant une diminution de la puissance du signal. Dans d'autres cas dues à des changements de caractéristiques de l'environnement radio ou à cause d'un trafic trop élevé sur le point d'accès. Dans ce cas, le standard fournit une fonction d'équilibrage de charge, ou Load Balancing, qui permet de répartir la charge de manière efficace au sein du BSS ou de l'ESS et ainsi d'éviter les réassociations. Le processus de réassociation est similaire au celui de l'association initiale. L'élément nouveau para rapport à l'association initiale est la spécification de l'ancien point d'accès de la station dans la trame Reassociation Request qui peut être utilisée pour échanger des messages entre points d'accès (l'ancien et le nouveau).[26, 23]

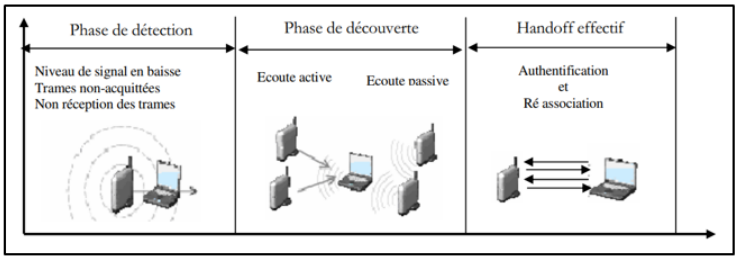


FIGURE II.12 – Les phases du handoff (Roaming) dans 802.11[23]

II.6 La sécurité dans les réseaux Wi-Fi

Le Wi-Fi utilise les ondes radio comme support de transmission, présente plusieurs avantages par rapport aux réseaux locaux filaires notamment la simplicité d'installation et la mobilité. Cependant, il est confronté à plusieurs problèmes de sécurité. Tandis que le support est partagé, tout ce qui est transmis et envoyé peut donc être intercepté.

II.6.1 Les principes de la sécurité

D'une manière générale, la sécurité dans les réseaux s'appuie sur les cinq principes fondamentaux [26, 15, 20] :

— **Identification :** L'utilisateur d'un système ou de ressources diverses possède une identité qui détermine ses lettres de crédit et ses autorisations d'usage. Cette dernière peut être vérifiée de multiple manières, compte utilisateur (Login) d'un système d'exploitation ou techniques biométriques tel que l'empreinte digitale, empreinte vocale.etc.

— **Authentification :**Cette opération consiste à faire la preuve de son identité. Par exemple on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé.

— **Confidentialité :** seules les personnes habilitées ont accès au contenu du message. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.

— **Intégrité :** garantit que les données reçues sont exactement celles qui ont été émises par l'émetteur autorisé.. Le chiffrement évite l'écoute indiscrète, mais il ne protège pas contre la modification illicite des informations par un intervenant mal intentionné. La définition de mécanismes et de techniques est nécessaire pour assurer cette dernière.

— **Disponibilité :** le réseau doit être accessible en tout temps et dans des conditions acceptables.

— **Non répudiation :** permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire. La fonction de non-répudiation peut s'effectuer à l'aide d'une signature à clé privée ou publique ou par un tiers de confiance qui peut certifier que la communication a bien eu lieu.

II.6.2 Les mécanismes de cryptographie

II.6.2.1 Définition

Lacryptographietraditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clef. Le but la cryptographie est de répondre aux objectifs de la sécurité. Pour cela, elle utilise les mécanismes décrits ci-après. [1]

II.6.2.2 Chiffrement symétrique ou à clé secrète

Il consiste à utiliser la même clé appelée "clé secrète" (connue seulement par les interlocuteurs) pour chiffrer et déchiffrer un message (voir Figure II.13). Les algorithmes les plus utilisés actuellement sont le DES/3DES, AES, RC5, etc

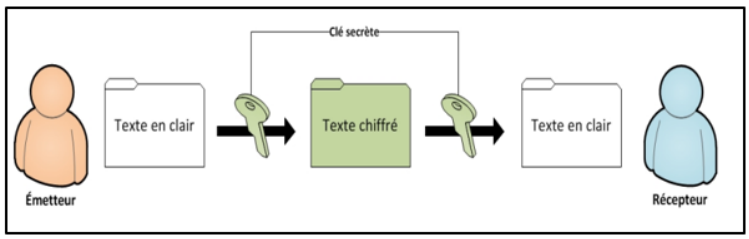


Figure II.13 – Algorithme Symétrique

1. Gh. Labouret. Introduction à la cryptographie. http ://www.labouret.net/crypto/ . consulter le 06/03/2020.

II.6.2.3 Chiffrement asymétrique ou à clé publique

Le concept de la cryptographie asymétrique a été inventé par Whitfield Diffie et Martin Hellman en 1976 pour résoudre le problème de distribution des clés posé dans la cryptographie symétrique. La cryptographie asymétrique utilise une paire de clés : une clé dite publique qui chiffre le message et une autre clé dite privée qui le déchiffre. La clé publique est connue par tous les autres utilisateurs, alors que la clé privée n'est connue que par son propriétaire ; de plus on ne peut pas déduire l'une grâce à l'autre. Ainsi, si on veut envoyer un message à un utilisateur on utilise la clé publique de ce même utilisateur pour chiffrer le message, et il est le seul à pouvoir déchiffrer le message grâce à sa clé privée. Les algorithmes les plus utilisés sont le RSA, DSA, le protocole d'échange de clés Diffie-Hellman, etc. L'avantage de ce type d'algorithmes est la facilité de distribution et de gestion des clés et l'inconvénient réside dans la lenteur des calculs qui sont très complexes (voir Figure II.14).

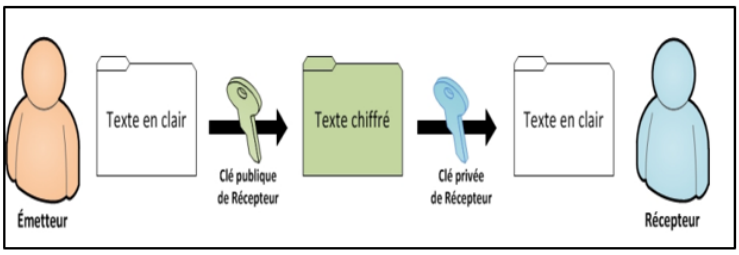


Figure II.14 – Algorithme Asymétrique

II.6.2.4 Signature numérique

Appelée aussi signature électronique, elle a pour fonction d'authentifier l'émetteur. Elle consiste à chiffrer le haché du message avec la clé privée de l'émetteur et l'envoyer au destinataire qui le déchiffre avec la clé publique de l'émetteur. A la réception du message chiffré, le récepteur déchiffre le message et calcule son haché pour le comparer avec le haché reçu ; si les deux hachés sont identiques alors le message est intègre sinon le message a été corrompu (voir Figure II.15)

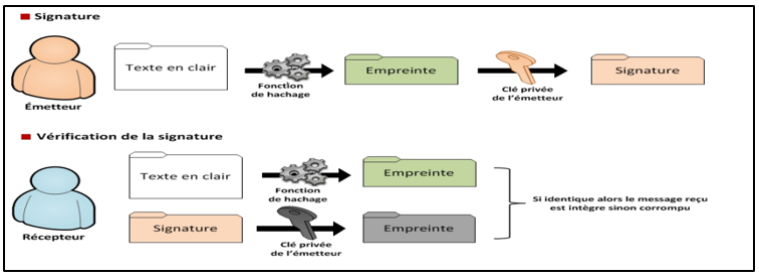


Figure II.15 – Signature numérique

II.6.2.5 Certificat numérique

C'est un document électronique représentant la carte d'identité numérique d'une entité à qui il appartient. Il contient sa clé publique, ainsi qu'un certain nombre d'informations concernant cette entité. Ce document est signé par une autorité de certification ayant vérifié les informations qu'il contient. Le format de certificat le plus courant provient du standard X.509 v2 ou v3. La syntaxe utilisée est l'ASN.1 [26].

importante des Fonctions de Hachage :

Une fonction de hachage ou fonction de condensation est une fonction qui convertie un message clair de longueur quelconque en un message de longueur fixe inférieure à celui du départ, le message obtenu est appelé "haché", "résumé", ou "condensé". La fonction doit être dans un seul sens de telle sorte qu'avec le haché on ne puissent pas trouver le message en clair. De plus on ne doit pas trouver avec deux messages clairs différents le même haché. Les fonctions de hachage garantir l'intégrité des données. Parmi les fonctions de hachage les plus utilisées, notons : MD5 (Message Degest 5), SHA-1 (Standard Hash Algorithm - 1)

II.6.3 Les attaques d'un réseau Wi-Fi

II.6.3.1 Spoofing (usurpation)

Le spoofing consiste à usurper soit l'adresse MAC, soit l'adresse IP (après l'intrusion) d'une autre machine. En modifiant l'adresse source dans l'en-tête du paquet, le récepteur croira avoir reçu un paquet de cette machine.

II.6.3.2 Le déni de service (DoS)

Dans ce type d'attaque, l'attaquant inonde le réseau par des messages valides ou non valides affectant la disponibilité des ressources du réseau. Ce type d'attaque peut s'opérer de différentes manières au niveau des couches 1 et 2 du modèle OSI :

— **Attaque par brouillage radio sur la couche physique :** les ondes radio sont très sensibles aux interférences, un pirate peut exploiter cette faille afin de brouiller toutes les communications d'un réseau Wi-Fi en utilisant un puissant émetteur radio sur la fréquence de celui-ci.

— **Attaque de désauthentification au niveau de la couche MAC :** cette faille vient du fait que rien n'est prévu dans le standard 802.11 pour sécuriser les trames de management. Un pirate peut alors usurper l'identité d'un AP

et utiliser des trames de dés-authentification pour déconnecter un utilisateur précis du réseau, ou alors envoyer un flux continu de ces trames à toutes les stations connectées au point d'accès pour empêcher l'utilisation de ce dernier [15].

II.6.3.3 La modification de messages (Man-In-The-Middle active)

Ce type d'attaque consiste à dévier toutes communications entre deux terminaux pour les faire transiter par la machine attaquante qui permet à l'attaquant de modifier un message légitime en supprimant, ajoutant, modifiant ou en réorganisant le message [15].

II.6.3.4 L'intrusion

L'intrusion consiste à s'introduire au sein du réseau WiFi pour consulter voire modifier les données du système informatique (bases de données, fichier, e-mails...) ou encore pour profiter de la connexion à Internet. Si aucune sécurité n'est mise en oeuvre l'intrusion est trivial il suffit de s'associer à l'un des points d'accès du réseau[15].

II.6.3.5 Attaque de dictionnaire

Pour la première option, le pirate doit parvenir a tromper le mécanisme d'identification, il suffit de trouver le mot de passe valable soit dans un échanges des mots passes en claire sinon si les mots de passes sont cryptés, il doit essayer d'attaquer l'algorithme de cryptage. Une autre technique, consiste à essayer des millions de mots de passe jusqu'à trouver le bon [34]. Il existe deux variantes de l'attaque de dictionnaire :

— **L'attaque en ligne :**L'utilisateur cherche à se connecter au système en essayant successivement chaque mot de passe jusqu'à trouver le bon[34].

— **L'attaque hors ligne :**De nombreux protocoles d'authentification fonctionnent de la façon suivante : le serveur envoie un "défi" (texte aléatoire) à l'utilisateur qui utilise ce " défi " ainsi que son mot de passe pour générer la réponse, selon un algorithme précis. Le serveur utilise le même algorithme pour vérifier la validité de la réponse. L'attaque de dictionnaire hors ligne fonctionne ainsi : Le pirate enregistre le dialogue d'une authentification réussie. Il possède alors le défi et la réponse, correcte, de l'utilisateur. Hors connexion, il essaye des millions de mots de passe avec le même défi et le même algorithme jusqu'à ce qu'il trouve la même réponse que celle donnée par l'utilisateur[34].

II.6.3.6 Détourner une session existante

Il existe des adaptateurs WiFi dont on peut changer l'adresse MAC, ce qui permet à un pirate de facilement détourner des sessions : il lui suffit d'espionner le réseau en attendant l'arrivée d'un utilisateur légitime. Une fois que celui-ci s'est identifié, le pirate regarde son adresse MAC et configure son propre adaptateur WiFi pour imiter cette adresse. On parle de *spoofing* de l'adresse MAC[15].

II.6.3.7 L'espionnage (sniffing)

L'attaque la plus utilisée car cela consiste à écouter les transmissions des différents utilisateurs du réseau sans fil, et de récupérer n'importe qu'elles données transitant sur le réseau. Il s'agit d'une attaque sur la confidentialité. Il suffit pour cela de disposer d'un adaptateur Wi-Fi capable de lire tous les messages et pas uniquement ceux qui lui sont adressés. Puis utiliser un logiciel d'analyse de réseau, comme " wireshark " ou "Kismet" pour "sniffer" tout ce qui se passe sur le réseau. [15].

II.6.4 Les solutions de sécurité de 802.11

Avant de présenter les protocoles de sécurité proposés par le 802.11, il y'a deux règles de protection élémentaires [26] :

— Cacher le nom du réseau, ou SSID, de telle sorte qu'un utilisateur ne voie pas le réseau et ne puisse donc pas s'y connecter. Cette mesure de sécurité n'est hélas que provisoire.

— N'autoriser que les communications contrôlées par une liste d'adresses MAC, ou ACL (Access Control List). Cela permet de ne fournir l'accès qu'aux stations dont l'adresse MAC est spécifiée dans la liste.

Depuis 1990, de nombreux protocoles de sécurité sans fil ont été développés et adoptés. Pour securiser les reseaux wifi, le groupe de travail 802.11 proposé 3 protocoles de sécurité principaux : **WEP**, **WPA** et **WPA2** [16, 6] : WEP (Wireless Equivalent Privacy) a été le premier protocole de chiffrement par défaut, dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations, Cependant, en raison de ses défaillances techniques, un nouveau protocole à été développé WPA (Wi-Fi protected Access). Le WPA2 est un nouveau protocole qui a été développé après WEP et WPA qui n'ont pas réussi à sécuriser la communication sur les réseaux Wi-Fi.WPA2, également connu sous le nom de norme IEEE 802.11i, est une amélioration de la norme 802.11 qui spécifie les mécanismes de sécurité pour les réseaux sans fil.

II.7 Conclusion

Au cours de ce chapitre, nous avons abordé la notion de réseau sans fil, son intérêt, ainsi que la classification selon la distance et l'infrastructure. Ensuite nous avons cité les réseaux Wi-Fi, leur architecture en couches, les différents techniques d'accès au support et la notion de mobilité Roaming. Nous nous sommes également intéressés à la sécurité des réseaux Wi-Fi. Après un rappel de quelques notions de sécurité et les mécanismes de cryptographie, nous avons présenté les attaques qui peuvent toucher les réseaux Wi-Fi. Enfin, nous avons terminé avec les solutions proposées pour la sécurité des réseaux Wi-Fi. Dans le chapitre qui suit, nous allons étudier de manière plus détaillée l'authentification avec 802.1X.

Chapitre III

Authentification dans les réseaux sans-fil WLAN

III.1 Introduction

Une borne Wi-Fi émet dans toutes les directions et aussi loin que porte son signal. Donc, partout dans le volume couvert par une borne, des "espions" peuvent s'installer et intercepter les communications ou s'introduire dans le réseau et l'utiliser à leur profit. Cette situation pose un problème pour les premières installations Wi-Fi à cause de l'absence de méthode d'authentification fiable des postes de travail et de mécanismes de chiffrement fort des communications.
Dans ce chapitre, nous allons voir les différentes solutions d'authentification dans les réseaux WLAN, avec une comparaison entre l'authentification centralisée et décentralisée. Ensuite, nous présentons les principes des protocoles Radius et 802.1X que nous avons jugés nécessaire à connaître car ils sont très répandus dans l'authentification dans les réseaux. :

III.2 L'authentification dans les WLAN :

L'authentification est le processus de vérification de l'identité de l'utilisateur ou bien de la machine lors de l'accès au réseau ; d'autre part, l'authentification permet également d'attribuer un ensemble de droits d'accès selon l'identité de l'utilisateur (autorisation). Il existe différents moyens par lesquels on peut s'authentifier. Les plus répandus sont [9] :

— Authentification avec l'adresse MAC (MAC-based) : la machine s'authentifie selon l'identifiant de la carte réseau (adresse MAC), mais cette adresse n'est

pas une preuve absolue d'identité puisqu'il est relativement facile de la modifier et d'usurper l'identité d'un autre poste de travail. Même si on met en place un chiffrement fort des communications, l'adresse MAC circule toujours en clair. Or, le problème du sans fil est que le périmètre du réseau est flou et incontrôlable. Par conséquent, n'importe qui écoutant ce réseau peut capter des adresses MAC et s'en servir très facilement ensuite pour s'authentifier.

— Authentification par identifiant et mot de passe : correspond à l'authentification des utilisateurs qui possèdent des mots de passe.

— Authentification par certificat électronique : consiste à faire présenter par le client un certificat électronique dont la validité pourra être vérifiée par le serveur.

Les protocoles de sécurité principaux **WEP**, **WPA** , **WPA2** et **WPA3** du protocole 802.11 spécifient les méthodes d'authentification décrites ci-après.

III.2.1 Authentification dans WEP

Le WEP, première solution de sécurité à avoir été intégrée dans le standard 802.11 est un protocole élaborée en 1999 dans le but d'offrir un moyen d'authentification, de confidentialité et de contrôle d'intégrité. Il se base sur un système à clé symétrique, utilisant l'algorithme RC4 (Rivest Cypher 4). La même clé étant utilisée pour chiffrer et déchiffrer les données. Cette clé est partagée par tous les clients du réseau et par le point d'accès[26].

Deux techniques d'authentification sont associées au WEP [26] :

— **Open System Authentication :**qui est le système d'authentification par défaut, l'authentification est explicite. Un terminal peut donc s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS.

— **Shared Key Authentication :** Cette technique, basée sur un secret partagé, se déroule en quatre étapes (voir Figure III.1)

1. La station envoie une requête d'authentification au point d'accès.
2. Lorsque le point d'accès reçoit cette trame, il envoie un texte en clair 128 bits (défi) généré par l'algorithme WEP.
3. La station chiffre cette valeur avec la clé partagée et l'envoyer au point d'accès.
4. Le point d'accès déchiffre le texte reçu avec le même secret partagé et le compare avec celui qui a été envoyé plus tôt. Si le texte est identique, le point d'accès lui confirme son authentification, sinon il envoie une trame d'authentification négative.

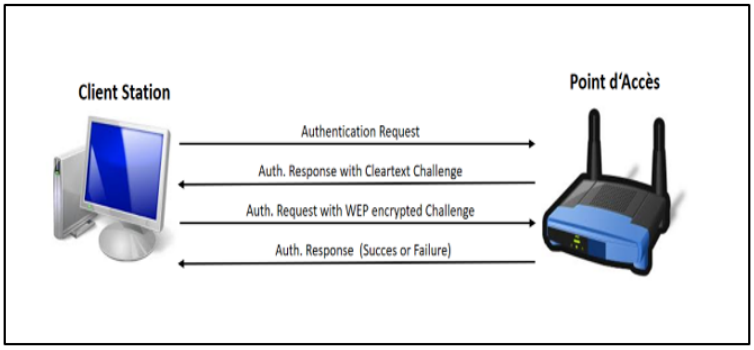


Figure III.1 – Fonctionnement du mécanisme Shared Key Authentication

Cependant, le WEP n'est pas considéré comme une méthode d'authentification sérieuse puisque la seule connaissance de la clé partagée entre tous les utilisateurs et les bornes donnait accès au réseau. Quant au chiffrement, les pirates ont très vite eu raison de l'algorithme utilisé, qui ne résiste pas à une simple écoute du trafic suivie d'une analyse. Des logiciels spécifiques ont été développés, tels que Aircrack ou Airsnort, qui permettent d'automatiser ce type d'attaques. Le groupe de travail IEEE 802.11i propose une solution plus robuste à ces problèmes de sécurité à travers les mécanismes WPA et WPA2 [9].

III.2.2 Authentication dans WPA

Le groupe de travaille IEEE 802.11i propose une solution plus robuste à ces problèmes de sécurité du WEP a été apportée par les mécanismes WPA et WPA2 [9]. Tous les versions WPA sont identiques du point de vue de leur architecture globale et donc de leur mise en oeuvre. Il existe deux architectures [15] :

— **WPA Personal :** également appelé WPA-PreShared Key (WPA-PSK) suppose la configuration d'une clé partagée dans tous les AP et équipements connectés au réseau. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une " passphrase " (phrase secrète), traduite en PSK par un algorithme de hachage.

— **WPA Enterprise :** impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (Remote Authentication Dial-in User Service), et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte.

Dans notre cas nous nous intéressons à la méthode d'authentification avec 802.1X (et EAP) que l'on va détailler dans ce qui suit.

III.2.2.1 variantes versions WPA

Le WPA1 :

Un groupe du travail du 802.11i été mis en place pour développer une solution de sécurité nettement plus sûre que la solution WEP qui souffre en effet de nombreuses failles qui le rendent peu recommandable ; mais la découverte des failles du WEP et la finalisation de la norme 802.11i, il s'est écoulé plusieurs années

Le WPA2 :

En 2002 une solution de sécurité appelée Wireless Protected Access (WPA) a été développée, qui est un sous-ensemble du 802.11i, en juin 2004. La WiFi Alliance a alors créé la certification WPA2 pour les produits respectant la norme 802.11i au complet. Le WPA repose sur un algorithme de cryptage défini par le protocole Temporal Key Integrity Protocol (TKIP), lui-même basé sur l'algorithme RC4, alors que le WPA2 repose, au choix, sur le TKIP ou sur un autre algorithme de cryptage appelé Advanced Encryption Standard (AES). Une autre différence importante est que le WPA n'est pas compatible qu'avec les réseaux de type infrastructure et non les réseaux Ad Hoc, quand au WPA2, il peut sécuriser les deux types de réseau [15].

Le WPA3 :

après les améliorations ajoutées fin 2017, la troisième version WPA est finalement lancée, des fonctionnalités ont été apportées pour permettre une authentification plus robuste et fournir une force cryptographie accrue pour les données sensibles de 192 bits (entreprise) ainsi le "cryptage des données individualisé ", cryptant votre connexion à un point d'accès quel que soit le mot de passe, WPA3 offre meilleur solution pour la sécurisation des appareils internet des objets Iot.

III.3 Authentification centralisé et décentralisé

III.3.1 Authentification décentralisée

Une authentification décentralisée est la méthode la plus ancienne où l'authentification des clients se fait au niveau des points d'accès. Chaque AP authentifie les clients qui appartiennent à son BSA. En plus authentification décentralise souffre du problème du Roaming, elle exige les clients a chaque déplacement vers une autre cellule d'initialiser le processus de l'authentification à nouveau.

III.3.2 Authentification centralisée

C'est la technique la plus utilisée dans les WLAN ; elle repose sur le standard 802.1x et dédie un serveur d'authentification qui peut être un serveur RADIUS, TACACS, ... Un système central de gestion des identités pour l'accès à toutes les applications et services du LAN permet de partager une base commune. Le principe est de disposer d'une base de données globale pour centraliser toutes les demandes d'authentification des utilisateurs. Elle unifie la gestion des authentifications et des autorisations. Cela permet également de centraliser la gestion de la politique de sécurité.

III.4 Services d'authentification applicatif

III.4.1 Le protocole RADIUS

RADIUS ou Remote Authentication Dial-In User est une norme de l'IETF (Internet Engineering TASK Force). C'est un protocole d'authentification standard Client/Serveur qui permet de centraliser les données d'authentification : les politiques d'autorisations, de droits d'accès, et de traçabilité. A l'origine, ce protocole a été créé pour permettre aux fournisseurs d'accès à internet (FAI) d'authentifier les utilisateurs distants. Au fil du temps, il a été enrichi et on peut envisager aujourd'hui de l'utiliser pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil .[9]

Le RADIUS est un protocole qui répond au modèle AAA qui permet de centraliser les trois fonctions suivantes : [9]

- **Authentication(Authentification) :**authentifier l'identité du client,
- **Authorization (Autorisation) :**accorder des droits du client,
- **Accounting (Compatibilité) :**c'est " journaliser " les accès, les temps de session, les ressources consommées, etc. afin de garantir la traçabilité des informations.

RADIUS utilise une architecture client / serveur qui repose sur le protocole UDP [26, 15] :

- **Les client RADIUS :**nommés NAS (Network Access Server), sont des intermédiaires entre l'utilisateur final et le serveur et sont responsables du transfert des informations envoyées par l'utilisateur vers les serveurs RADIUS.
- **Le serveur RADIUS :** il est connecté à une base d'identification (annuaire LDAP, base de données MySQL, ...) et prend en charge la réception des de-

mandes d'authentification, l'authentification des utilisateurs et les réponses contenant toutes les informations de configuration nécessaires aux NAS.

III.4.1.1 Format général des paquets RADIUS :

Le protocole établit une couche applicative au-dessus de la couche de transport UDP. À l'origine, les ports utilisés étaient 1645 et 1646. Comme ces ports étaient en conflit avec d'autres services IP, ils ont ensuite été remplacés par : [9]

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

Tous les paquets ont le format général indiqué par la figure III.2 :

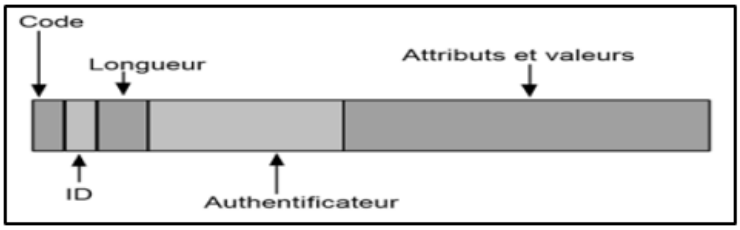


Figure III.2 – Format du paquet RADIUS.

— **Code :** Ce champ identifie le type de paquet, RADIUS utilise quatre types de paquets pour assurer les transactions d'authentification.

1. Access-Request (code = 1) : La conversation commence toujours par un paquet Access-Request émis par le NAS vers le serveur , contenant les informations sur l'utilisateur (login/mot de passe,....)
2. Access-Accept : (code =2) : envoyé par le serveur si l'authentification est succès.
3. Acces-Reject : (code =3) : envoyé par le serveur si l'authentification a échouée.
4. Access-Challenge : (code =11) : envoyé par le serveur pour demander des informations complémentaires, et donc la réémission d'un paquet Access-Request.

— **ID :** Ce champ permet au client RADIUS d'associer les requêtes et les réponses,

— Longueur : Ce champ contient la longueur totale du paquet

— **Authentificateur :**Ce champ a pour but de vérifier l'intégrité du paquet. Il permet de vérifier que la requête n'a pas été modifiée pendant la transmission.

— **Attributs et valeurs :** Ce champ contient les attributs qui sont envoyés soit par le NAS soit par le serveur.

III.4.1.2 Les attributs RADIUS

LLe format de chaque attribut est très simple. Chaque attribut précise les trois éléments suivants (voir Figure III.3) [14, 15, 9] :

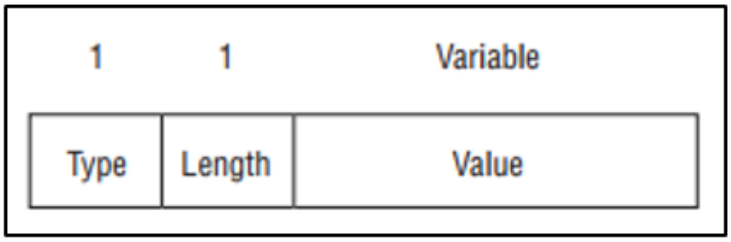


Figure III.3 – Le champ Attributs et valeur d'un paquet RADIUS [14]

1. **le type :** Il existe un grand nombre d'attributs dans le protocole Radius mais peu d'entre eux sont utiles pour l 'authentification sur réseau local. Le nom de l'attribut n'est jamais présent dans les paquets. Seul son numéro apparaît la correspondance entre un numéro d'attribut et son nom sera faite grâce à un dictionnaire. On trouve par exemple les attributs suivants :

N° d'attribut	NOM d'attribut
1	User-Name,
2	User-Password
4	Nas-IP-Address
5	Nas-port

Tableau III.1 – les différents attributs du protocole RADIUS [14]

   Le nom de l'attribut n'est jamais présent dans les paquets. Seul son numéro apparaît la correspondance entre un numéro d'attribut et son nom sera faite grâce à un dictionnaire.
2. **la longueur :** est celle de l'ensemble de l'attribut, pas uniquement de la valeur ;
3. **La valeur d'un attribut :** peut correspondre à l'un valeurs suivantes :
   - adresse IP (4 octets) ;
   - date (4 octets) ;

- chaîne de caractères (jusqu'à 255 octets) ;
- entier (4 octets) ;
- valeur binaire (1 bit) ;
- valeur parmi une liste de valeurs (4 octets).

Dans la terminologie Radius, ces attributs et leur valeur sont appelés Attributes Value-Pair (AVP). Le champ Attributs et valeurs peut contenir plusieurs couples attribut-valeur comme le montre la Figure III.4 :

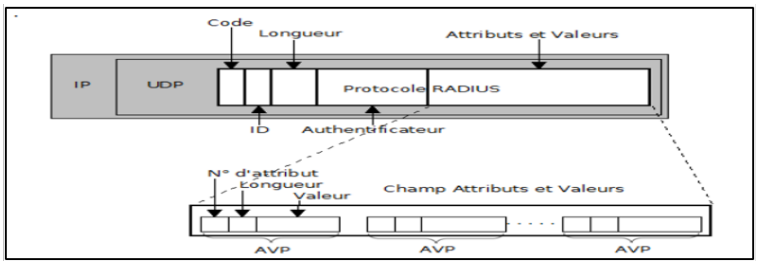


Figure III.4 – Format du champ Attributs et Valeurs

On distingue deux sortes d'authentifications RADIUS [9] :

1. **L'authentification RADIUS-MAC :** Elle est basée sur l'adresse MAC du poste de travail. Le serveur vérifie si l'adresse MAC est présente dans sa base, selon le résultat il donne ou refuse l'accès au réseau contrôlé. Dans ce type d'authentification, il n'y a pas de communication entre le poste de travail et le serveur Radius.Cette solution est plus simple à mettre en oeuvre mais est également la moins sûre.
2. **L'authentification 802.1X :** Cette solution est basée sur le protocole 802.1x et sera détaillée dans ce qui suit.

III.4.2 Le protocole TACACS+

Comme RADIUS, TACACS+ permet de centraliser l'authentification et les autorisations d'accès dans un réseau. TACACS+ est un protocole propriétaire Cisco qui a remplacé TCACS et X TACACS (mais actuellement c'est un standard ouvert défini dans le RFC 1492) utilisé pour la communication du client Cisco et du serveur Cisco ACS (Access Control Server). L'architecture sous-jacente du protocole TACACS+ est un complément à l'architecture AAA. Ce protocole a été conçu pour mesurer la croissance des réseaux et s'adapter aux nouvelles technologies de sécurité au fur et à mesure que le marché s'agrandit. La particularité de TACACS+ par

rapport aux serveurs d'authentification traditionnelle est ça séparation Protocolaire des trois fonctions AAA [1].

III.4.3 Différence entre le protocole RADUIS et TACACS+

La différence entre le protocole RADUIS et TACACS+ réside dans les points suivants [1] :

	RADIUS	TACACS+
Protocole	Utilise UDP	Utilise TCP
Ports	Utilise les ports UDP : 1812 et 1813	Utilise le ports TCP : 49
Chiffrement	crypte les mots de passe uniquement et le reste est envoyé dans un contexte clair	crypte toute la communication
Authentification et autorisation	RADIUS combine l'authentification et l'autorisation	séparer l'authentification, l'autorisation et traçabilité
Prise en charge multi-protocole	Ne prend pas en charge multi-protocoles	Prend en charge de ces protocoles : Appletalk Remote Access (ARA), NetBIOS Frame, Protocol Control, (NASI), Connexion X.25 PAD
Utilisation	Principalement utilisé pour l'accès au réseau	Principalement utilisé pour l'administration des périphériques

Tableau III.2 – Comparaison entre RADUIS et TACACS+

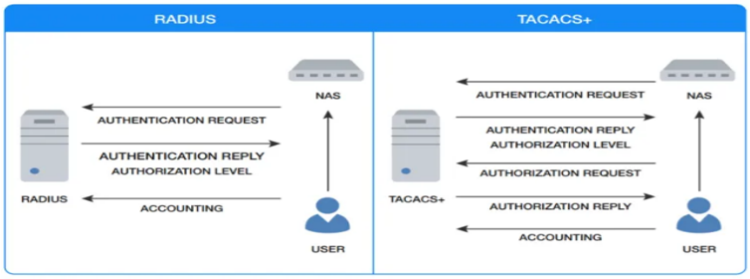


Figure III.5 – Authentification et autorisation RADIUS et TACACS+

III.5 Le Protocole 802.1x

802.1X est un protocole de contrôle d'accès au réseau " Port-Based Network Access Control " ou " Accès au réseau basé sur le contrôle de port " initialement proposé par l'IEEE pour sécuriser l'accès aux réseaux filaires de type Ethernet. Il est également utilisé pour sécuriser l'accès aux réseaux de type sans fils [3]. Le protocole 802.1x effectue une authentification de l'équipement client au moment de la

1. https ://www.cisco.com/c/fr_ca/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html. consulter le 21/04/2020

connexion physique au réseau local [28]. La phase d'authentification sera assurée au travers du protocole EAP [13], le protocole 802.1x ne fournissant qu'un cadre fonctionnel à l'interaction entre les équipements. Donc l'objectif de ce standard est d'autoriser l'accès physique au réseau local, indépendamment du support de transmission utilisé, et en s'appuyant sur des mécanismes d'authentification existants[30].

III.5.1 Principe général du protocole 802.1x

Le protocole 802.1x est composé de trois entités (voir Figure III.6) qui interagissent pour le processus d'authentification : [29, 10, 21] :

1. **Le système à authentifier(Supplicant) :**c'est le client qui demande l'accès au réseau.
2. **Le système authentificateur (Authenticator) :** c'est un équipement réseau (commutateur, routeur, point d'accés ...) qui agit comme une barrière de sécurité entre le supplicant et le réseau protégé. Il sert de relais entre le supplicant et le serveur d'authentification et gère le PAE (Port Access Entity) qui permet au Supplicant d'accéder ou non au résau.
3. **Le serveur d'authentification(Authentication Server) :** c'est le serveur fournissant l'autorisation d'accès. il s'agit généralement d'un serveur RADIUS, ou tout autre équipement capable de faire de l'authentification tel que : TACACS+ ou encore DIAMETER.

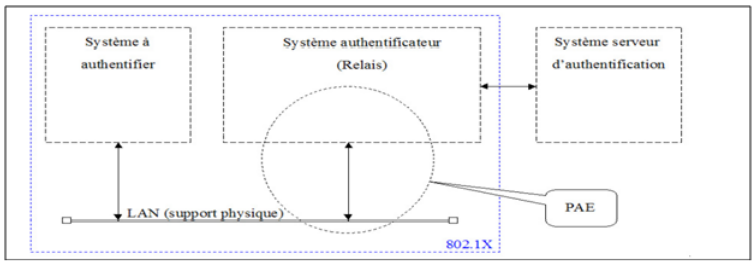


Figure III.6 – les trois entités qui interagissent dans 802.1X

point d'accès au réseau (PAE) : Le système authentificateur contrôle une ressource disponible via PAE qu'il s'agit un point d'accès physique au réseau géré par le système authentificateur et sur lequel va être réalisée l'authentification. La principale innovation du protocole 802.1x réside dans ce concept : le port physique est scindé en deux ports logiques : [29] :

— **port appelé "non contrôlé " :**qui gère toutes les trames spécifiques au protocole 802.1x et qui est toujours accessible

— **Un port appelé "contrôlé" :**qui peut prendre deux états " ouvert " ou "fermé" et son état est commandé par le serveur d'authentification après authentification et autorisation d'un supplicant. Ainsi avant l'authentification du supplicant, seul le mode non contrôlé est possible, permettant les échanges d'information d'authentification. Ces flux sont appelés flux EAPOL (EAP Over Lan).

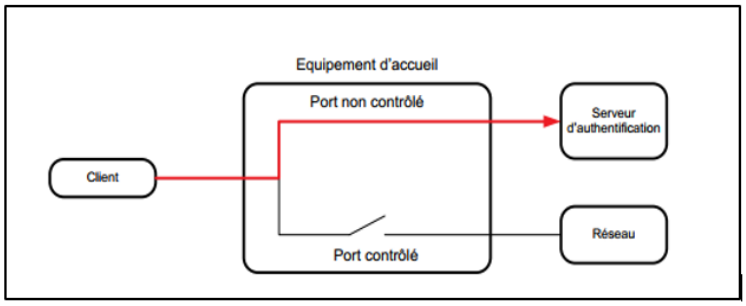


Figure III.7 – État du PAE avant la phase d'authentification

Par défaut l'état du port contrôlé est "ouvert" une fois que l'authentification est réussie, son état est basculé de l'état ouvert à l'état fermé et les flux autorisés peuvent être émis à destination du réseau.

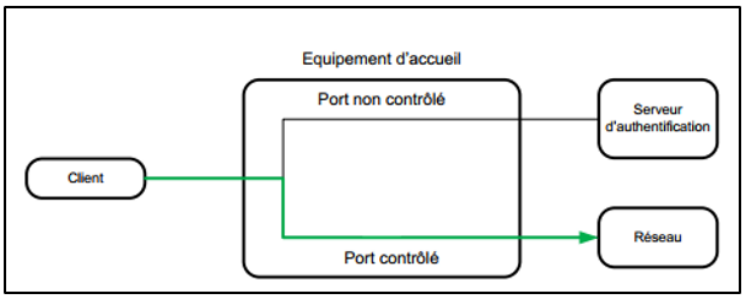


Figure III.8 – État du PAE après une authentification réussie

La norme 802.1x ne prévoie pas le support physique du port. Ainsi il est possible que le port soit un connecteur RJ45 Ethernet, une fibre optique ou un point d'accès sans fil.La figure III.9 décrit le PAE :

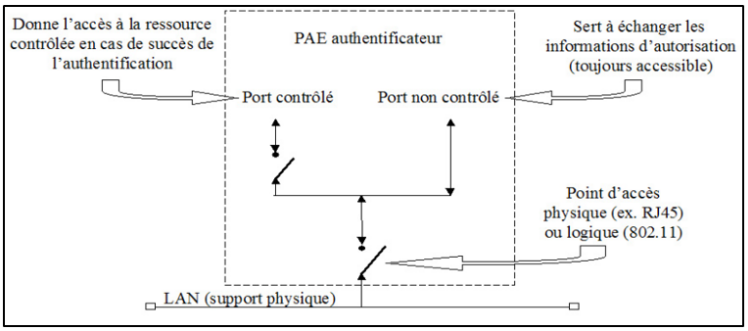


Figure III.9 – Le PAE [29]

III.5.2 Fonctionnement du protocole 802.1x

Le standard 802.1X ne crée pas un nouveau protocole d'authentification, mais s'appuie sur les standards existants. 802.1x définit plusieurs techniques d'encapsulation utilisées dans le but de transporter les paquets d'authentification et de gestion du protocole EAP. Cette technique est connue sous le nom EAPOL (EAP over LAN) entre le client et le point d'accès et sous le nom " EAP over RADIUS " entre le point d'accès et le serveur d'authentification RADIUS. Le serveur d'authentification effectue les actions nécessaires sur le port contrôlé (blocage ou déblocage), selon les informations d'authentification transportées dans les paquets EAPOL. Ainsi, le système authentificateur se comporte comme un mandataire entre le système à authentifier et le serveur d'authentification. Si l'authentification réussit, le système authentificateur donne l'accès à la ressource qu'il contrôle (voir Figure III.10)[29]

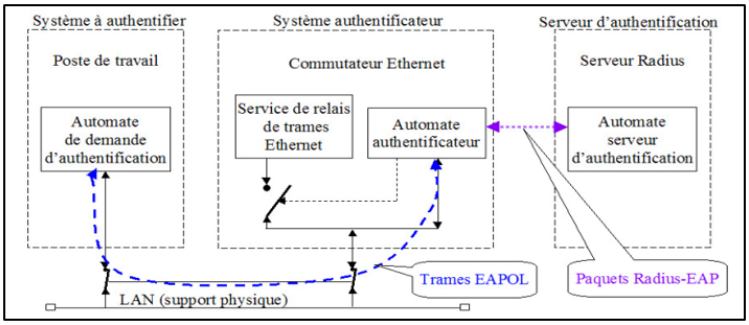


Figure III.10 – Les différents protocoles composant le 802.1x [29]

III.5.3 Extensible Authentication Protocol (EAP)

Le protocole EAP est le protocole qui assure le transport des informations d'authentification. Il est défini dans la RFC 3748 [1] et a été initialement développé pour être utilisé avec PPP (Point to Point Protocol). Mais aujourd'hui, EAP est le plus

souvent utilisé dans les réseaux locaux sans fil. EAP est un protocole d'authentification général qui supporte de multiples méthodes d'authentification définies dans la RFC 3748 [1]., telles que TLS, MD5, TTLS (voir Figure III.11). Avec un EAP standardisé, l'interopérabilité et la compatibilité entre les méthodes d'authentification deviennent plus simple[32].

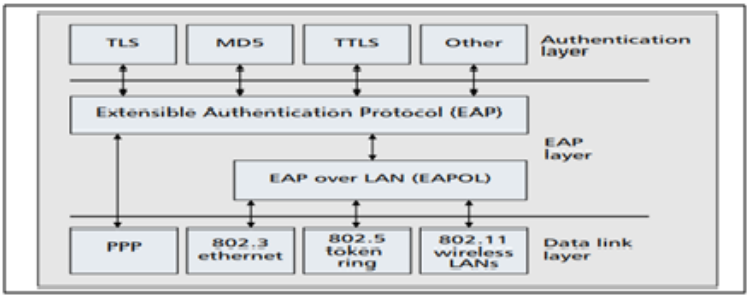


Figure III.11 – EAP et couches associées [10]

III.5.3.1 Format des trames EAP

Comme illustré à la figure III.12,une trame EAP contient cinq champs [26] :

— **Code :** ce champ indique le type de paquet. Il existe quatre types de paquets utilisés par le protocole EAP permettent de réaliser l'authentification d'un suplicant sur un serveur :

- EAP REQUEST (code = 1) : demande d'authentification ;
- EAP RESPONSE (code = 2) : réponse à une requête d'authentification ;
- EAP SUCCESS (code = 3) : pour indiquer le succès de l'authentification ;
- EAP FAILURE (code = 4) : pour informer le client du résultat négatif de l'authentification.

— **Identifier :** ce champ indique à quelle requête correspond une réponse,

— **Length :** ce champ indique la longueur du paquet EAP,

— **Type :** indique quel type de méthode d'authentification est utilisée.

— **Data :** contient, en fonction du champ " Type ", les données transportées par la trame.

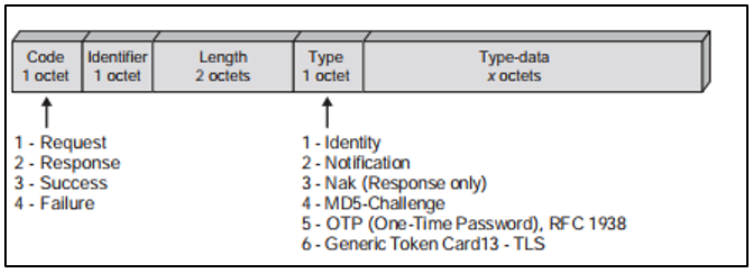


Figure III.12 – Format d'un paquet EAP [26]

III.5.3.2 Les couches EAP

EAP est un protocole qui place trois couches au-dessus de la couche liaison IEEE 802 (voir Figure III.13)[9] :

- **La couche EAP :** sert d'intermédiaire entre la couche de liaison de données et la couche EAP peer. Elle reçoit et envoie les paquets vers la couche basse (802) et transmet les paquets de type Request, Success et Failure à la couche EAP Peer. Les paquets Response sont transmis à la couche EAP Authenticator.
- **Les couches EAP Peer et EAP Authenticator :** la couche EAP Peer est implémentée sur le Supplicant tandis que la couche EAP Authenticator est implémentée sur l'Authentificateur et le serveur d'authentification. Ces couches ont pour rôle d'interpréter le type de paquet Request ou Response et de les diriger vers la couche EAP-Method correspondant à la méthode d'authentification utilisée.
- **La couche EAP Method :** elle traite la donnée encapsulée dans un paquet EAP qui correspond à l'information d'authentification échangée entre le Supplicant et le serveur d'authentification. La nature de la donnée d'authentification qui peut être transportée par un paquet particulier est dépendante du type EAP.

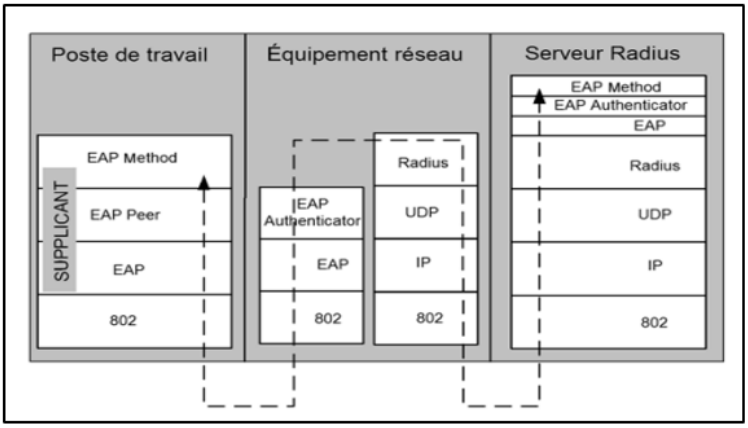


Figure III.13 – Les couches EAP [9]

III.5.4 Le Procédure d'authentification 802.1x

La première étape est bien sûr l'association physique (ex. RJ45) ou logique (802.11) avec le port physique du PAE du système authentificateur ; le port contrôlé de ce dernier est bloqué et seul le port non contrôlé est accessible. Cette étape doit être réalisée préalablement à la phase d'authentification 802.1X. La procédure d'authentification est la suivante (voir Figure III.14) :

1. L'authentificateur envoie un message "EAP-Request / Identity" au supplicant lorsqu'il détecte que la liaison est active.
2. Le Supplicant envoie un paquet " EAP-Response / Identity " avec son identité à l'authentificateur et les méthodes d'authentification supportées.
3. A ce moment l'authentificateur transmet au serveur d'authentification le message EAP Response/Identity encapsulé dans une requête RADIUS. Durant l'échange des messages EAP (requêtes et réponses) entre le serveur d'authentification et la station mobile, l'authentificateur agit comme un simple relais passif.
4. Le serveur d'authentification prend la décision d'accepter ou de refuser l'accès au réseau et il indique le succès ou l'échec de la procédure d'authentification via le message EAP-Success ou EAP-Failure. Si le serveur d'authentification accepte le client, alors l'état du port change. Il passe à l'état autorisé, sinon, le port reste dans l'état non autorisé [29, 30, 7].

À la fin de la connexion (déconnexion logicielle), le supplicant envoie un message EAP-Logoff ou changement de statut du lien physique, l'authentificateur modifie alors l'état du port à non autorisé. 802.1X définit également un temporisateur de réauthentification, qui peut être utilisé pour obliger le supplicant à se ré-authentifier

périodiquement [2]

. **Remarque :** Si la phase d'authentification s'est bien déroulée, le serveur d'authentification peut transmettre une clé de chiffrement au client, lequel l'utilise pour chiffrer les données émises. Cette dernière phase est optionnelle pour le protocole EAP car elle dépend du protocole d'authentification utilisé [26].

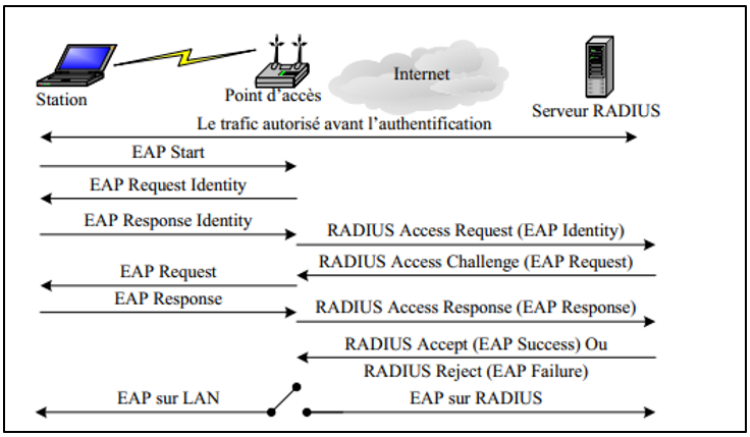


Figure III.14 – Procédure standard d'authentification 802.1x [7]

III.6 Les méthodes d'authentification EAP

Le protocole 802.1X ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés plusieurs types d'authentification. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client : login / mot de passe ; certificat électronique ; biométrie ; puce (SIM). Certaines méthodes combinent plusieurs critères (certificats et login/mot de passe, etc.) En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement (WEP) [30]. Une méthode EAP correspond à la façon dont une authentification est conduite. C'est une méthode particulière utilisée pour réaliser une authentification en utilisant EAP comme mécanisme de transport. Il existe plusieurs méthodes d'authentification possédant différents niveaux de sécurité. Les méthodes d'authentification les plus fréquemment utilisées sont décrites ci-après.

III.6.1 EAP-MD5 (Message Digest 5)

Cette méthode est définie dans la RFC 3748[1] ,MD5 ne propose pas d'authentification mutuelle, le client s'authentifie simplement par un couple login / mot de

2. https ://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html#wp386822. consulter le 21/04/2020

passe. Le processus de l'authentification EAP-MD5 est défini comme suit (voir Figure III.15) :

1. l'association physique au point d'accès et la phase EAP standard de demande d'identification,
2. le serveur initie le processus d'authentification EAP-MD5 par requête EAP-MD5 sous forme d'un texte de défi ou challenge.
3. Le client chiffrer le défi avec son mot de passe en utilisant l'algorithme de hachage MD5, L'empreinte obtenue est renvoyée au serveur.
4. Le serveur chiffre le défi de son côté en utilisant le mot de passe du client stocké dans sa base. Ensuite il compare l'empreinte calculée avec l'empreinte reçue. Si les deux empreintes sont identiques alors l'authentification du client est acceptée sinon, l'authentification du client est refusée.

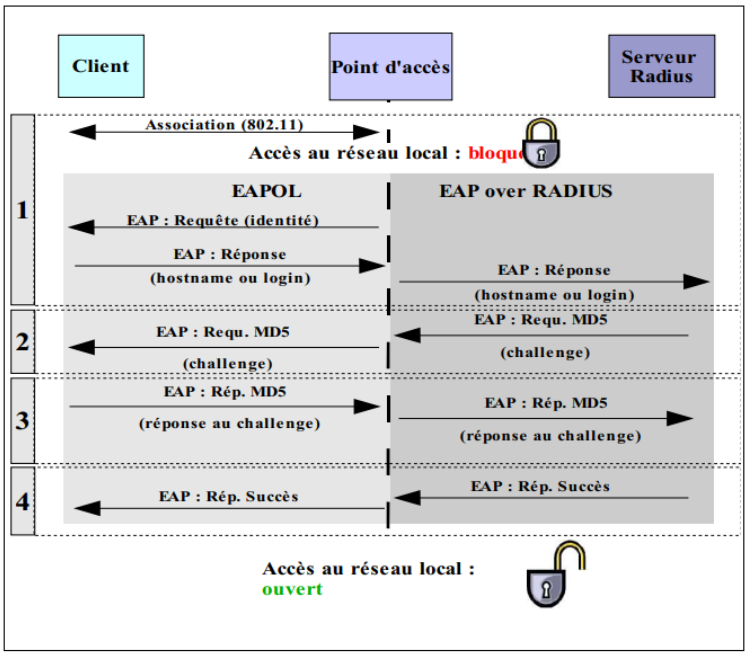


Figure III.15 – Diagramme d'échanges EAP-MD5 [30]

Les Avantages :

— la simplicité : Cette méthode est très facile à mettre en place.

Les Inconvénients :

— Cette méthode est vulnérable aux attaques par dictionnaire, Man In the Middle, session hijacking.

— Elle ne permet pas d'authentifier le serveur (ne propose pas d'authentification mutuelle)

— Les échanges ne sont pas chiffrés et cette méthode ne gère pas la distribution dynamique des clés WEP.

Cette méthode est beaucoup utilisée pour des réseaux filaires où la contrainte liée au chiffrage des échanges est moins forte que pour les réseaux Wi-Fi. Des améliorations permettent de chiffrer les échanges entre le client et le serveur (utilisation de tunnel chiffré), mais le fait que EAP-MD5 n'offre pas la possibilité de générer dynamiquement des clés WEP le rend inutilisable pour les réseaux sans fil[14, 30, 3].

III.6.2 EAP-TLS (Transport Layer Security)

EAP-TLS défini par la RFC 2716 d'octobre 1999, est un protocole d'authentification mutuelle par certificat du supplicant et du serveur. Chacun doit donc posséder un certificat qu'il envoie à l'autre qui l'authentifie. Ces certificats sont délivrés par une autorité de certification (Certificate Authority) commune. Cela impose donc que EAP-TLS nécessite une Infrastructure à Gestion de Clé (IGC) ou Public Key Infrastructure (PKI) [14, 3, 15].
Donc cette méthode dispose de trois fonctions :

— L'authentification du serveur,

— L'authentification du client,

— Le chiffrement.

Le processus général d'authentification EAP-TLS est défini comme suit (voir Figure III.16) : [30] :

1. Le supplicant(le client) s'associe physiquement au point d'accès.
2. La phase EAP standard de demande d'identification
3. Le serveur d'authentification initie le processus d'authentification TLS par EAPTLS/START.
4. Le supplicant répond avec un message client_hello, qui contient : la version TLS du client, un nombre aléatoire (défi ou challenge) , un identifiant de session et une liste d'algorithmes de chiffrement supportés par le client.
5. Le serveur renvoie une requête contenant un message server_hello suivi de :
   — son certificat (x509) et de sa clé publique ;
   — la demande du certificat du client ;
   — un nombre aléatoire (défi ou challenge) ;
   — un identifiant de session (en fonction de celui proposé par le client).

Le serveur choisit un algorithme de chiffrement parmi ceux qui lui ont été proposés par le supplicant.

6. Le supplicant vérifie le certificat du serveur et répond avec son propre certificat et sa clé publique.
7. Le serveur et le supplicant, chacun de son côté, définissent une clé de chiffrement principale (Master key) utilisée pour la session. Cette clé est dérivée des valeurs aléatoires que se sont échangées le supplicant et le serveur. Les messages change_cipher_spec indiquent la prise en compte du changement de clé. Le message TLS_finished termine la phase d'authentification TLS (TLS handshake), dans le cas d'EAP-TLS la clé de session ne sert pas à chiffrer les échanges suivants.
8. une fois la vérification de l'identité du serveur se fait par le supplicant (avec le certificat et la clé publique), il renvoie une réponse EAP sans donnée. Le serveur retourne une réponse EAP success.
9. La clé de session générée en (8) est réutilisée par L'authentificateur pour créer une clé WEP qui est transmise au client,dans le cas où il s'agit d'une station Wifi. cette clé est valide jusqu' à ce que le client se déconnecte ou que son authentification expire, auquel cas il doit s'identifier à nouveau.

Le tunnel TLS créé lors de la création de la clé de session n'est pas exploité. Seul le TLS Handshake est utilisé, il permet l'authentification mutuelle des deux parties.

Les avantages :

- EAP-TLS est l'une des techniques d'authentification plus solides grâce à l'authentification mutuelle par certificat.
- EAP-TLS est idéal pour les entreprises qui ont déjà des certificats numériques déployés et qui utilisent des suppliants basés sur Microsoft Windows.

Les inconvénients :

- chaque utilisateur doit posséder un certificat électronique : la gestion de ces certificats peut être assez lourde et poser des problèmes de sécurité.
- requise d'une infrastructure de gestion de clés (IGC).

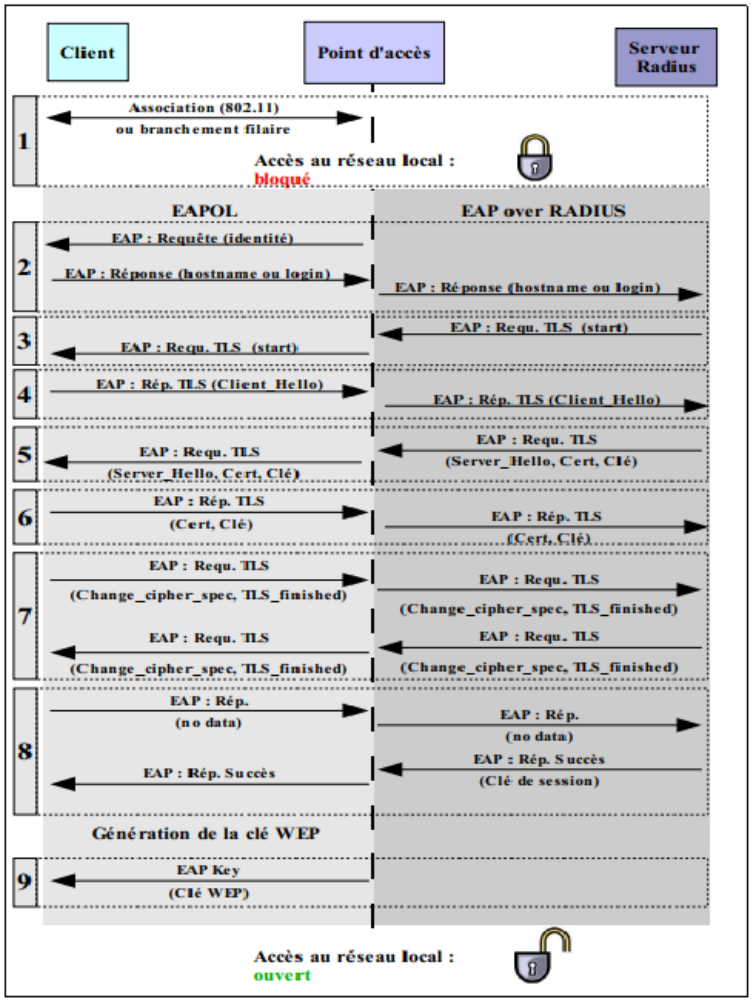


Figure III.16 – Diagramme d'échanges EAP-TLS [30]

III.6.3 EAP-TTLS (Tunneled Transport Layer Security)

Cette méthode a été développé par les sociétés Funk Software et Certicom comme une extension d'EAP-TLS. Similair à EAP-TLS,EAP-TTLS est un protocole d'authentification mutuelle par certificat. Cependant, EAP-TTLS ne nécessite que des certificats côté serveur tant quant le supplicant s'authentifier via l'utilisation d'un couple login/mot de passe. Cela se fait en connectant le supplicant au serveur d'authentification à travers un tunnel crypté via TLS. On distingue deux phases d'authentification :

— **Première phase :** identification du serveur par le client en utilisant un certificat (validé par une autorité de certification)

— **Deuxième phase :** identification du client par le serveur par login/password

Durant la première phase, le supplicant authentifie le serveur au moyen d'un certificat afin de créer un tunnel TLS garantissant une grande confidentialité des

échanges entre les deux parties. L'authentification du supplicant s'effectue durant la seconde phase, à l'intérieur du tunnel TLS précédemment créé et à l'aide d'une méthode d'authentification interne (inner method). Cette méthode peut être une méthode EAP (EAP-MD5 par exemple) ou non EAP comme MSCHAPv2. Dans la majorité des déploiements, les méthodes internes utilisées sont PAP, CHAP, EAP-MD5, EAP-MSCHAPv2 ou MSCHAPv2.
EAP-TTLS utilisent des AVP (Attribute-Values Pairs) encapsulées dans des paquets EAP-TTLS comme une manière d'encapsuler les échanges lors de la deuxième phase, le format AVP d'EAP-TTLS est compatible avec le format AVP de Radius, ce qui simplifie les échanges entre le serveur EAP-TTLS et le serveur Radius qui contient les informations relatives aux utilisateurs, dans le cas où les informations ne sont pas directement stockées sur le serveur EAP-TTLS. [26, 30, 9, 14].

Le processus général d'authentification EAP-TTLS est définit comme suit (Les explications se réfèrent aux étapes numérotées dans la figure III.17) [30] :

(1) à (5) Les échanges sont presque similaires à EAP-TLS. Le client authentifie le serveur par certificat (étape (5)).

(6) Cette étape est déférente d'EAP-TLS, la clé qui sert à chiffrer la session créée directement(le client n'a pas besoin de fournir de certificat). À la fin de cette étape, le TLS handshake est terminé, les échanges suivants seront donc chiffrés par la clé de session.

(7) En effet, l'établissement d'un tunnel TLS permet de chiffrer les échanges, le client fournit donc ses identifiants (login/mot de passe) au serveur en utilisant par exemple MS-CHAPv2.

(8) et (9) Similaires à EAP-TLS.

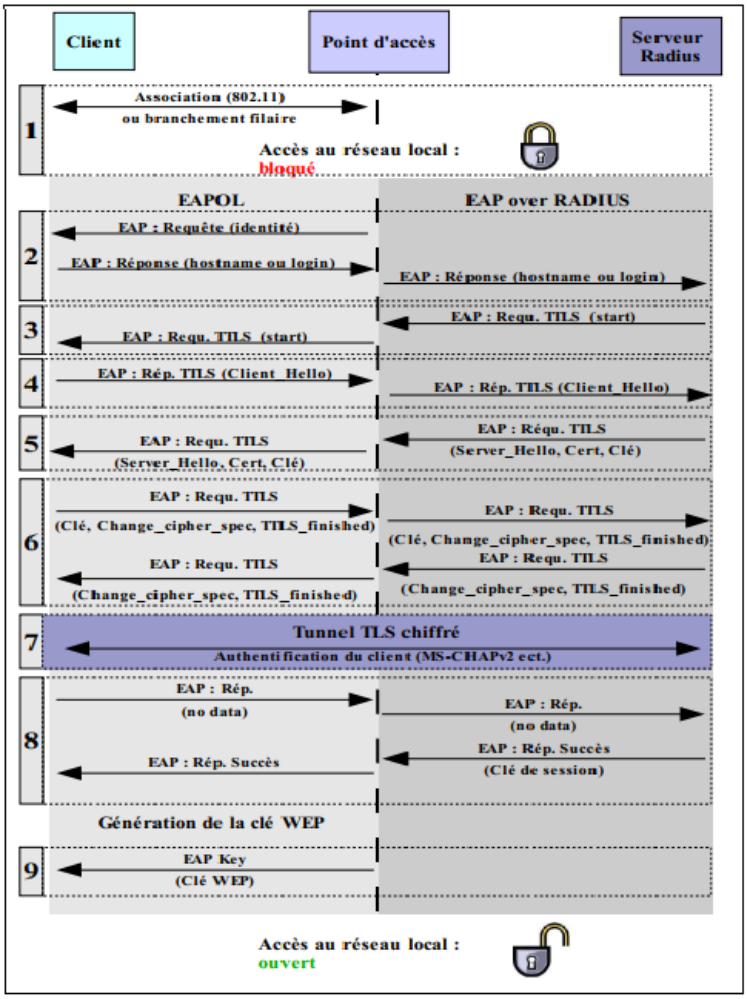


Figure III.17 – Diagramme d'échanges EAP-TTLS [30]

Les avantages :

— L'identité du supplicant est masquée durant la phase d'authentification

— Il requiert uniquement un certificat serveur, l'utilisation de certificats clients n'est pas obligatoire (réduit la complexité de gestion liée aux certificats).

— S'adressent principalement aux sites ne disposant pas d'IGC

— EAP-TTLS permet une meilleure interopérabilité avec les serveurs Radius.

Les inconvénients :

— EAP-TTLS n'est pas intégré nativement au système d'exploitation Windows.

— Méthode d'authentification par mot de passe vulnérable aux attaques par dictionnaires.

III.6.4 EAP-PEAP (Protected EAP)

PEAP est un protocole qui a été développé par Microsoft, Cisco et RSA security pour pallier le principal problème d'EAP/TLS, à savoir la nécessité de distribuer des certificats à tous les utilisateurs ou machines [9]. EAP-PEAP similaire à EAP-TTLS sauf que La différence principale entre EAP-PEAP et EAP-TTLS vient de la manière d'encapsuler les échanges lors de la deuxième phase (identification du client par le serveur par login/password). Pour EAP-PEAP, les données échangées entre le client et le serveur au travers du tunnel TLS sont encapsulées dans des paquets EAP. EAP-TTLS utilisent des AVP encapsulées dans des paquets EAP-TTLS. La méthode EAP-PEAP ne peut-être utilisée qu'avec un serveur Radius supportant EAP (Figure III.18). EAP-TTLS est plus souple, il est toujours nécessaire de dialoguer avec un serveur EAP, cependant ce serveur peut retransmettre directement la requête auprès d'un serveur Radius ne gérant pas EAP (FigureIII.19)[30].

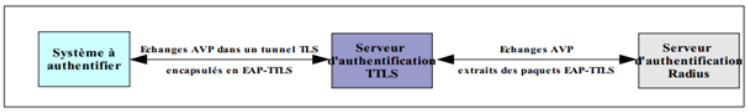


Figure III.18 – Echanges EAP-TTLS [30]

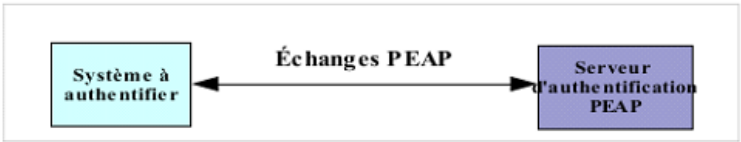


Figure III.19 – Echanges EAP-PEAP [30]

Les Avantages :

- Le supplicant peut être authentifié par mot de passe : c'est une simplification de gestion par rapport à EAP-TLS, tout en proposant une authentification mutuelle sécurisée.
- l'identité du supplicant est cachée. Avec PEAP, un espion peut savoir que quelqu'un cherche à se connecter, mais il ne peut pas savoir qui.
- PEAP est proposé nativement dans les versions Windows , ce qui peut grandement faciliter son déploiement.
- S'adressent principalement aux sites ne disposant pas d'IGC.

Les Inconvénients :

- Cisco et Microsoft ont distribué des versions différentes de PEAP, il faut donc s'assurer que la méthode d'authentification est compatible.

— La méthode EAP-PEAP ne peut-être utilisée qu'avec un serveur Radius supportant EAP.

— L'utilisation d'une méthode d'authentification par mot de passe rend vulnérable aux attaques par dictionnaire en ligne.

III.6.5 LEAP (Lightweight Extensible Authentication Protocol)

Ce protocole a été développé par Cisco pour les réseaux sans fil. Il fournit des clés WEP dynamiques par session et par utilisateur à chaque fois qu'un utilisateur s'authentifie et repose sur une authentification mutuelle via un couple identifiant/ mot de passe. Ce protocole est dérivé de MS-CHAP de Microsoft.

LEAP est basé sur le paradigme défi / réponse. Avec cette méthode, le serveur d'authentification envoie un défi d'authentification au client. Ce dernier utilise un hachage unidirectionnel du mot de passe fourni par l'utilisateur pour créer une réponse au serveur RADIUS. La réponse du client est décryptée et comparée avec le défi envoyé par le serveur. S'il y a correspondance, l'accès est accordé, sinon le l'accès est refusé. En conséquence, un message de réussite / échec EAP est envoyé au client et au serveur RADIUS et le client dérive la clé WEP Dynamique [30, 26, 3].

Les Avantages :

— Solution simple à mettre en oeuvre avec des équipements Cisco ou compatibles

Les Inconvénients :

— Les échanges EAP ne sont pas chiffrés, le login passe en clair, seul le mot de passe est protégé par le hachage MS-CHAPv1

— Méthode d'authentification propriétaire (Cisco).

— Vulnérable aux attaques par dictionnaire.

III.6.6 FAST (Flexible Authentication via Secure Tunneling)

Il s'agit également d'une méthode propriétaire Cisco pour résoudre les faiblesses et les vulnérabilités de son protocole propriétaire LEAP. FAST est une méthode d'authentification mutuelle très similaire à TTLS, mais la différence entre les deux c'est que : [15] :

— TTLS nécessite un certificat numérique coté serveur alors que l'utilisation du certificat du serveur est facultative dans EAP-FAST.

— Dans EAP-FAST le tunnel créé pour protéger l'authentification est établi avec un algorithme de cryptage symétrique (ce qui permet de se dispenser du certificat du serveur). Pour établir un tunnel avec un algorithme symétrique, il faut que le serveur partage une clé avec chaque client ! Ces clés sont stockées dans des fichiers protégés par un mot de passe, appelés PAC (Protected Access Credential). [15].

EAP-FAST s'exécute en trois phases [3][9] :

— **Phase 0 :** : ll'objectif de cette phase est de fournir un certificat PAC à chaque client. Cette phase est optionnelle car les PAC peuvent également être provisionnés manuellement aux clients au lieu d'utiliser la phase zéro.

— **Phase 1 :** : le serveur et le client établissent des tunnels TLS grâce aux PAC présents dans les clients.

— **Phase 2 :** l'authentification du client s'effectue à l'intérieur du tunnel TLS créé dans la phase 1 et à l'aide d'une méthode d'authentification EAP interne (inner method) supportée par EAP-FAST.

Les avantages :

— l'utilisation de certificat coté serveur ou coté client est optionnelle.

— la capacité de chaîner plusieurs authentifications (en utilisant plusieurs méthodes internes) et de les lier cryptographiquement ensemble (chaînage EAP).

— l'authentification est plus rapide : la création du tunnel est plus rapide avec un algorithme symétrique qu'avec TLS (d'où le jeu de mot avec fast qui signifie "rapide ").

— La rapidité de l'EAP/FAST permet de réduire le délai de handover (réauthentification rapide).

Les inconvénients :

— C'est une méthode d'authentification propriétaire (Cisco),

— la difficulté de mise en oeuvre(la gestion des PAC est lourd).

Le tableau ci-dessous fait une comparaison des cinq méthodes d'authentification présentées.

3. https ://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99791-eapfast-wlc-rad-config.html . consulté le 19/03/2020 22 :54

	MD5	LEAP	FAST	TLS	TTLS	PEAP
Implémentation	Basé sur le défi	Basé sur un mot de passe	PAC	Basé sur un certificat	Certificat de serveur	Certificat de serveur
Attributs d'authentification	Unidirectionnel	Mutuelle	Mutuelle	Mutuelle	Mutuelle	Mutuelle
Difficultés de déploiement	facile	facile	Facile à modérer selon la sécurité	Difficile	Modérée	Modérée
Génération dynamique des clés	Non	Oui	oui	Oui	Oui	Oui
Certificat de serveur	Non	Non	Oui pour une sécurité maximale	Oui	Oui	Oui
Certificat client	Non	Non	Oui pour une sécurité maximale	Oui	Non	Non
Tunnel TLS	Non	non	Oui	Non	Oui	Oui
Compatible WPA	Non	Oui	Oui	Oui	Oui	Oui
Security WLAN	faible	modérée	Faible à sécuriser selon la mise en œuvre	Sécurité maximale	Sécurise	Sécurise
Vulnérabilités	Identité exposée, attaque Dictionnaire, attaque MIM.	Identité exposée, attaque Dictionnaire	La sécurité maximale est comparable à PEAP et TTLS.	Identité exposée	attaque MIM.	attaque MIM

Tableau III.3 – Propriétés des méthodes d'authentification EAP [3]

III.7 Conclusion

Le protocole 802.1x est un protocole robuste qui permet par l'intermédiaire de protocoles préexistants (EAP et Radius) d'assurer l'authentification. Par le contrôle de port qu'il apporte, il permet d'empêcher des trames de source inconnue de circuler sur le réseau. Il permet alors d'obtenir un réseau local sécurisé à partir de la couche de liaison de données. Ce protocole a été repris comme élément pour bâtir le standard en réseau Wifi, dans le domaine où il était le moins pertinent. Enfin, c'est un protocole récent et qui est mis à jour pour corriger les problèmes qui peuvent apparaître. Dans le chapitre suivant, nous nous intéresserons à l'implémentation des cinq méthodes d'authentification dans le but de les comparer en termes de sécurité et de performances réseaux. Cela nous permettra d'avoir une idée sur la méthode qui convient le mieux aux WLAN.

Chapitre IV

Implémentation et Teste

IV.1 Introduction :

Après avoir décrit dans le chapitre précédent le fonctionnement et les mécanismes de l'authentification dans les réseaux sans-fil WLAN avec le standard 802.1x, nous présentons dans ce chapitre l'étape d'implémentation ainsi que celle de test. Nous commençons par décrire le contexte de not projet en présentant l'organisation d'accueil, puis nous présentons le processus d'implémentation des méthodes d'authentification EAP à travers le mécanise de sécurité WPA2-Entreprise dans le but de les comparer entre eux en termes de **performance réseau**.

IV.2 Organisme d'accueil :

ICT-Towers est une **entreprise** fondée début 2014, qui qui offre des services de formation, d'audit et de déploiement de solutions ainsi que de recherche et de développement. Ces services sont liés à divers domaines des TIC (Technologies de l'information et de la communication) : routage et commutation, haute disponibilité et sécurité, Voix IP et sans fil, systèmes d'exploitation, virtualisation, sauvegarde et stockage, qualité des services.

FIGURE IV.1 – ICT-TOWERS logo

Les activités de ICT-Towers peuvent être divisées en trois entités différentes :

formation :

ICT-Towers a fait des investissements importants pour dispenser efficacement une formation professionnelle avec des instructeurs hautement qualifiés (dans les plans techniques et pédagogiques), avec un contenu enrichi ainsi que des plateformes matérielles et logicielles complètes pour les travaux pratiques.

Consultation :

ICT-Towers propose des missions de déploiement des solutions techniques, missions d'audit permettant aux clients d'avoir une vision approfondie de leurs solutions, ainsi que des recommandations concernant les meilleures pratiques liées à chaque problème détecté, anomalie, faille et/ou vulnérabilité.

ICT-Towers propose aussi des missions d'assistance, de support et de suivi technique qui aident considérablement les clients dans la gestion et la maintenance de leurs projets et solutions TIC.

Recherche et développement :

ICT-Towers continue de développer des solutions spécifiques en mettant en place une structure de recherche et développement. Son objectif principal est de mener des recherches sur la base des besoins des clients et de procéder au développement de solutions TIC utiles et utilisables.

ICT-Towers soutient tous les travaux et activités qui contribuent aux innovations technologiques et encourage tous les types de découverte et d'invention dans le domaine des TIC.

IV.3 Objectifs du stage :

Durant notre stage au sein du l'entreprise **ICT-TOWERS**, nous avons dû réaliser plusieurs types de missions. Le stage s'est déroulé en trois parties :

- Une phase de remise à niveau réseau par la pratique de plusieurs travaux dirigés ;
- Puis une rédaction du module pédagogique via une étude et application du protocole 802.1x, Radius et de ses dépendances ;
- et enfin, la mise en place des implémentations des différentes méthodes d'authentification EAP afin de réaliser des tests et des analyses.

La dernière partie correspond à la majeure partie de notre stage qui nous permet de mieux appréhender la mise en place d'une authentification au sein d'un réseau WLAN.

IV.3.1 Topologie du réseau :

Afin de configurer le scénario de test, nous avons reproduit la topologie dans un enivrement réel de la société **ICT-TOWERS**. La figure (IV.2) montre la topologie reproduite.

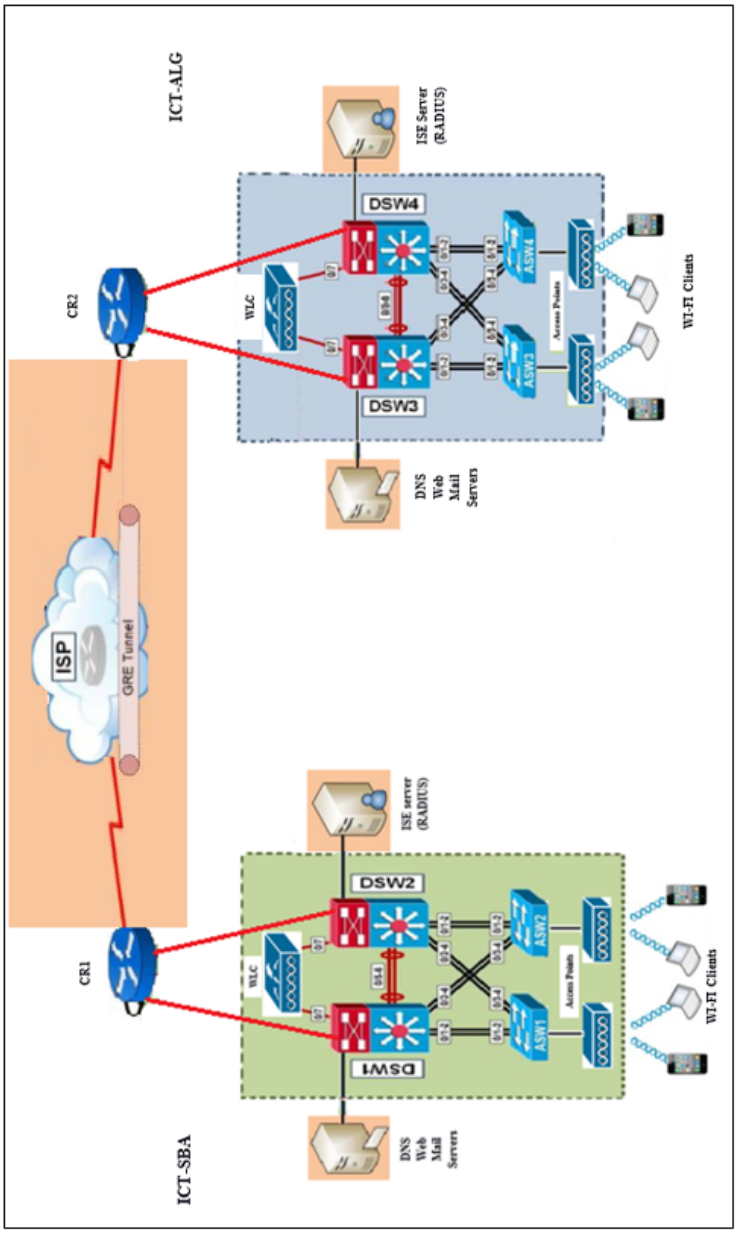


Figure IV.2 – topologie globale

Il s'agit d'une topologie haute disponibilité qui répond à la conception du réseau (network design) professionnelle. Elle est constituée de trois niveaux :

— **La couche Coeur :** est considérée comme l'épine dorsale des réseaux, généralement elle se compose de routeurs puissants de grande capacité, associe des ressources plus élevées et très rapides. Ces routeurs sont conçus pour fusionner des réseaux géographiquement séparés. Les commutateurs qui fonctionnent au niveau de cette couche commutent les paquets le plus rapidement possible.
Les routeurs CR1 et CR2 sont situés respectivement dans l'entreprise ICT-SBA à **Sidi-Bel-Abbès** et l'entreprise ICT-ALG à **Alger**.

— **La couche distribution :**c'est la couche centrale. Le but de cette couche est de fournir une définition des limites en implémentant des listes d'accès et d'autres filtres. Par conséquent, la couche de distribution définit la stratégie pour le réseau. Elle comprend des commutateurs de couche 3 (multi-layer) haut de gamme. La couche de distribution garantit que les paquets sont correctement acheminés entre les sous-réseaux et les VLAN de l'entreprise.

Les switches multi-layer : DSW1, DSW2, DSW3 et DSW4 sont considérés comme des switches de distribution.

WLC est le contrôleur du réseau WLAN : il s'agit d'un point central qui sert à contrôler et à gérer ainsi que la supervision des points d'accès.

— **La couche d'accès :** comprend des commutateurs d'accès et les points d'accès qui sont connectés aux périphériques finaux (ordinateurs, imprimantes, serveurs, etc.). Les commutateurs de couche d'accès garantissent que les paquets sont livrés aux périphériques finaux.

Les switches ASW1, ASW2, ASW3 et ASW4 ainsi que les points d'accès sont considérés comme des équipements de la couche d'accès.

ICT-SBA : le centre de l'entreprise ICT-TOWERS à Sidi-Bel-Abbès.

ICT-ALG : le centre de l'entreprise ICT-TOWERS à Alger.

ISE-Server : est une plate-forme de gestion des politiques de sécurité d'une manière centralisée qui met en place un accès sécurisé aux ressources du réseau filaire et sans fils. Cisco ISE (Identity Services Engine) offre une plus grande visibilité de contrôle d'accès sur les utilisateurs et les terminaux.

ISP(internet service provider) : c'est un réseau propre d'une compagnie qui sert les clients d'internet et sur lequel les réseaux d'entreprises se connectent à travers internet.

GRE-Tunnel : GRE est un protocole de tunnel conçu par Cisco. Il permet de placer n'importe quel trafic (via un autre réseau non maitrisé), dans un tunnel pour transporter des paquets entre des réseaux distants sous un tunnel sécurisé.

Dans notre banc de test nous nous intéressons seulement à la partie décrite par la Figure IV.3 :

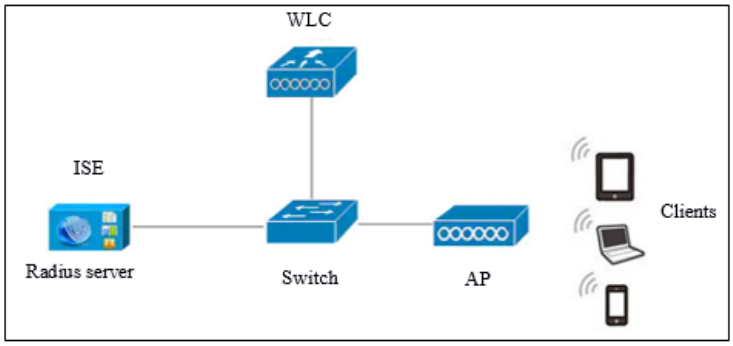


Figure IV.3 – banc de test

IV.3.2 Objectifs du Test

Comme nous avons mentionné précédemment, les tests sont conçus pour visualiser l'impact du processus de l'authentification sur les performances réseaux dans le but d'avoir un équilibrage entre la sécurité requise et les performances réseaux avec les différents critères de performance réseau comme le débit binaire, la latence.

L'analyse de toutes ses informations nous permettra d'avoir une vue globale sur les méthodes d'authentification afin de recommander la plus **équitable qui convient aux** réseaux WLAN.

IV.4 Les facteurs de sélection :

Comme nous avons vu précédemment, il existe de nombreuses méthodes d'authentification qui pourraient être prises en charge par 802.1x (EAP). La question qui se pose est laquelle est la meilleure ? Il n'y a pas de réponse simple ; chaque méthode peut être un choix idéal pour un environnement réseau spécifique. Pour cela, il existe plusieurs facteurs dont la décision de sélection de la méthode d'authentification EAP la plus appropriée dépendra sur la base de ces facteurs.

Pour fournir aux organisations et aux clients WLAN la solution d'authentification la plus adaptée à leurs besoins de sécurité et à leurs environnements réseau spécifiques, des procédures de sélection de méthodes d'authentification EAP ont été développées sur la base de ces facteurs.

IV.4.1 Niveau de protection :

Les différentes méthodes d'authentification ont des capacités de sécurité différentes et fournissent aux organisations différents niveaux de protection. Le niveau de protection fourni par une méthode d'authentification dépend de [4] :

— La technique d'implémentation de la méthode d'authentification ;

— L'attribut d'authentification : mutuel ou unilatéral.

La plupart des méthodes d'authentification EAP (à l'exception de MD5, qui n'est pas recommandé pour les WLAN) fournissent une authentification mutuelle, donc le facteur décisif de la comparaison du niveau de protection fourni par les différentes méthodes d'authentification sera leur technique de mise en oeuvre. En se basant sur ce facteur, la sélection de la méthode de l'authentification sera comme suit :

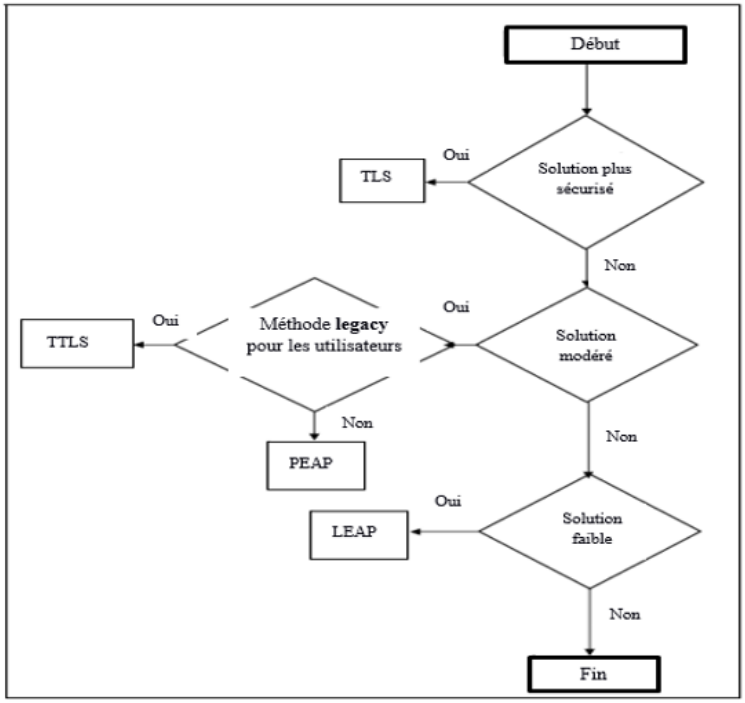


Figure IV.4 – : la sélection de la méthode de l'authentification basé sur le niveau de protection [4]

IV.4.2 La vulnérabilité d'un réseau WLAN :

Le niveau de protection fourni par les méthodes d'authentification et le niveau de protection requis par les organisations sont deux concepts totalement différents. Le premier dépend uniquement de la technique de mise en oeuvre utilisée, tandis que le second dépend des risques et des attaques possibles dans un certain environnement ainsi que des raisons commerciales pour le déploiement des WLAN. Tous ces

éléments affectent la vulnérabilité d'un WLAN dans un environnement spécifique. La sélection de la méthode d'authentification EAP basée sur les attaques possibles sera comme suit :

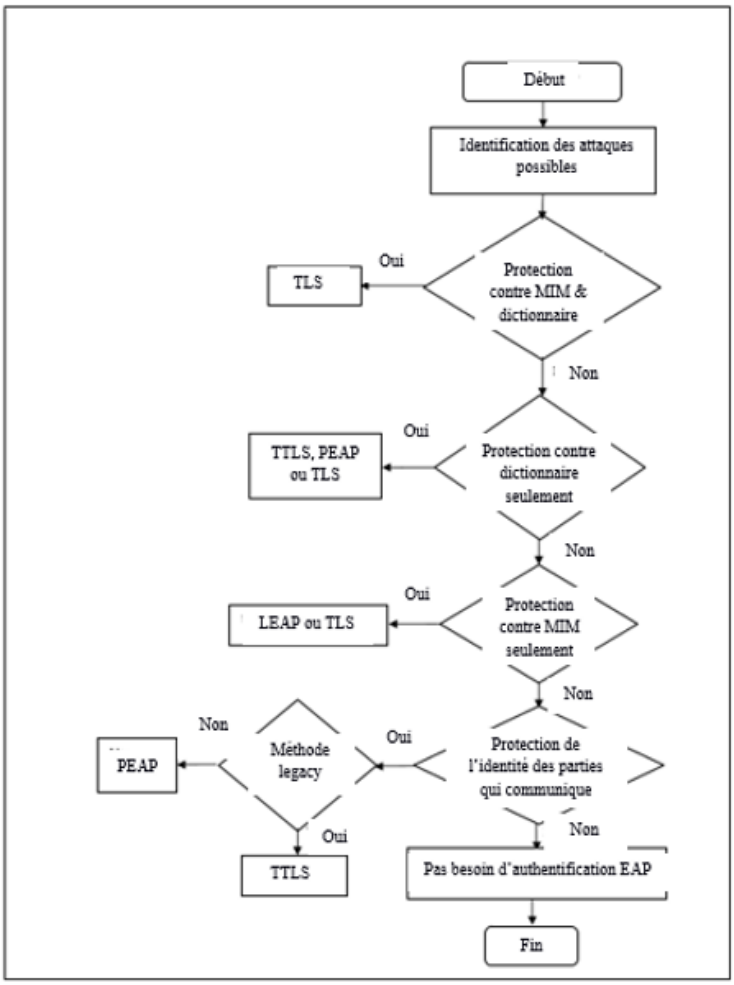


Figure IV.5 – : la sélection de la méthode de l'authentification basé sur la vulnérabilité du réseau [4]

IV.4.3 La nature de l'infrastructure réseau :

Certaines méthodes exigent comme condition préalable de base l'existence d'une infrastructure réseau de soutien, l'adaptation ou la possibilité de la mettre à niveau pour répondre aux exigences de la méthode d'authentification et ce pour la rendre capable de fournir la protection requise.

Une infrastructure réseau de support comprend tous les composants matériels, logiciels requis par une certaine méthode d'authentification. Différentes méthodes d'authentification, en fonction de leur implémentation technique, nécessitent une infrastructure WLAN différente ; le déploiement de TLS nécessite l'existence d'une

infrastructure à clé publique (PKI), LEAP nécessite des produits Cisco ou conformes au programme des "extensions compatibles Cisco" (Cisco Compatible Extension CCX) pour une infrastructure non Cisco, etc[4]. La sélection de la méthode d'authentification EAP basée sur l'infrastructure réseau sera comme suit :

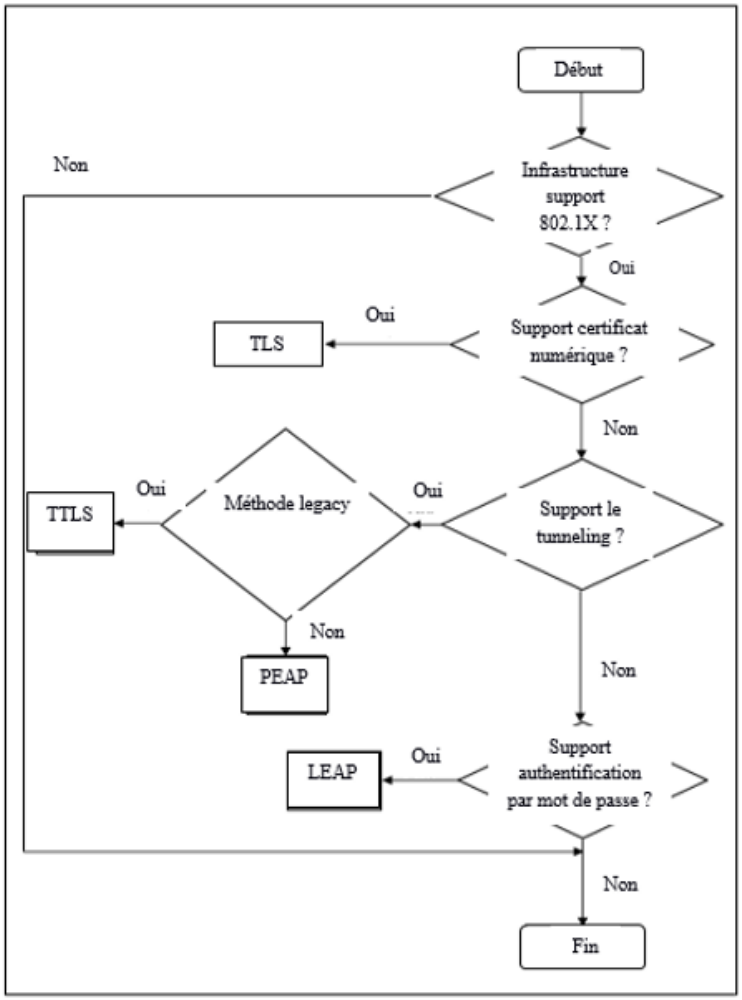


Figure IV.6 – : sélection de la méthode de l'authentification basé sur l'infrastructure réseau [4]

IV.4.4 Les coûts :

Le coût de la mise en oeuvre de la méthode d'authentification comprend toujours le coût de toute mise à niveau de l'infrastructure requise pour mettre en oeuvre la méthode. Il comprend aussi le coût associé à la mise à niveau des connaissances et des compétences des utilisateurs des clients WLAN à un niveau qui leur permet d'utiliser sans difficulté la méthode d'authentification implémentée. Le fait que chacune des méthodes d'authentification soit implémentée en utilisant une technique différente (basée sur un mot de passe, basée sur un certificat et tunneling), les coûts de la

mise en oeuvre de différentes méthodes d'authentification **varieront**. Non seulement cela, mais le coût de la mise en oeuvre de la même méthode d'authentification dans différents environnements de réseau sera différente en fonction de l'infrastructure WLAN existante.[4]

La capacité des organisations ou des clients WLAN à répondre au coût d'implémentation imposée par la méthode d'authentification qui peut leur fournir le niveau de protection souhaité est **un élément critique**. La sélection de la méthode d'authentification EAP basée sur la mise à niveau sera comme suit :

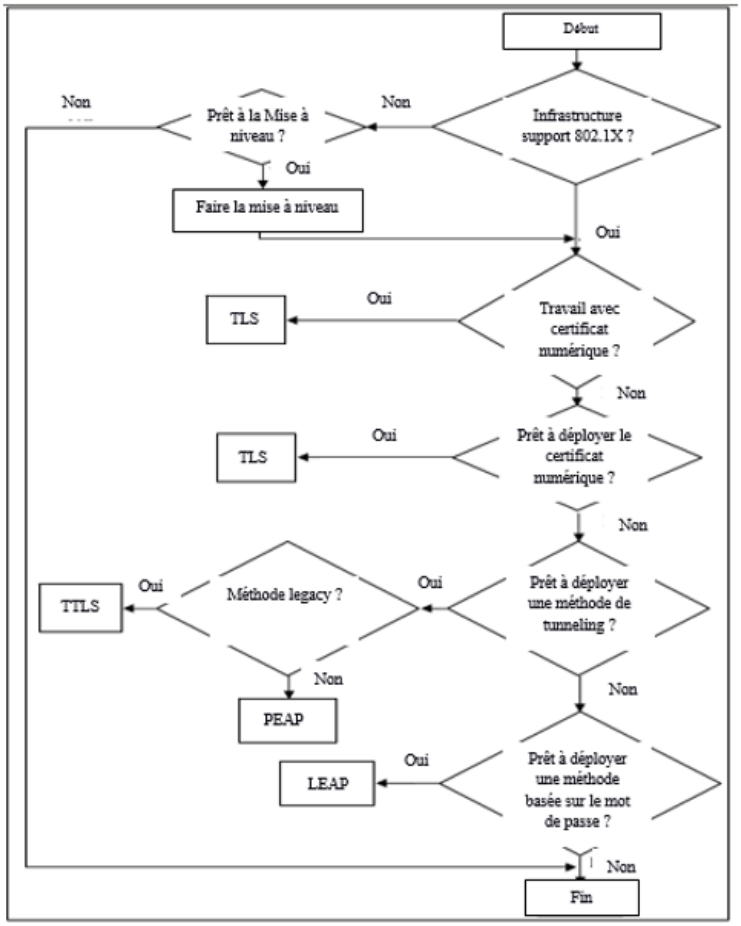
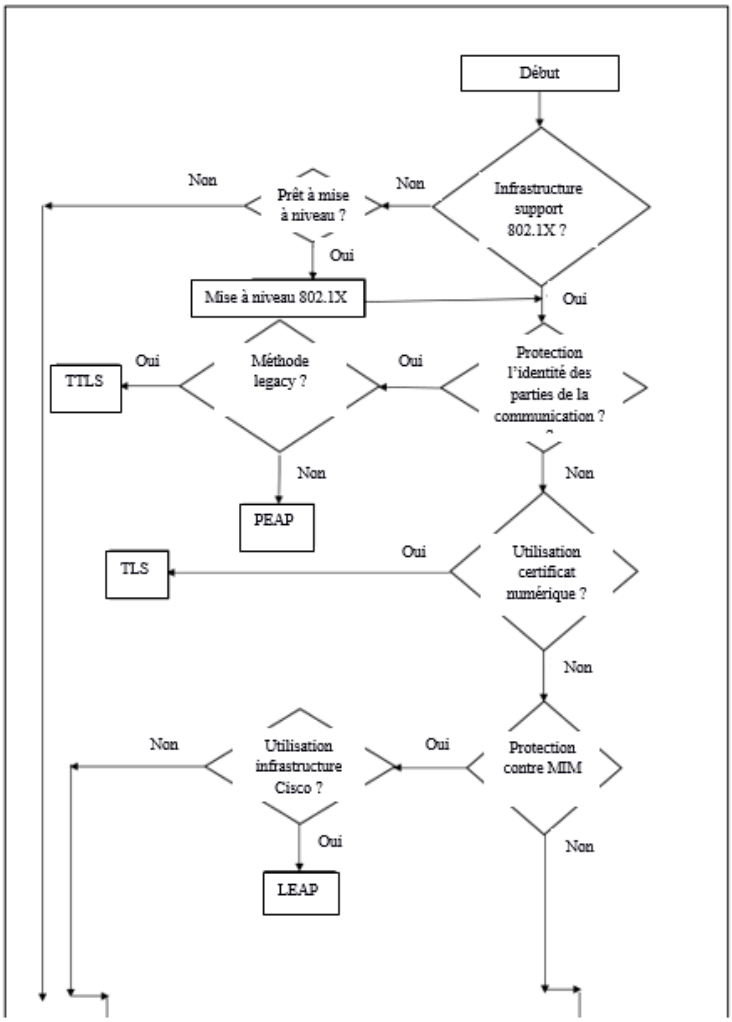


Figure IV.7 – la sélection de la méthode de l'authentification basé sur les couts [4]

Il est évident qu'il existe une forte relation entre les facteurs de sélection, chacun d'eux ayant un impact important sur les autres facteurs et le processus de sélection lui-même. Par exemple, si la méthode d'authentification sélectionnée n'est pas prise en charge par l'infrastructure existant du WLAN, il est alors nécessaire de la mettre à niveau, ce qui signifie des coûts de mise en oeuvre supplémentaires. Si une mise à niveau est inacceptable, la deuxième meilleure méthode d'authentification prise en charge par l'infrastructure existante doit être sélectionnée, mais elle peut ne pas

être efficace suffisamment pour assurer le degré de protection souhaité [4].

D'autre part, il existe d'autres facteurs moins importants tels que les difficultés de déploiement, la complexité de l'administration et de la gestion, etc. La sélection de la méthode d'authentification EAP basée sur tous les facteurs sera comme suit :



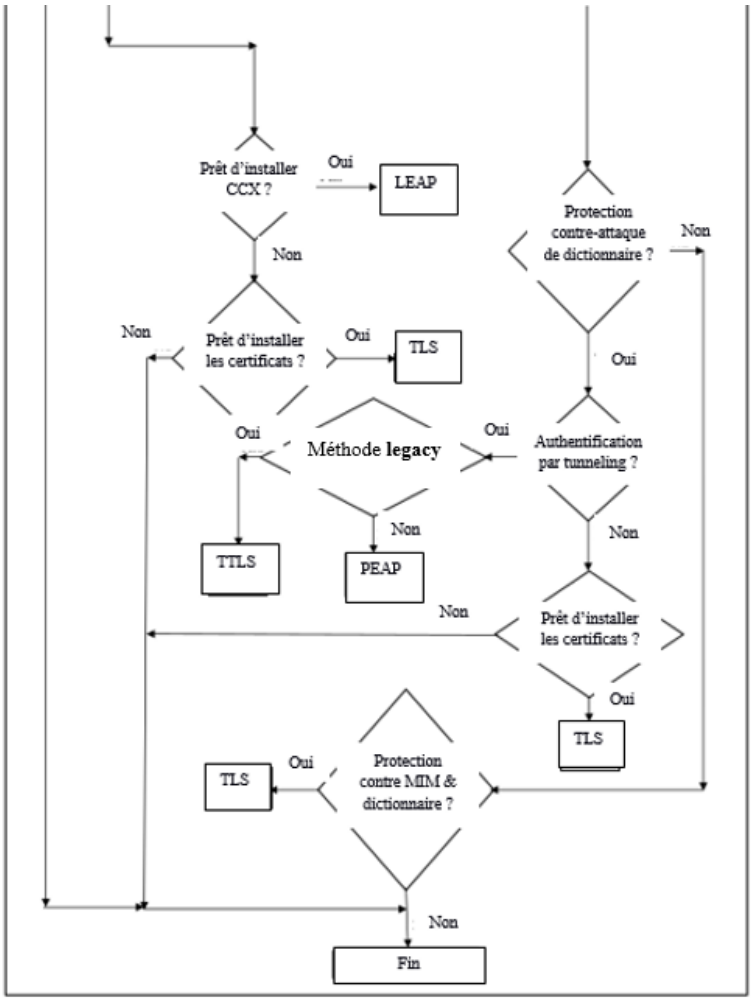


Figure IV.8 – processus globale de la sélection de la méthode de l'authentification [4]

IV.5 Tests et discussion :

IV.5.1 Scenario :

La configuration du banc d'essai mentionnée dans la figure (IV.3) était basée sur l'architecture client / serveur en utilisant des connexions sans fil. Le matériel utilisé pour effectuer les expériences est indiqué dans la configuration respective. Les spécifications techniques des équipements utilisés dans le banc d'essai sont présentées dans le tableau suivant :

Equipements	Spécifications techniques
Client A	Système d'exploitation : Linux distribution Manjaro CPU : intel® core™ i3 3110M CPU @2.40 GHz (4 CPUs) 2.4GHz RAM : 4096 MBytes Carte réseau Wi-Fi : Atheros AR956x 802.11b/g/n
Client B	Système d'exploitation : Windows 7 professionnel 64 Bits version (6.1 version 7601) CPU : intel® core™ i5 2450M CPU @2.50 GHz (4 CPUs) 2.5GHz RAM : 6144 MBytes Carte réseau Wi-Fi : Ralink RT5390 802.11b/g/n
Serveur ISE du Cisco Identity Services Engine (ISE) Utilisé comme serveur Radius	Cisco Application Deployment Engine OS Release: 2.3 ADE-OS Build Version: 2.3.0.187 ADE-OS System Architecture: x86_64
Contrôleur WLC du Cisco série 2500	Prend en charge jusqu'à 75 points d'accès Prend en charge jusqu'à 1 000 clients Prend en charge les clients Wi-Fi conforme au norme : IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac
Access point (AP) du Cisco Aironet série 1400	Point d'accès Aironet série 1140 du Cisco AIR-LAP1142N-E-K9 - Prend en charge les normes 802.11a/g/n - mode « Controller-based »
Commutateur (Switch) du Cisco Série 3500	-24 ports PoE -commutateur multicouche

Tableau IV.1 – caractéristiques physiques des équipements du test

Un échange de données entre plusieurs clients a été testé comme le montre la figure (IV.9) :

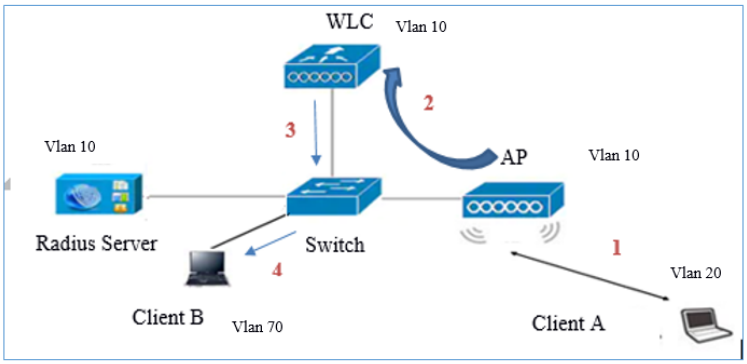


FIGURE IV.9 – processus d'échange de donné dans le réseau WLAN

Pour évaluer les performances du réseau dans cet environnement, des expériences ont été effectués de telle façon que des données ont été échangées entre le **client A** et le **client B**.

Cette analyse comparative a été réalisée en étudiant expérimentalement les performances de chaque méthode d'authentification en ce qui concerne le débit binaire et le delai (RTT).

IV.5.2 Les outils utilisés :

- **Logiciel Filezilla :** c'est un outil basé sur l'architecture client / serveur (Filezilla client et Filezilla server) qui sert à transférer des fichiers entre deux machines dans un réseau.
- **NetworkPinger :** c'est un outil de supervision des réseaux ; il offre des statistiques sur le parcours des paquets entre deux machines dans un réseau.

IV.5.3 Résultats expérimentaux :

Débit binaire :

Le client B doté de l'outil Filezilla serveur va transférer des fichiers vers le client A doté de Filezilla client via le protocole FTP pour l'observation de la quantité de données transmises dans un intervalle de temps.

Les mésures du débit binaire ont été observées dans les différentes situations suivant la méthode d'authentification appliquée. La figure (IV.10) montre les résultats obtenus dans le test effectué.

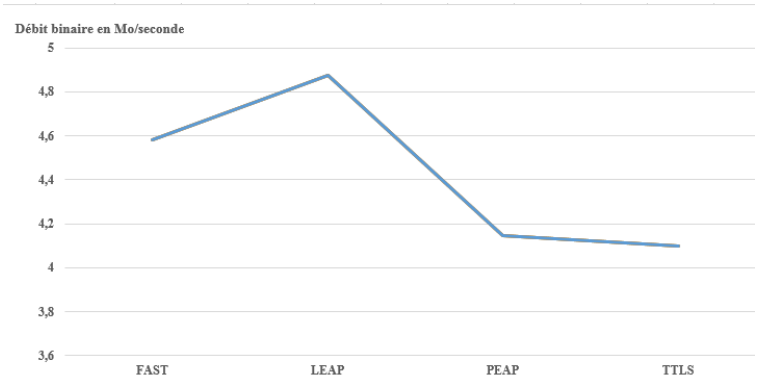


Figure IV.10 – Comparaisons des débits binaires

Le Delai RTT :

Le client B a été configuré pour envoyer des paquets au client dans les différentes situations suivant à la méthode d'authentification utilisée. La taille de paquet varié à chaque opération du teste : 1000 octets, 2000 octets et 8000 octets .

La figure suivante montre le résultat pour chaque transfert :

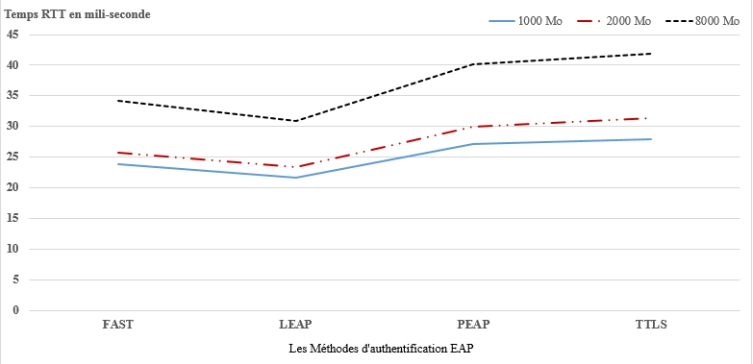


Figure IV.11 – Comparaison du Delai (RTT)

IV.5.4 Discussion :

Les métriques que nous avons mesurées pour évaluer les performances du processus de l'authentification sont le débit binaire et le délai (RTT). Étant sélectionnés, la méthode d'authentification, les résultats d'évaluation des performances sont comparés aux résultats des autres méthodes d'authentification.

Le débit binaire détermine la vitesse de transmission des données dans le réseau. En variant la méthode d'authentification ; la mise en oeuvre montre :

— Un meilleur débit était marqué par la méthode d'authentification LEAP que les autres suivie par la méthode d'authentification EAP-FAST qui offre un débit binaire moins relatif.

— Les débits marqués par les méthodes d'authentification PEAP et EAP-TTLS sont presque identiques.

Le délai (RTT) c'est le temps de parcours d'un paquet en millisecondes (ms) (le temps d'aller-retour) entre deux extrémités dans un réseau. En variant la taille du paquet 1000 Mo, 2000 Mo ensuite 8000 Mo ; les résultats obtenus montrent :

— Initialement, la taille du paquet était définie sur 1000 M octets ; y a aucun effet majeur sur le délai (RTT) qui est presque le même pour tous les méthodes.

— Variant les tailles des paquets de 1000 Mo à 8000 Mo octets nous a conduit de visualiser un délai minimal avec la méthode d'authentification LEAP suivie par EAP-FAST par apports aux autres méthodes d'authentifications EAP-TTLS et PEAP qui ont des délais presque identiques.

Les résultats indiquent que l'authentification introduit des charges supplémentaires sur les performance réseaux en fonction du type de méthode d'authentification déployé, tel que les performances de LEAP qui repose sur une authentification très simple via un couple identifiant /mot de passe sont mieux que PEAP, EAP-TTLS et

EAP-FAST. Cette dernière possède des performances acceptables par apport PEAP, EAP-TTLS due l'utilisation des certificats est optionnelle. Cependant PEAP, EAP-TTLS utilisent des certificats dans le côté de serveur et reposent sur une authentification mutuelle.

L'authentification dans les réseaux sans fil basé sur le standard 802.1x qui repose sur l'architecture AAA engendre plus de trames d'authentification transférés dans le réseau ce qui provoque des charges supplémentaires. Ces trames d'authentification imposent une dégradation significative des performances réseaux. L'augmentation du délai (RTT) ainsi que la diminution du débit sont constatées lors du passage de l'authentification avec une méthode très basique LEAP à des méthodes d'authentification plus complexes comme FAST, PEAP et TTLS qui repose sur le l'utilisation des certificats.

IV.6 Conclusion :

Ce travail visait à analyser l'impact des mécanismes de sécurité sur les différents méthodes d'authentification utilisés dans les réseaux WLAN.

Cette analyse nous a confirmé que les niveaux de sécurité de chaque méthode d'authentification aient des impacts différents sur les performances réseaux. Ce qui nous a fournir une visibilité cohérente en ce concerne le choix de la méthode d'authentification tout en pendre en considération le niveau de sécurité approprié par rapport aux performances du réseau à aboutir.

Conclusion générale

Les réseaux sans fil sont quasi-indispensable de nos jours, ils présentent divers avantages parmi lesquels leur simplicité de déploiement, mobilité, faible coût en comparaison de l'installation et la maintenance d'un réseau câblé. Il faut le considérer a priori comme un réseau ouvert au public mais également comme une bulle de risque à cause principalement d'absence de support physique qui augmente le niveau d'écoute non désirée. La norme IEEE 802.11 est l'un des mécanismes les plus largement adoptés pour les réseaux WLAN, elle fournit des directives complètes pour leur fluidité opérationnelle.

Le 802.11 souffrait d'une confidentialité limitée des données et d'une procédure lourde d'échange des paramètres de sécurité. IEEE a introduit le 802.1x pour l'authentification et la gestion des clés. Le 802.1x est un protocole de contrôle d'accès réseau basé sur les ports qui utilise le protocole d'authentification extensible (EAP) au niveau de la couche de transport. Le 802.1x définit uniquement le mécanisme d'authentification et ne recommande aucune méthode d'authentification appropriée.

Dans ce mémoire, nous avons étudié le protocole 802.1x, tout en se concentrant sur la phase d'authentification qui est assurée par le protocole EAP. Ce dernier supporte de multiples méthodes d'authentification telles que MD5 (Message Digest 5), TLS (Transport Layer Security), TTLS (Tunneled TLS), PEAP (Protected Extensible Authentication Protocol), LEAP (Lightweight Extensible Authentication Protocol), etc.

L'objectif de ce travail étant d'étudier et d'implémenter les différentes méthodes d'authentifications afin de mesurer les performances réseaux telles que le débit, et le délai (RTT Round Time Trip). Et ce afin nous a fournir une visibilité cohérente pour le choix de la méthode d'authentification en considérant le niveau de sécurité approprié par rapport aux performances du réseau à aboutir.

Comme perspectives de notre travail, nous allons continuer la réalisation d'une application permettre d'analyser les performances réseau de chaque méthode et le

choix dynamique de la méthode d'authentification EAP la plus appropriée pour les besoins et les spécifications des réseaux WLAN.

Bibliographie

[1] Bernard Aboba et al. « Extensible authentication protocol (EAP) ». In : (2004).

[2] Djamil Aissani et al. « Proposition d'un protocole d'accès au médium dans les réseaux locaux sans fil IEEE 802.11 à fortes contraintes temporalles ». Thèse de doct. université Abderahmane Mira, 2009.

[3] Khidir M Ali et Ali Al-Khlifa. « A comparative study of authentication methods for wi-fi networks ». In : *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*. IEEE. 2011, p. 190-194.

[4] Khidir M Ali et Thomas J Owens. « Selection of an EAP authentication method for a WLAN ». In : *International Journal of Information and Computer Security* 1.1-2 (2007), p. 210-233.

[5] Giuseppe Anastasi, Luciano Lenzini et Enzo Mingozzi. « HIPERLAN/1 MAC protocol: stability and performance analysis ». In : *IEEE Journal on Selected Areas in Communications* 18.9 (2000), p. 1787-1798.

[6] Paul Arana. « Benefits and vulnerabilities of Wi-Fi protected access 2 (WPA2) ». In : *INFS* 612 (2006), p. 1-6.

[7] Mohamad Badra. « Le transport et la sécurisation des échanges sur les réseaux sans fil ». Thèse de doct. 2004.

[8] Boris Bellalta. « IEEE 802.11 ax: High-efficiency WLANs ». In : *IEEE Wireless Communications* 23.1 (2016), p. 38-46.

[9] Serge Bordères. *Authentification réseau avec Radius: 802.1 x, EAP, FreeRadius*. Editions Eyrolles, 2006.

[10] Jyh-Cheng Chen et Yu-Ping Wang. « Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience ». In : *IEEE communications magazine* 43.12 (2005), supl-26.

[11] Mario Collotta et al. « Bluetooth 5: A concrete step forward toward the IoT ». In : *IEEE Communications Magazine* 56.7 (2018), p. 125-131.

[12] Der-Jiunn Deng, Kwang-Cheng Chen et Rung-Shiang Cheng. « IEEE 802.11 ax: Next generation wireless local area networks ». In : *10Th international conference on heterogeneous networking for quality, reliability, security and robustness*. IEEE. 2014, p. 77-82.

[13] Dominique Dhoutaut. « Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc: de la simulation à l'expérimentation ». In : *Laboratoire CITI, INSA de Lyon* 11 (2003), p. 26.

[14] Jim Geier. *Implementing 802.1 X security solutions for wired and wireless networks*. John Wiley & Sons, 2008.

[15] Aurélien Géron. *WiFi Professionnel-3e édition-: La norme 802.11, le déploiement, la sécurité*. Dunod, 2009.

[16] Mahmoud Khasawneh et al. « A survey on Wi-Fi protocols: WPA and WPA2 ». In : *International Conference on Security in Computer Networks and Distributed Systems*. Springer. 2014, p. 496-511.

[17] Evgeny Khorov et al. « A tutorial on IEEE 802.11 ax high efficiency WLANs ». In : *IEEE Communications Surveys & Tutorials* 21.1 (2018), p. 197-216.

[18] Jacques-Olivier Lachaud. « INFO006 (ex INFO913)-Cryptologie et Sécurité Informatique ». In : (2011).

[19] Zihuai Lin, Goran Malmgren et Johan Torsner. « System performance analysis of link adaptation in HiperLAN type 2 ». In : *Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No. 00CH37152)*. T. 4. IEEE. 2000, p. 1719-1725.

[20] Cédric Llorens et al. *Tableaux de bord de la sécurité réseau*. Editions Eyrolles, 2011.

[21] Leonardo Maccari et al. « Secure, fast handhoff techniques for 802.1 X based wireless network ». In : *2006 IEEE International Conference on Communications*. T. 9. IEEE. 2006, p. 3917-3922.

[22] Paul MüHLETHALER. « Sécurité dans les réseaux sans fil: Norme IEEE 802.11 ». In : *Techniques de l'ingénieur. Sécurité des systèmes d'information* TE7377 (2003), TE7377-1.

[23] Laurentiu Sorin Paun. « Gestion de la mobilité dans les réseaux ambiants ». Thèse de doct. 2005.

[24] Jean-François Pillou et Jean-Philippe Bay. *Tout sur la sécurité informatique-4e édition*. Dunod, 2016.

[25] Jean-François Pillou et Fabrice Lemainque. *Tout sur les réseaux et Internet-4e éd.* Dunod, 2015.

[26] Guy Pujolle. *les réseaux*. Eyrolles, 2008.

[27] Michel Riguidel. « La sécurité des réseaux et des systèmes ». In : *Vuibert, encyclopédie informatique* (2006).

[28] Katia Runser. « Méthodologies pour la planification de réseaux locaux sans-fil. » Thèse de doct. Université de Poitiers, 2005.

[29] Luc Saccavini. « 802.1 X et sécurisation de l'accès au réseau local ». In : *INRIA,[en ligne]. Disponible sur http://2003. jres. org/actes/paper* 111 (2003).

[30] Christophe Saillard. « 802.1 X: Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur ». In : *Centre Réseau Communication, Université Louis Pasteur, Strasbourg* (2003).

[31] Rüdiger Schollmeier. « A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications ». In : *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE. 2001, p. 101-102.

[32] Prashant Singh, Mayank Mishra et PN Barwal. « Analysis of security issues and their solutions in wireless LAN ». In : *International Conference on Information Communication and Embedded Systems (ICICES2014)*. IEEE. 2014, p. 1-6.

[33] Adrien Van Den Bossche. « Proposition d'une nouvelle méthode d'accès déterministe pour un réseau personnel sans fil à fortes contraintes temporelles ». Thèse de doct. 2007.

[34] Ferroudja Zidani. « Solution d'authentification et de gestion de clés pour le standard 802.11 i des réseaux WiFi ». Thèse de doct. 2018.