الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد– تلمسان –

Université Aboubakr Belkaïd– Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : **Soulimane kamel Eddine**
& Sebbagh Saadallah

Sujet

Problème et solution de sécurité d'un réseau WiFi

Soutenu publiquement, le 29 / 06 / 2022 , devant le jury composé de :

Mr.Baba Ahmed Mohammed Zakarya	MCA	Université de Tlemcen	Président
Mr.Bouabdellah Reda	MAA	Université de Tlemcen	Examinateur
Mr.Hadjila Mourad	MCA	Université de Tlemcen	Encadrant
Mr.Sadi Abdelbari	SI&RM	ICT –TOWERS SBa	Co-Encadrant

Année universitaire : 2021 /2022

Remerciements

Nous tenons à remercier Allah le tout puissant qui nous a donné durant toutes ces années d'études la santé, le courage, la confiance et la foi en nous-mêmes ce qui nous a permis de progresser et d'arriver jusqu'à ce jour.

J'adresse mes sincères remerciements à mes parents. Si je suis ici aujourd'hui, c'est grâce à eux.

Nous ne saurions, réellement trouver les expressions éloquentes que mérite notre encadrant Monsieur HADJILA MOURAD maître de conférences à l'université Abou-Bekr Belkaid, pour sa grande patience, ses conseils et sa disponibilité. Sa compétence a rendu ce travail particulièrement intéressant.

Nos remerciements à Monsieur SADI ABDELBARI 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 adressons nos remerciements aux membres du jury qui nous ferions l'honneur d'évaluer, d'examiner et d'enrichir cette modeste contribution.

Nous remercions cordialement, Monsieur BABA AHMED MOHAMMED ZAKARYA maître de conférences à l'université Abou-Bekr Belkaid d'avoir accepté de présider ce jury de mémoire.

Nous remercions également Monsieur BOUABDELLAH REDA maître assistant à l'université Abou-Bekr Belkaid d'avoir accepté de participer à ce mémoire en qualité d'examinateur.

Nous profiterons aussi de ce mémoire pour exprimer nos plus vifs remerciements envers tous les professeurs de la faculté de technologie de Tlemcen qui nous a apporté du soutien durant nos études.

Que ce travail soit pour le gage de notre profonde estime à tous nos amis et tout celui qui nous ont aidés.

Merci enfin à tous ceux qui, de près ou de loin, nous ont aidés et donc ont contribué au succès de ce travail.

Sebbagh saadallah & Soulimane Kamel Eddine

Dédicaces

Je dédie ce travail à :

Mes très chers parents, Pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études.

Ma chère et adorable sœur et mon grand frère Qui ont su me comprendre, m'épauler et m'encourager dans les moments les plus difficiles. Je vous souhaite une vie pleine de bonheur et de succès et que Allah, le tout puissant, vous protège et vous garde.

.

A Tous les membres de ma grande famille pour leurs soutient.

Mes amis de toujours et à tous les étudiants et mes frères de ma promotion de Master En souvenir de notre sincère et profonde amitié et des moments agréables que nous avons passés ensemble.

Et spécialement à Mon binôme Kamel, Pour son accompagnement, son soutien et son amitié durant toutes ces années d'étude et tout au long de ce projet

A tous ceux qui m'ont aidé de loin ou de prés.

Veuillez trouver dans ce travail l'expression de mon respect le plus profond et mon affection la plus sincère.

SEBBAGH SAADALLAH

Dédicaces

Je dédie ce travail à :

C’est avec une joie immense et le cœur ému que je dédié ce mémoire a mes chers parents et mon adorable sœur pour leurs soutiens, leurs précieux conseils et leurs attentions. ils m’ont permis de réaliser que la est sacrée .ils étaient pour moi , une vraie source d’inspiration et ont été toujours a mes cotés durant les moments difficiles.

Mes mots ne seraient jamais a la hauteur de l’amour et l’affection que vous m’avez témoignée tout au long de mes études. J’aimerais vous exprimer toute ma gratitude et reconnaissance. Cette dédicace serait pour moi ,la meilleure façon de vous honorer et vous monter a quel point vous avez été magnifique Je vous souhaite une vie pleine de bonheur et de succès et que Allah, le tout puissant, vous protège et vous garde.

Mes pensées vont aussi a tous mes amis qui m’ont toujours motivé et encourager je ne pourrais oublier tous les collègues de la même promotion. Leurs sincérités m’ont vraiment touchée. Ils ont contribué a cette réussite et je tiens également a leur souhaiter le meilleur.

Et spécialement mon cher binôme Saad Allah qu’est plus qu’un collègue un frère pour son accompagnement et ses efforts, son soutien et son amitié durant toutes ces années d’étude.

Enfin je remercie toute personne qui a participé de prés ou de loin a l’exécution de ce modeste travail.

SOULIMANE KAMEL EDDINE

Résumé

La transmission radio rend les réseaux sans fil faciles à utiliser, faciles à déployer et économiques, mais pose en revanche des problèmes de sécurité en raison de la nature ouverte du support de transmission utilisé. La norme IEEE 802.11 est l'un des mécanismes les plus largement adoptés pour les WLAN. Il fournit des directives complètes pour leur liquidité opérationnelle. Le 802.11 est en proie à des limitations de la confidentialité des données et à des procédures fastidieuses pour l'échange de paramètres de sécurité. En réponse aux limites de sécurité du 802.11, l'IEEE a introduit le 802.1x pour l'authentification et la gestion des clés.
802.1x est un protocole de contrôle d'accès au réseau basé sur les ports qui utilise le protocole d'authentification extensible (EAP) au niveau de la couche de transport et prend en charge plusieurs méthodes d'authentification telles que TLS, TTLS, PEAP, LEAP, etc.
L'objectif de cette étude est d'évaluer la possibilité d'augmenter la sécurité d'un WiFi.

Mots Clés : Wi-Fi, sécurité, protocole, attaque, cryptage, authentification.

.

Abstract

Radio transmission makes wireless networks easy to use, easy to deploy, and cost-effective, but on the other hand poses security concerns due to the open nature of the transmission medium used. The IEEE 802.11 standard is one of the most widely adopted mechanisms for WLANs. It provides comprehensive guidelines for their operational liquidity. 802.11 is plagued with data privacy limitations and cumbersome procedures for exchanging security parameters. In response to the security limitations of 802.11, the IEEE introduced 802.1x for authentication and key management.
802.1x is a port-based network access control protocol that uses Extensible Authentication Protocol (EAP) at the transport layer and supports multiple authentication methods such as TLS, TTLS , PEAP, LEAP, etc.
The objective of this study is to evaluate the possibility of increasing the security of WiFi.
Keywords: Wi-Fi, security, protocol, attack, encryption, authentication.

ملخص

يجعل الإرسال اللاسلكي الشبكات اللاسلكية سهلة الاستخدام ، وسهلة النشر ، وفعالة من حيث التكلفة ، ولكن من ناحية أخرى تثير مخاوف أمنية بسبب الطبيعة المفتوحة لوسيط الإرسال المستخدم. يعد معيار IEEE 802.11 أحد أكثر الآليات المعتمدة على نطاق واسع لشبكات WLAN. يوفر إرشادات شاملة للسيولة التشغيلية. 802.11 يعاني من قيود خصوصية البيانات والإجراءات المرهقة لتبادل معلمات الأمان. استجابة لقيود أمان 802.11 ، قدم IEEE 802.1x للمصادقة وإدارة المفاتيح.
x802.1 هو بروتوكول تحكم في الوصول إلى الشبكة قائم على المنفذ يستخدم بروتوكول المصادقة المتوسع (EAP) في طبقة النقل ويدعم طرق مصادقة متعددة مثل TLS و TTLS و PEAP و LEAP وما إلى ذلك.الهدف من هذه الدراسة هو تقييم إمكانية زيادة أمان WiFi.
الكلمات المفتاحية : واي فاي ، أمن ، بروتوكول ، هجوم ، تشفير ، مصادقة.

Table de matières

Liste des figures

Liste des tableaux

Liste des abréviations

AES: Advanced Encryption Standard
AP: Access Point.
BSA: Basic Service Area.
BSS: Basic Service Set.
BSSID: Basic Service Set Identifier.
CCMP: Counter Mode CBC-MAC Protocol
CHAP: Challenge Handshake Authentification Protocole.
CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance.
CTS: Clear To Send.
DCF: Distributed Coordination Function.
DoS: Deny of Service.
DS: Distribution System.
EAP: Extended Service Set.
EAP-FAST: EAP Flexible Authentication via Secure Tunneling.
EAP-TLS: EAP Transport Layer Security.
EAP-TTLS: EAP **Tunneled** TLS.
ESS: Extended Service Set.
FHSS: Hopping Spread Spectrum
IBSS: Independent Basic Service Set.
IEEE: Institute of Electrical and Electronics Engineers.
IV: vecteur d'initialisation.
LEAP: Lightweight Extensible Authentication Protocol
LLC : Logical Link Control.
MAC: Media Access Control.
MAN: Metropolitan Area Network.
MD5: Message Digest 5.
MIC: Message Integrity Code.
MS-CHAP: Microsoft Challenge Handshake Authentification Protocol.
OFDM: Orthogonal Frequency Division Multiplexing.
OSI: Open Systems Interconnection.
PAE: Port Access Entity.
PAN: Personal Area Network.
PAP: Password Athentication Protocol
PEAP: Protected EAP.
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent
PPP: point to point protocole.
PSK: Pre Shared Key.
RADIUS: Remote Authentication Dial In User Service.
RC4: Rivest Cipher 4.
RAN: Regional Area Network.
RF: Fréquences Radio.
RTS: Request to Send.
SSID: Service Set Identifier.
TKIP: Temporal Key Integrity Protocol.
WEP: Wired Equivalent Privacy.
WLAN: Wireless LAN.

WLC: Wireless Lan Controller
WPA: Wireless Protected Access.

Introduction Générale

Introduction Générale

À une époque où communication et technologie sont les maîtres mots de notre société, on ne peut douter que l'avenir des réseaux informatiques soit de grandir et de se développer. Cet avenir est pour une bonne part lié aux techniques et aux supports de communication utilisés dans les réseaux.

À l'heure actuelle, la tendance est à la transmission numérique et à l'utilisation de la communication sans fil. De plus, la technologie actuelle permet d'accroître les volumes et les vitesses de transfert des données tout en diminuant les coûts.

De ce fait, nous avons assisté ces dernières années a un essor en puissances des réseaux locaux sans fil ou encore le WiFi (Wireless Fidelity), revient aux différents avantages qu'apportent ces technologies, comme la mobilité, la simplicité d'installation, la disponibilité.

Les réseaux sans fil « Wi-Fi » sont aujourd'hui monnaie courante en entreprise, et pour cause, ils offrent à vos utilisateurs une facilité d'utilisation et un confort évident ! Quel que soit le secteur d'activité et la taille de votre entreprise, mais chaque entreprise a des informations confidentielle et très sensibles, Qui se dit, se fait en confidence, qui contient des informations qui doivent rester secrètes : dossier confidentiel. Qui ne s'adresse qu'à un petit nombre de personnes : une diffusion confidentielle comme la santé et le domaine Militaire … , et installer un réseau sans fils ou bien WiFi sans le sécuriser permet à des personnes non autorisées « les cybercriminels d » écouter, de modifier et d'accéder à ce réseau, il est donc indispensable de le sécuriser dès son installation de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde.

Dans ce mémoire, nous nous intéressons aux problématiques de cyber sécurité réseau sans fil au sein de l'entreprise. Compte tenu des faiblesses des normes de sécurité Wi-Fi, et face à toutes les failles de sécurité et attaques possibles comment assurer la sécurité des mécanismes de sécurité dans les réseaux 802.11 compte tenu de l'hétérogénéité des appareils Wi-Fi (WEP,802.1X, WPA, WPA2,WPA3), optimal, excitants dans l'entreprise en ce moment.

Notre projet est composé de quatre chapitres planifiés comme suit :

Le premier chapitre consiste à définir les généralités sur les réseaux.

Dans le deuxième chapitre, nous présentons une étude générale de la technologie Wi-Fi.

Dans le troisième chapitre nous concentrons sur les notions importantes sur la sécurité et les mécanismes de sécurités des réseaux WiFi et les différentes solutions**.**

A la fin dans quatrième chapitre, allons implémenter et tester l'authentification de protocole 802.1x

chapitre I. **Généralité sur les réseaux**

Chapitre I Généralité sur les réseaux

I.1) Introduction

Les réseaux ont pour fonction de transporter des données d'une machine terminale à une autre. Une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter .

Dans la première partie de 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 de réseau sans fils bien que la technologie WiFi et ses avantages.

I.2) **Généralités sur les réseaux informatiques**

I.2.1) **Définition**

Un réseau informatique est un ensemble des équipements informatiques reliés physiquement entre eux par un support de transmission afin de pouvoir échanger des données, transfert de fichiers, partager des ressources (imprimantes et données)…[1]

I.2.2) **Intérêt d'un réseau**

Il y a deux types principaux des objectifs des réseaux :

- **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,...) [2].

I.2.3) **Les supports réseaux**

Le médium de transport correspond aux éléments matériels et immatériels capables de transporter des éléments binaires, comme les câbles et les ondes radio. Dans le premier cas, ce

sont des fils métalliques ou des fibres optiques qui transportent l'information et dans le second les ondes hertziennes.

Les deux types de support sont plus complémentaires que concurrents. Le hertzien permet la mobilité mais au prix de débits plus faibles. De son côté, le câble propose des débits de plus en plus importants. Même si les débits des équipements mobiles augmentent, l'écart reste stable avec ceux des câbles. On arrive aujourd'hui à des dizaines de gigabits par seconde sur la fibre optique contre des centaines de mégabits par seconde pour le hertzien[1].

I.2.4) 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.

I.2.4.1) La topologie physique

Elle décrit le plan du réseau (la manière dont les équipements réseaux est connectée entre eux). On distingue généralement les topologies suivantes [2] :

- **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 reliés 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 œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.
- **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, aucune communication entre les ordinateurs du réseau n'est possible .En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub ou switch).
- **La topologie en anneau :** Dans cette architecture, les ordinateurs sont reliés sur une seule boucle de câbles. Les signaux se déplacent le long de la boucle dans une

direction et passent par chacun des ordinateurs. A un instant donné, un seul nœud 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 nœud n'émet de message, le jeton est dans un état libre (trame vide). Seul le nœud qui a envoyé le message est en attente d'un accusé de réception. Les autres nœuds 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.

- **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, les 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.

Topologie en arbre : Le réseau est divisé en niveaux. Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds 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.

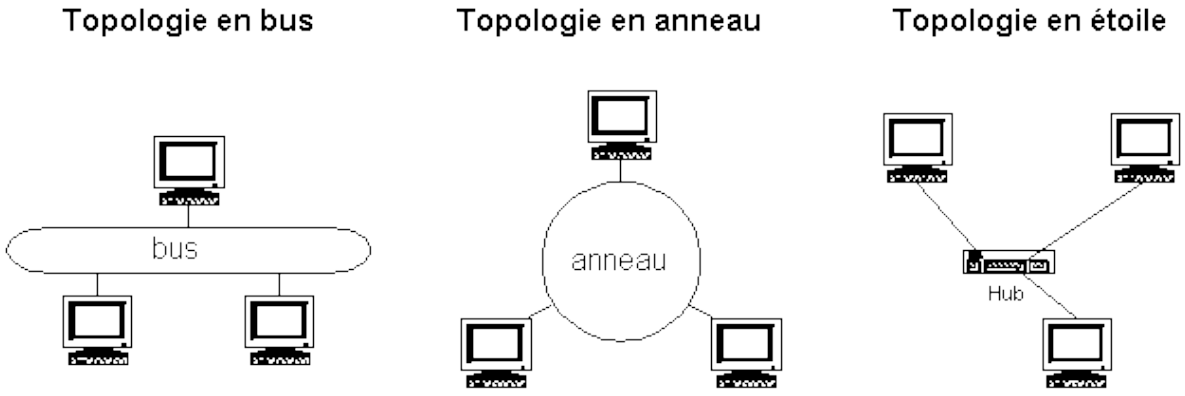


Figure I-1 Exemple de topologie physique de réseau

I.2.4.2) La topologie logique

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

I.2.5) Les Equipements d'interconnexion

Les équipements d'interconnexion entre les réseaux sont :

- **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 et 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 telle façon 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.2.6) 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 deux grandes architectures suivantes se disputent le marché mondial des réseaux [3]:

- L'architecture OSI (Open Systems Interconnection).
- L'architecture TCP/IP (Transmission Control Protocol / Internet Protocol) utilisée dans le réseau internet.

I.2.6.1) 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 du modèle OSI sont :

- **Couche 1 (physique) :** Elle décrit les caractéristiques électriques, logiques et physiques de la connexion de la station au réseau : câbles, connecteurs, cartes réseau.
- **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.
- **Couche 3 (réseau) :** Elle permet 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.
- **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
- **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.
- **Couche 6 (présentation) :** Elle définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.
- **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.2.6.2) 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.2 résume les couches des modèles OSI et TCP/IP.

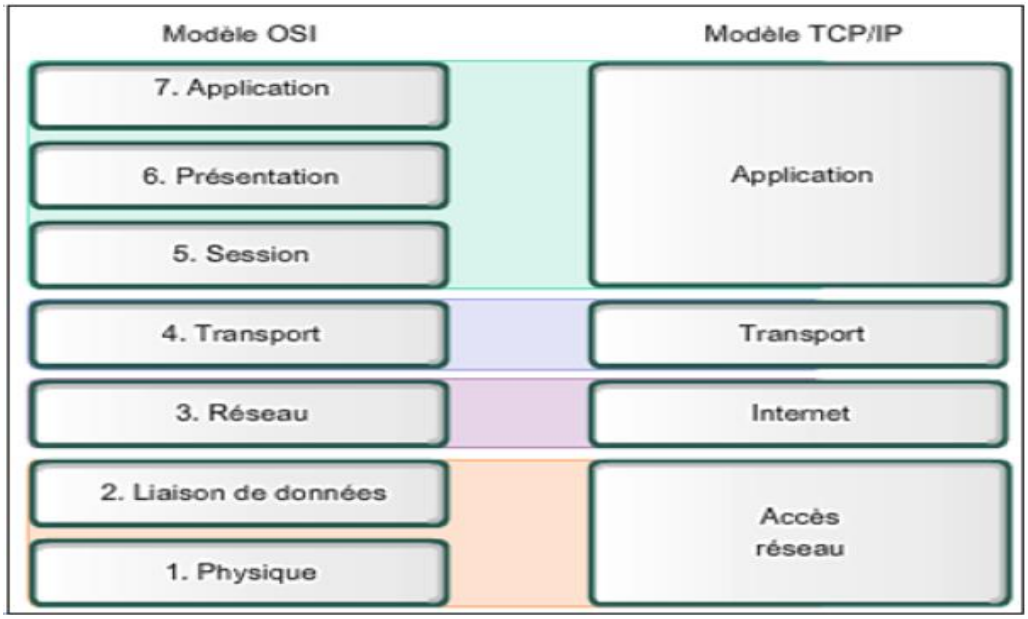


Figure I-2 – architecture OSI et TCP/IP

I.2.7) 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 traditionnelle, 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 [3] :

I.2.7.1) 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.2.7.2) LAN (Local Area Network)

C'est 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.

I.2.7.3) 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.2.7.4) 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.2.7.5) 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.

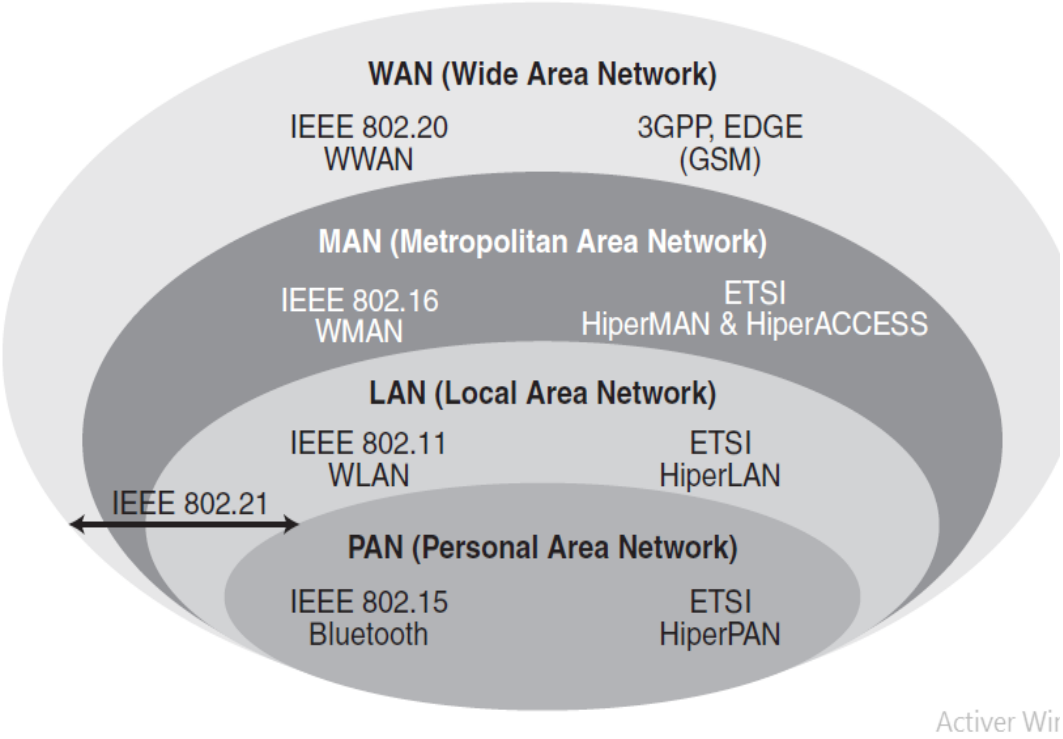


Figure I-3– Les grandes catégories de réseaux informatiques [2]

I.3) **Réseaux filaires vers les réseaux sans fils**

Un réseau câblé utilise des câbles pour connecter des périphériques, tels que des ordinateurs portables ou de bureau, à Internet ou à un autre réseau. Un réseau filaire présente certains inconvénients par rapport à un réseau sans fil. Le plus gros inconvénient est que votre appareil est connecté à un routeur. Les réseaux câblés les plus courants utilisent des câbles connectés à une extrémité à un port Ethernet sur le routeur du réseau et à l'autre extrémité à un ordinateur ou un autre périphérique

Les réseaux sans fil ont été créés pour permettre aux utilisateurs d'effectuer des communications sans utiliser les câbles de connexion.

De ce fait, nous avons assisté ces dernières années à un essor en puissances des réseaux locaux sans fil ou encore le Wi-Fi (Wireless Fidelity), qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises.

Auparavant, on pensait que les réseaux câblés étaient plus rapides et plus sûrs que les réseaux sans fil. Mais les améliorations continues apportées à la technologie de réseau sans fil, telles que la norme de réseau Wi-Fi, ont érodé les différences de vitesse et de sécurité entre les réseaux filaires et sans fil.

I.4) Réseau sans fil

I.4.1) Définition

Un réseau sans fil (en anglais Wireless network) est comme son nom l'indique 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 d'une part par la fréquence d'émission utilisée, ainsi que le débit et la portée des transmissions.

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 (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies.

Ils sont en pleine expansion du fait de la flexibilité de leur interface, ce qui permet à l'utilisateur de changer de place tout en restant connecté **[4].**

I.4.2) Techniques de transmission dans les réseaux sans fil

Il existe principalement deux méthodes pour la transmission dans les réseaux sans fil :

- **Transmission par ondes infrarouges**

La transmission par les ondes infrarouges nécessite que les appareils soient en face l'un des autres et aucun obstacle ne sépare l'émetteur du récepteur car la transmission est directionnelle. Cette technique est utilisée pour créer des petits réseaux de quelques dizaines de mètres. (Télécommande de : télévision, les jouets, etc.) .

- **Transmission par ondes radios :**

La transmission par les ondes radios est utilisée pour la création des réseaux sans fil qui a une étendue de plusieurs kilomètres. Les ondes radios ont l'avantage de ne pas être arrêtés par les obstacles car elles sont émises d'une manière omnidirectionnelle. Le problème de cette technique est les perturbations extérieures qui peuvent affecter la communication à cause de l'utilisation de la même fréquence par exemple [5].

I.4.3) 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 I.4).

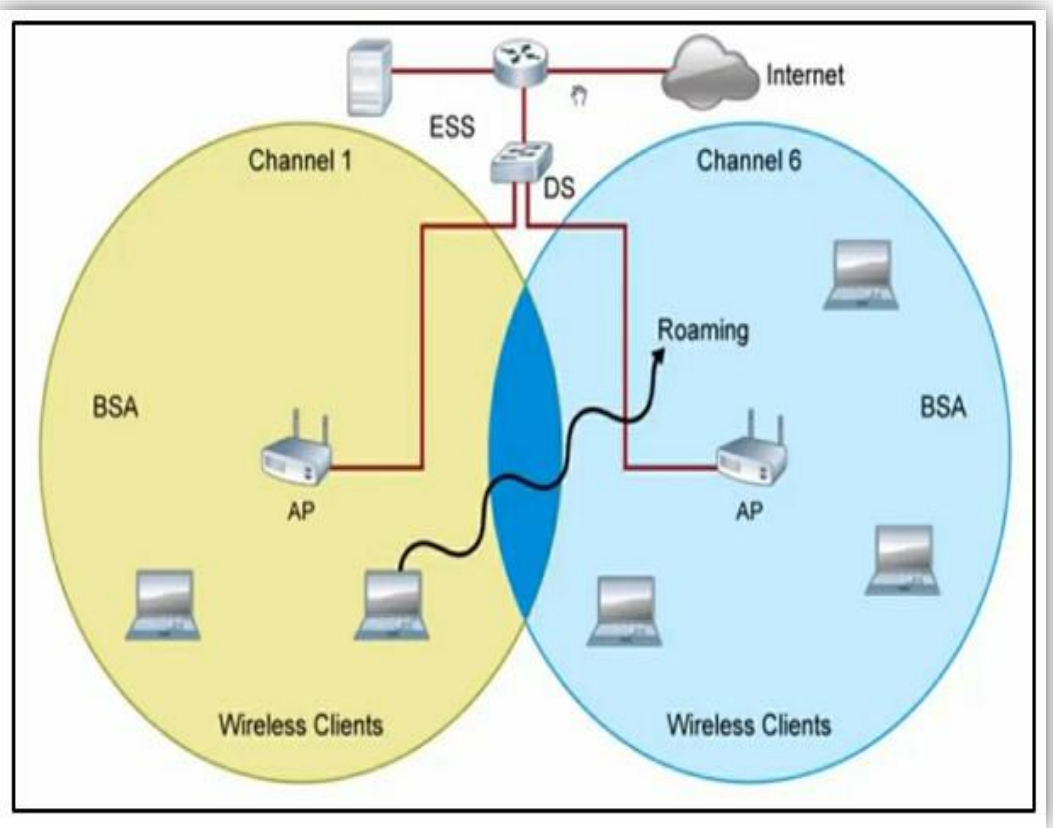


Figure I-4 – handover (Roaming) dans les WLAN

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 [2].

I.4.4) Les catégories de réseau sans fil [6]

On distingue habituellement plusieurs catégories de réseaux sans fils

I.4.4.1) Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domotique sans fils et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN comme **Bluetooth, HomeRF, ZigBee et liaisons infrarouges.**

I.4.4.2) Réseaux métropolitains sans fils (WMAN)

Le réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

I.4.4.3) Réseaux étendus sans fils (WWAN)

Le réseau étendu sans fils (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes :

- **GSM** (Global System for Mobile Communication ou Groupe Spécial Mobile)
- **GPRS** (General Packet Radio Service)
- **UMTS** (Universal Mobile Telecommunication System)
- **LTE** (Long Term Evolution)
- **WiMax** standard de réseau sans fils basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs itinérants.

I.4.4.4) Réseaux locaux sans fils (WLAN)

Le réseau local sans fils (WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture.

Il existe plusieurs technologies et la plus utilisée de nos jours c'est le WI-FI « WIRLESS-FIDELITY » ou IEEE 802.11

La tendance est à la transmission numérique et à l'utilisation de WiFi qu'il est nécessaire et plus avantageux que les autres technologies. « **C'est notre sujet à aborder ».**

I.5) Les avantages d'un réseau sans fil Wi-Fi [7]

- **Commodité** : Accédez à vos ressources réseau depuis n'importe quel endroit dans la zone de couverture de votre réseau sans fil ou depuis n'importe quel point d'accès Wi-Fi.
- **Mobilité** : Vous n'êtes pas lié à votre bureau, comme vous l'êtes avec une connexion filaire. Vous et vos employés pouvez vous connecter en ligne lors de réunions en salle de conférence, par exemple.
- **Productivité** : L'accès sans fil à Internet et aux principales applications et ressources de votre entreprise aide votre personnel à faire son travail et encourage la collaboration.
- **Installation facile** : Vous n'avez pas besoin d'enchaîner les câbles, l'installation peut donc être rapide et économique.
- **Extensibilité** : vous pouvez facilement étendre les réseaux sans fil avec l'équipement existant, alors qu'un réseau câblé peut nécessiter un câblage supplémentaire.
- **Sécurité** : Les progrès des réseaux sans fil offrent des protections de sécurité robustes.
- **Coûts réduits** : Etant donné que les réseaux sans fil éliminent ou réduisent les dépenses de câblage, ils peuvent coûter moins cher à exploiter que les réseaux câblés.

I.6) Conclusion

Dans ce chapitre, on a bien vu que lors du déploiement d'un réseau sans fil, le WiFi (802.11) semble être la solution répondant au mieux aux besoins des réseaux locaux sans fil grâce à l'avantage qu'elle procure, qui est son interopérabilité avec les réseaux de type Ethernet. Cette technologie, est fréquemment utilisée dans les entreprises désirant accueillir des utilisateurs mobiles ou souhaitant une alternative au réseau filaire tout en conservant des performances quasi identiques.

En conclusion, les réseaux sans fil en général, et le WiFi en particulier sont des technologies intéressantes et très utilisées dans de divers domaines comme l'industrie, la santé et le domaine militaire. Cette diversification d'utilisation revient aux différents avantages qu'apporte cette technologie.

chapitre II.
Technologies des réseaux Wi-Fi

Chapitre I I Technologies de réseau WiFi

II.1) **Technologies des réseaux Wi-Fi**

Le Wi-Fi est un ensemble de fréquences radio qui élimine les câbles, partage une connexion Internet et permet l'échange de données entre plusieurs postes.

II.1.1) **Historique**

En 1997, alors que l'attention est accaparée par le succès d'Internet et l'euphorie boursière montante, un événement est passé inaperçu sauf pour quelques spécialistes et observateurs : l'adoption du standard IEEE 802.11 ou Ethernet sans fil. Exploitant la bande de fréquence de 2,4 GHz, le 802.11 plafonnent à un débit de 2 Mbits/s au maximum.

Ce précurseur est suivi de plusieurs déclinaisons dont le célèbre Wi-Fi qui connaît un franc succès, aidé par le volontarisme des fabricants, distributeurs et fournisseurs de services... Wi-Fi, est un nom composé à la manière de Hi-fi et signifiant Wireless Fidelity. Il désigne les différentes déclinaisons de la norme IEEE 802.11 qui permet à plusieurs ordinateurs de communiquer sans fil en utilisant comme support les ondes radio. Les câbles disparaissent enfin. Avantage: le déploiement d'un réseau Wi-Fi est assez simple, le prix plutôt modeste en comparaison d'autres technologies. Le Wi-Fi est une technologie intéressante pour de nombreuses sociétés liées au monde des télécoms et d'Internet. Les collectivités locales et surtout les particuliers profitent de la facilité d'accès à Internet haut débit liée à cette norme. Dans sa déclinaison la plus connue, 802.11 b, le Wi-Fi utilise la bande de fréquence de 2,4 GHz et atteint un débit théorique de 11 Mbits/s (contre 128, 512 Kbits/s ou 1 Mbits/s pour l'ADSL), le 802.11a culmine à 22 Mbits/s et le 802.11 g, enfin, flirte avec les 54 Mbits/s. Le Wi-Fi peut certes servir à surfer sur Internet, mais pas seulement. Il autorise l'organisation de réseaux -pourvus ou pas d'Internet - pour échanger des fichiers, des données, et bien entendu pour jouer. Ce ne sont là que quelques exemples de ses usages possibles Les avantages des réseaux sans fil ne sont plus à démontrer surtout à une génération de plus en plus habituée à la mobilité. La multiplication des appareils (PDA, PC portables, terminaux et bientôt les téléphones portables) capables de communiquer entre eux en fait le support idéal des réseaux modernes [7].

II.1.2) **Les différentes normes WiFi**

Les normes WiFi ont évolué avec le temps et ont apporté des améliorations successives en termes de débit.

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps.

Chapitre I I Technologies de réseau WiFi

Depuis 1999, de nombreuses normes ont vu le jour et ont toutes apportées avec elles d'importantes évolutions technologiques autour du WiFi. On compte aujourd'hui 20 normes WiFi jusqu'à la norme WiFi 7.

Les normes 802.11a, 802.11b et 802.11g sont désormais clairement dépassées et la norme 802.11n est probablement la norme la plus ancienne dont certains peuvent encore disposer à l'heure actuelle. La Wi-Fi Alliance parle désormais de WiFi 1, 2, 3, 4, 5 et 6 passant des lettres aux chiffres pour les technologies normes WiFi destinées au grand public. À noter que seul les WiFi 4, 5 et 6 ont été officiellement validés mais à titre de correspondance rétroactive les normes 802.11b, 802.11a et 802.11g coïncident respectivement aux WiFi 1, 2 et 3.

La norme WiFi 802.11n fut d'ailleurs un sacré bond en avant avec des débits théoriques bien plus élevés allant jusqu'à 450Mbps sur la fréquence 5GHz. Elle coïncida avec l'arrivée de la fibre optique et permit ainsi de profiter pleinement de cette connexion à très haut débit. Certains des adaptateurs 802.11n peuvent aussi émettre sur les deux fréquences simultanément (2,4 GHz ou 5 GHz) et permettre ainsi la connexion des différents appareils sur l'une ou l'autre de celles-ci. La norme WiFi 802.11n a aussi vu l'apparition des MIMO : des antennes émettrices et réceptrices bien plus performantes que les antennes auparavant utilisées. La largeur de la bande (ou du canal) a aussi pour la première fois été étendue avec du 40MHz ce qui permit de doubler la vitesse de débit, la largeur de bande permettant de faire transiter plus de données sur le même laps de temps. Selon les modèles de routeurs 802.11n, 12 combinaisons différentes existent avec la largeur de bande à 20 ou 40MHz, de 1 à 3 antennes MIMO et les fréquences de 2,4 et 5GHz ce qui explique des débits variables entre 72,2 et 450Mbps**.**

La norme 802.11ac est arrivée en deux vagues successives et a encore amélioré les débits avec une largeur de bande jusqu'à 160MHz sur la seconde vague. La norme 802.11ac introduit aussi 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 (auparavant le signal WiFi émettait à pleine puissance dans toutes les directions).

Les technologies Massive Mimo et le Beamforming sont d'ailleurs des technologies qui sont aussi utilisées pour le développement de la 5G dans le monde.

La dernière version de la norme WiFi est la 802.11ax qui correspond au WiFi 6 et qui devrait être commercialisée fin 2019 [9].

Le Wi-Fi 7 est encore une norme à définir, qui est pour l'instant loin d'une commercialisation. De nombreuses étapes restent encore à passer pour définir les contours de cette nouvelle norme. C'est la Wi-Fi Alliance qui interviendra notamment sur ce dossier. Ensuite, il faudra que les constructeurs et fabricants de puces et appareils s'en saisissent [10].

On retrouve dans le tableau ci-dessous les évolutions les plus importantes dans l'histoire des normes WiFi :

Norme WiFi	Année de création	Débit théorique	Portée maximale	Bande de fréquence
WiFi 802.11a (WiF 1)	1999	54 Mbit/s	10 m	5 GHz
WiFi 802.11b (WiFi 2)	2000	11 Mbit/s	140 m	2.4Ghz
WiFi 802.11g (WiFi 3)	2003	54 Mbit/s	140 m	2.4 Ghz
WiFi 802.11n (WiFi 4)	2006	450 Mbit/s	250 m	2.4/5 GHZ
WiFi 802.11ac (WiFi 5)	2014	1.3Gbit/s	35 m	5 GHz
Wifi 802.11ad		7 Gbit/s	10 m	60Ghz
WiFi 802.11ax (WiFi 6)	2019	10Gbit/s	35 m	2.4/5 Ghz
Wifi 802.11 be (Wifi 7)	2022 (2024 à la grand public)	30Gbit/s		2.4/5/6 Ghz

Tableau II-1 Les différentes révisions de la norme 802.11 [11]

II.1.3) LE MATÉRIEL POUR LE DÉPLOIEMENT

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

II.1.3.1) Point d'accès

La technologie Wi-Fi a beaucoup évolué ces dernières années, mais il n'y a pas encore de solution adaptée à tous les types de structure et à toutes les tailles d'entreprises. Les grands espaces de bureaux avec un trafic de données important utilisent généralement des points d'accès Wi-Fi, tandis que les petites structures avec un nombre limité d'utilisateurs sont plus susceptibles d'utiliser des routeurs Wi-Fi et des amplificateurs de signal [12].

Un point d'accès est un appareil qui crée un réseau local sans fil, ou WLAN, habituellement dans un bureau ou dans un grand bâtiment. Un point d'accès se connecte à un routeur filaire, commutateur ou hub par câble Ethernet et délivre un signal Wi-Fi à une zone dédiée. Si vous souhaitez par exemple activer le Wi-Fi dans le hall de réception de votre entreprise, mais vous ne disposez pas d'un routeur à portée de main, vous pouvez alors installer un point d'accès près de la réception en acheminant un câble Ethernet à travers le plafond vers à la salle des serveurs [12].

II.1.3.1.1) Types courants de configuration de point d'accès

- **Point d'accès racine :**

Dans cette configuration, un point d'accès est connecté directement à un réseau local filaire pour fournir un point de connexion pour les utilisateurs sans fil. En cas de connexion de plusieurs points d'accès au réseau local, les utilisateurs peuvent utiliser leur appareil en se déplaçant d'une zone à l'autre du site sans perdre la connexion au réseau.

- **Point d'accès en mode répéteur :**

Un point d'accès ou module d'extension maillé peut être configuré en répéteur autonome pour étendre la portée de l'infrastructure ou pour éliminer les obstacles bloquant la communication radio.

Le répéteur transfère le trafic entre les utilisateurs sans fil et le réseau filaire en envoyant les données à un autre répéteur ou à un point d'accès connecté au réseau filaire. Les données sont envoyées par le chemin fournissant les meilleures performances au client.

- **Ponts :**

Les points d'accès peuvent être configurés en ponts racines ou non racines pour joindre plusieurs réseaux. Ce mode de point d'accès permet d'établir une liaison sans fil avec un pont non racine. Le trafic est ensuite transmis par la liaison sans fil vers le réseau filaire.

- **Pont pour équipe de travail :**

Les points d'accès en mode pont pour équipe de travail peuvent « s'associer » à d'autres points d'accès et fournir des connexions réseau aux appareils connectés aux ports Ethernet. Par exemple, si votre entreprise nécessite une connectivité sans fil pour un groupe d'imprimantes en réseau, vous pouvez connecter les imprimantes à un concentrateur ou à un commutateur, connecter ce dernier au port Ethernet du point d'accès et configurer le point d'accès en pont pour équipe de travail. Le pont pour équipe de travail « s'associera » ensuite à un point d'accès sur votre réseau.

- **Unité centrale dans un réseau sans fil**

Pour un réseau sans fil, un point d'accès fait office d'unité racine autonome. Il n'est pas branché à un réseau local filaire. Le point d'accès agit plutôt en tant que concentrateur pour permettre l'interconnexion de tous les postes. Il sert de point focal pour les communications, en augmentant la portée de la communication des utilisateurs sans fil.

II.1.3.1.2) **Principaux avantages de la mise à niveau vers les AP :**

Les AP constituent une alternative plus pratique, plus sécurisée et plus économique par rapport aux câbles et aux fils pour connecter chaque ordinateur ou appareil sur votre réseau. Utiliser des WAP pour configurer un réseau sans fil peut également fournir de nombreux avantages et bénéfices pour votre petite entreprise.

Premièrement, l'accès au réseau sans fil est plus pratique. L'ajout d'utilisateurs est également moins complexe. Puis, vous pouvez facilement fournir un accès Internet aux utilisateurs invités en leur donnant un mot de passe pour accéder à votre réseau sans fil en toute sécurité.

Vous pouvez également facilement segmenter les utilisateurs, y compris les invités pour mieux protéger les ressources et les actifs de votre réseau.

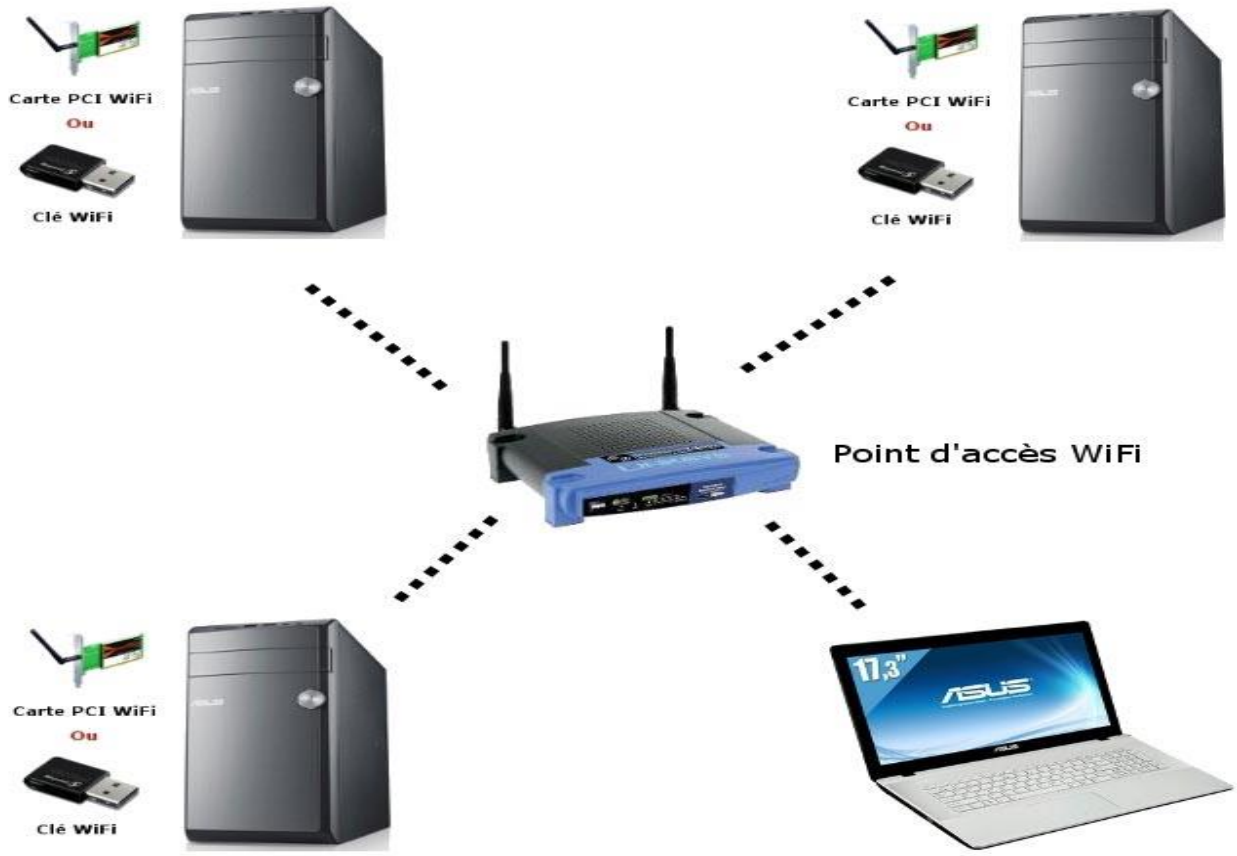


Figure II-1. Exemple raccords d'un point d'accès

II.1.3.2) Les Contrôleurs LAN sans fil (WLC) [13]

Avec la demande croissante d'accès Wi-Fi, de plus en plus de points d'accès sans fil (AP) sont déployés dans les réseaux pour assurer une couverture complète du signal dans les bâtiments des entreprises ou sur les campus, ce qui complique les opérations de maintenance pour les administrateurs.

Les contrôleurs d'accès sans fil (WLC) ont été créés pour éliminer ce goulot d'étranglement en contrôlant et gérant ces points d'accès multiples. Le point d'accès sans fil perd ainsi sa capacité de dispositif intelligent, tandis que le contrôleur d'accès sans fil devient le nouveau "cerveau" de l'ensemble du WLAN.

Un contrôleur de réseau local sans fil, ou contrôleur WLAN, surveille et gère les points d'accès sans fil en masse et permet aux appareils sans fil de se connecter au WLAN. En tant que dispositif centralisé, le contrôleur de réseau local sans fil est généralement situé au centre de

données, auquel tous les points d'accès sans fil du réseau sont directement ou indirectement connectés.

II.1.3.2.1) **Fonctionnement d’un contrôleur de réseau local sans fil**

Le contrôleur d'accès sans fil prend la bande passante qui provient d'un routeur et l'étend pour l'adapter aux besoins du réseau. Semblable à un amplificateur dans une chaîne stéréo, le contrôleur sans fil permet de connecter des appareils situés à des distances plus éloignées. Il permet également aux administrateurs de réseau de vérifier toutes les données relatives au réseau et est capable de détecter les points d'accès non autorisés et les problèmes récents générés.

II.1.3.2.2) **Objectif d’utilisation des contrôleurs de réseau local sans fil**

Lors du déploiement d’un WLAN d'entreprise, chaque point d'accès sans fil est initialement configuré et géré indépendamment des autres points d'accès sur le même réseau. C'est-à-dire que chaque AP doit fonctionner individuellement, ce qui rend une gestion centralisée difficile à obtenir. Pire encore, ces points d‘accès ne peuvent pas communiquer entre eux, ce qui provoque des problèmes techniques et finit par rendre les conditions du réseau instables. Contrairement à la solution traditionnelle, sans contrôleur d’accès, l'adoption de contrôleurs LAN sans fil lors de la mise en réseau permettra de résoudre une fois pour toutes les problèmes mentionnés ci-dessus. Accompagnés de points d‘accès en mode léger, les contrôleurs de réseau local sans fil peuvent aider à réaliser une gestion efficace et simplifiée du réseau.

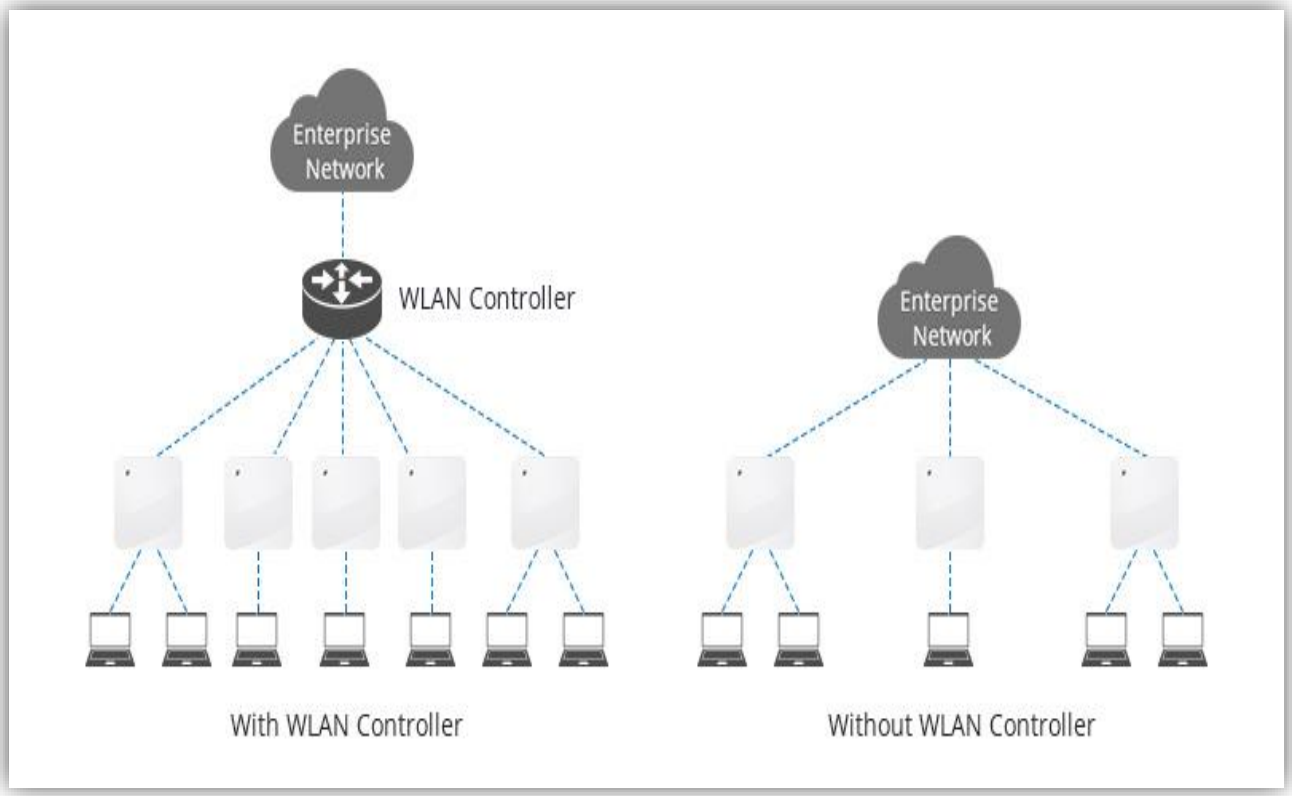


Figure II-2 Exemple de schéma de réseau avec WLC et sans WLC

II.1.3.2.3) **Les avantages d'utiliser un contrôleur de réseau local sans fil**

- Réseau câblé et sans fil sécurisé: Contrôle des privilèges d'accès des utilisateurs de réseaux sans fil à l'aide de divers critères (méthode d'authentification, type de dispositif, application demandée, etc.) afin de fournir un accès personnalisé pour maintenir la sécurité. Au lieu de stopper le cryptage au niveau du point d'accès, il permet de maintenir le trafic WLAN totalement isolé jusqu'à son passage à travers un pare-feu au niveau du contrôleur d'accès sans fil. Il détecte et bloque les points d'accès non autorisés pour empêcher toute connectivité sans fil indésirable dans le réseau. Les contrôleurs WLAN, littéralement, "verrouillent les airs".
- Gestion centralisée et flexible du réseau: Un contrôleur sans fil centralisé offre une certaine flexibilité pour le déploiement, ce qui permet de réduire les coûts, l'utilisation d'outils et le temps de mise en place.Il permet une surveillance centralisée de l'ensemble de l'infrastructure sans fil, ce qui réduit les coûts de propriété et facilite la convergence des accès câblés et sans fil, un investissement de mise à niveau durable.
- Maintenance simplifiée du réseau: Les contrôleurs de réseau local sans fil éliminent les sondages sur site en incluant un logiciel de planification RF (Fréquences Radio) intelligent. Le réseau sans fil avec auto-configuration et autoréparation est meilleur pour la gestion et le dépannage. Il peut

localiser et identifier avec précision chaque utilisateur. En raison de la caractéristique des fréquences radio, le contrôleur d'accès sans fil peut facilement détecter les interférences entre les points d'accès voisins et reconfigurer automatiquement leurs paramètres de puissance et de canal. Si un point d'accès tombe en panne, celui-ci peut ordonner aux points d'accès voisins d'augmenter leurs niveaux de puissance pour combler le déficit de couverture.

II.1.4) **Architecture**

II.1.4.1) Mode de fonctionnement

La norme Wi-Fi définit deux modes opératoires:

II.1.4.1.1) **Le mode Infrastructure**

Un réseau 802.11 est un ensemble de cellules de base (BSS). Chaque cellule BSS comporte un point d'accès matérialisé par un dispositif d'émission/réception. Les cellules sont reliées par une infrastructure de communication fixe et interconnectées par un système de distribution afin de former un ESS.

Cette infrastructure incorpore un portail permettant d'assurer l'interface avec un réseau local.

Chaque BSS est identifiée par un BSSID. Dans le mode infrastructure, le BSSID correspond à l'adresse physique (adresse MAC) du point d'accès.

II.1.4.1.2) **Le mode Ad Hoc**

Ce mode représente un ensemble de stations 802.11 qui communiquent entre elles sans avoir recours à un point d'accès. Chaque station peut établir une communication avec n'importe quelle autre station dans la cellule que l'on appelle cellule indépendante.

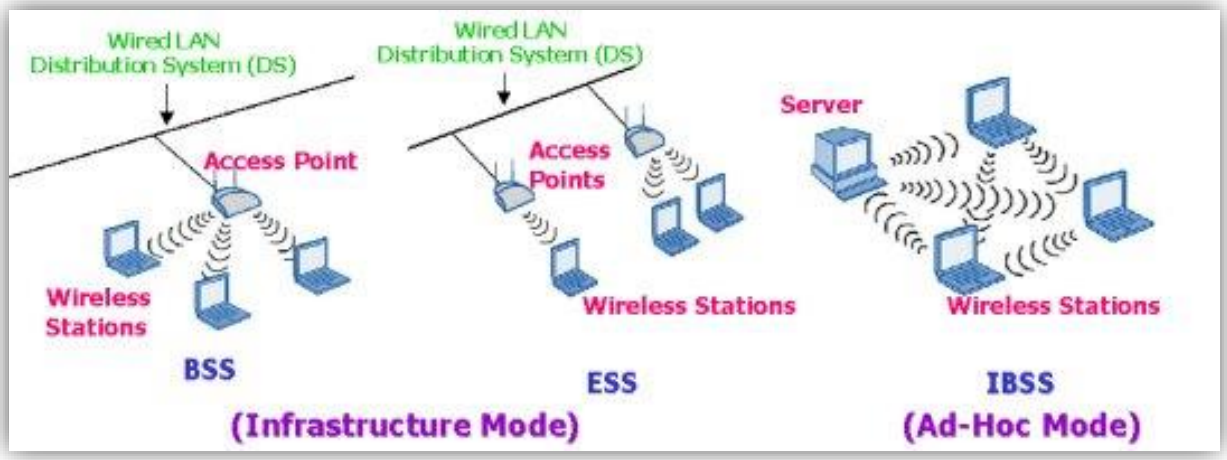


Figure II-3 Exemple d'une installation en mode infrastructure et mode ad hoc

Dans les deux modes infrastructure et ad hoc, chaque réseau de service est identifié par un identificateur de réseau SSID. Par conséquent, toute station désirant se connecter à un réseau de service particulier doit connaître au préalable la valeur de son SSID [14].

Ces deux modes précédents peuvent se diviser en trois configurations différentes [15] :

- « Independant Basic Service Set » (IBSS).
- « Basic Service Set » (BSS).
- « Extended Service Set » (ESS).

Le mode d'opération IBSS n'utilise pas de point d'accès et n'est constitué que d'équipements clients qui communiquent entre eux sans aucune fonction de contrôle, de gestion de la sécurité ou de statistique centralisée.

Réseau IBSS	
Avantages	Inconvénients
Facile à configurer	Fréquences radio limitées
Aucun oint d'accès	Pas de gestion centralisée
	Pas de gestion centralisée
	Pas évolutif
	Difficile à sécuriser

Tableau II-2 Avantage et inconvénients réseau IBSS

Le mode d'opération BSS est la base du réseau sans fil. Il est constitué d'un point d'accès connecté à l'infrastructure réseau appelée « Distribution System » (DS) et des clients sans fil qui lui sont associés. La zone de couverture RF, appelée « Basic Service Area » (BSA), dépend de plusieurs facteurs tels que le gain de l'antenne et les réglages de puissance RF.

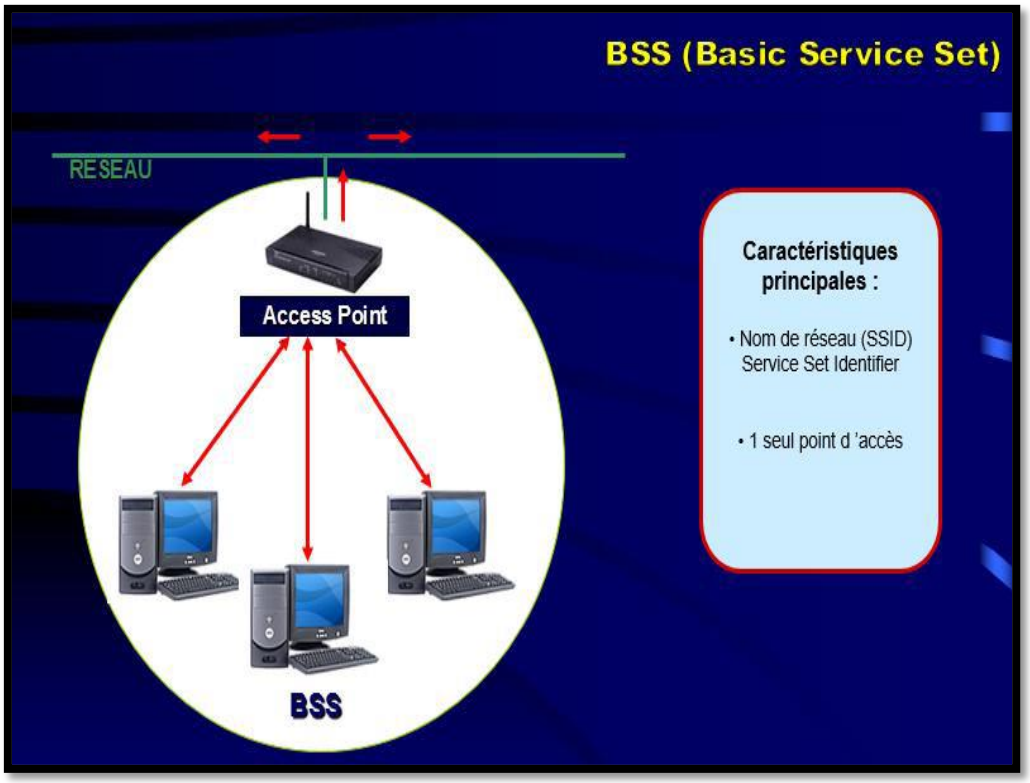


Figure II-4 Le mode d'opération BSS[16]

Réseau BSS	
Avantages	Inconvénients
Points d'accès intelligents	Matériels à rajouter par rapport à l'IBSS
Utile pour le domicile, le SOHO et de la petite à la grande entreprise	Peut nécessiter une étude de site pour déterminer la couverture et la capacité
Évolutif	Doit être connecté à un DS qu'il soit filaire ou sans fil
Gestion et contrôle centralisés	Nécessite des compétences complémentaires pour configurer et déployer
Sécurité pouvant être centralisée	

Tableau II-3 avantage et inconvénients réseau BSS

Un ESS est un ensemble de BSS interconnectés qui apparaissent comme un seul BSS pour la couche « Logical Link Control » (LLC) d'une « Station » (STA) associée à l'un de ces BSS. Ce mode d'opération est très répandu dans les déploiements en entreprise. Tous les BSS doivent posséder des paramètres en commun, tels que le SSID et les paramètres de sécurité. Dans la majorité des cas, les BSA de chaque BSS se recouvrent pour permettre le « roaming » d'un BSS à un autre.

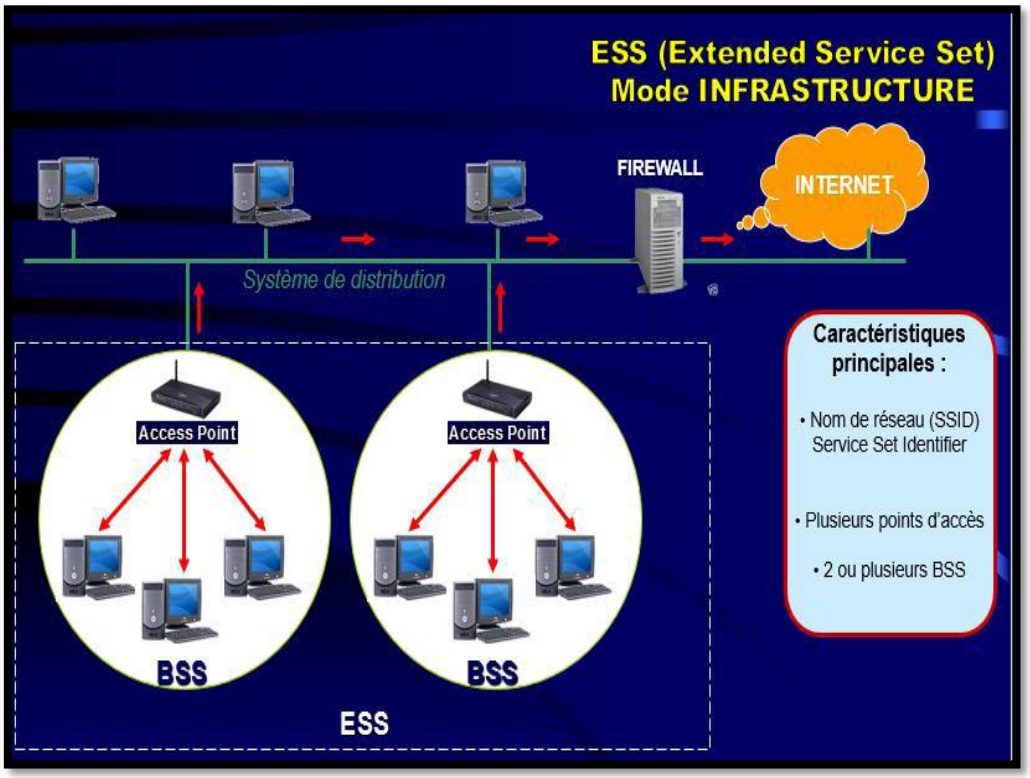


Figure II-5. Exemple ESS [16]

II.1.4.2) Les couches de L'EEE802.11

Comme tous les standards de l'IEEE, 802.11 couvre les deux premières couches du modèle de référence OSI. L'une de ses caractéristiques essentielles est qu'il définit une couche MAC commune à toutes les couches physiques. De la sorte, de futures couches physiques pourront être ajoutées sans qu'il soit nécessaire de modifier la couche MAC.

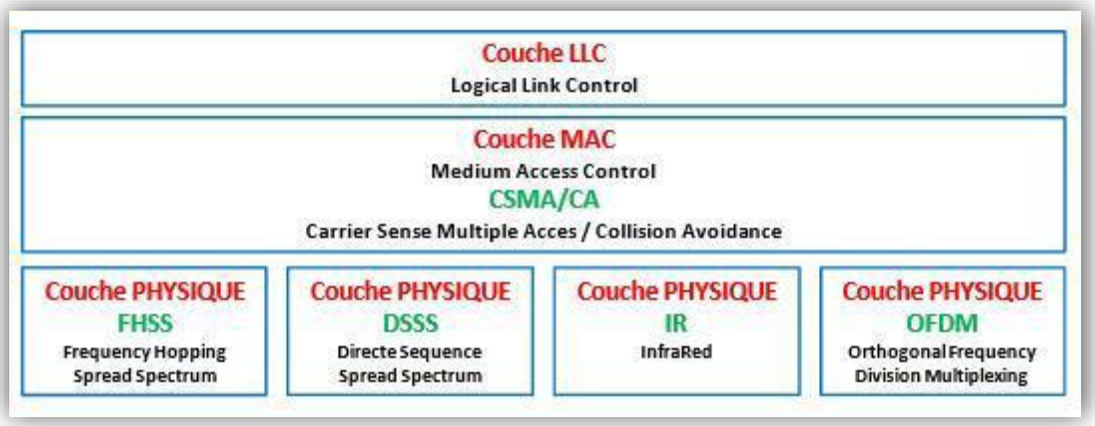


Figure II-6. Description des couches IEEE 802.11 [14]

II.1.4.2.1) **La couche physique**

Le rôle de la couche physique est de transmettre correctement la séquence de 0 ou de 1 que l'émetteur souhaite envoyer au récepteur. Il est divisé en deux sous-couches, PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent).

La sous-couche PMD est responsable du codage des données, tandis que la sous-couche PLCP est responsable de l'écoute du support. Il fournit pour cela CCA (Clear Channel Assessment), qui est un signal utilisé par la couche MAC pour savoir si le support est occupé.

IEEE 802.11 définit quatre couches physiques différentes :

• FHSS (Frequency Hopping Spread Spectrum).

• DSSS (spectre étalé à séquence directe).

• IR (infrarouge).

• OFDM (Multiplexage par répartition orthogonale de la fréquence).

Le FHSS et le DSSS utilisent la bande des 2,4 GHz de l'ISM (Industrial, Scientific, and Medical. L'infrarouge n'est utilisé que dans les cas où les distances entre les différentes stations sont faibles.

La quatrième couche physique a été définie dans la bande des 5,2 GHz. Grâce au codage OFDM, des débits compris entre 6 et 54 Mbit/s peuvent être atteints. 802.11 est le premier standard à utiliser un codage OFDM pour une communication de type paquet.Cette technologie était jusqu'à présent utilisée pour des systèmes de transmission de données continues, tels que DVB (Digital Video Broadcasting) ou DAB (Digital Audio Broadcasting).

Pour qu'un signal soit reçu correctement, sa portée ne peut dépasser 150 m dans un environnement de bureau, 600 m sans obstacle et 1,5 km avec une antenne extérieure. En règle générale, les stations ont une portée maximale de 50 m. Lorsqu'il y a traversée de murs, cette distance est souvent plus restrictive [1].

II.1.4.2.2) 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 de 802.11. Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, 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 terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

• Procédures d'allocation du support ;

• Adressage des paquets ;

• Formatage des trames ;

• Contrôle d'erreur CRC (Cyclic Redundancy Check) ;

• Fragmentation-réassemblage.

II.1.4.3) Méthode d'accès [16]

La couche MAC définit deux méthodes d'accès différentes :

• La méthode CSMA/CA utilisant la Distributed Coordination Function (DCF)

• La Point Coordination Function (PCF).

II.1.4.3.1) La méthode d'accès CSMA/CA

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le CSMA/CD (Carrier Sense Multiple Access with Collision Detect), pour lequel chaque machine est libre de communiquer à n'importe quel moment. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.

Dans un environnement sans fil, ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur

rayon de portée. Ainsi la norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur :

la station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre. La station transmet un message appelé Ready To Send (noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.

Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant Le champ est libre pour émettre), puis la station commence l'émission des données.

A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elles considèrent être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

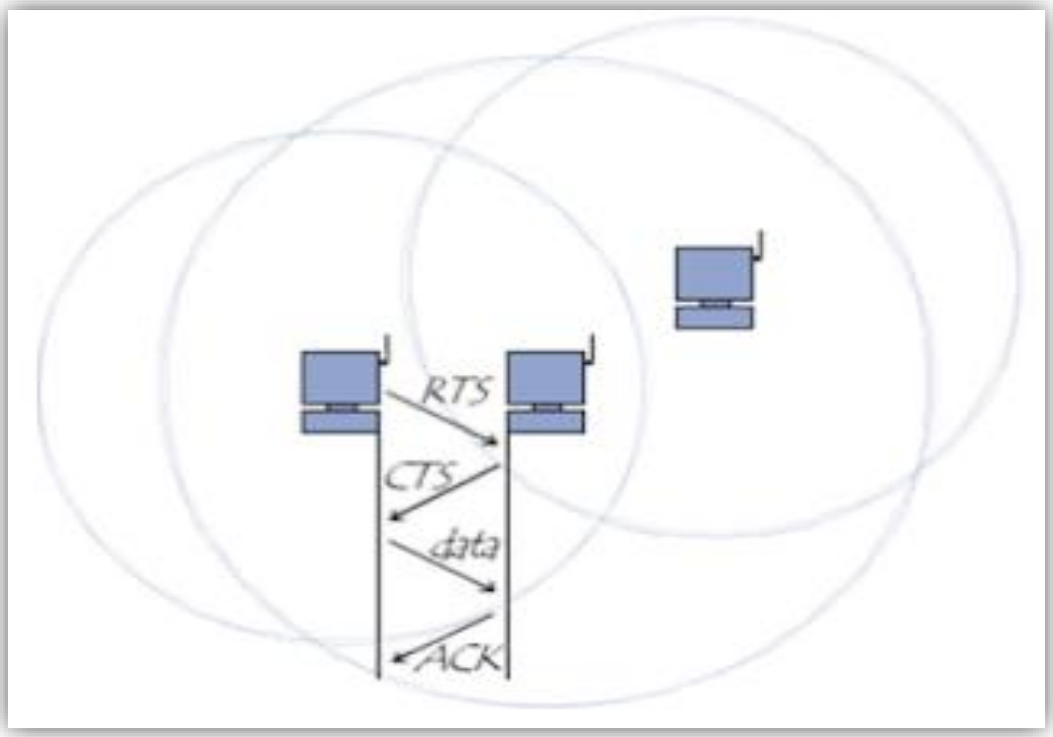


Figure II-7. Schéma de la méthode d'accès CSMA/CA

II.1.4.3.2) **Point Coordination Function (PCF)**

En plus de la fonction de base de coordination distribuée (DCF), il y a la fonction optimale de coordination par point (PCF) qui peut être utilisée pour implémenter des services temps réel, comme la transmission de voix ou de vidéo.

Cette PCF fait qu'on utilise des priorités supérieures que le point d'accès peut gagner en utilisant des temps inter-trames plus petits (PIFS).

En utilisant un accès par priorité supérieure, le point d'accès peut envoyer des données aux stations en réponse à une Polling Request, tout en contrôlant l'accès au support. Pour permettre aux stations classiques d'avoir accès au support, il y a une condition qui est que le Point d'Accès doit laisser suffisamment de temps DCF par rapport au PCF.

chapitre III. **Les mécanismes de sécurité du réseau WiFi**

III.1) **Introduction**

Malgré tous ces avantages de l'utilisation de WiFi et toute cette importance à donner, il y a des failles en sécurité qui rend ce dernier moins sécurisé et non fiable .C'est pour cela, on va étudier et détailler dans ce chapitre les mécanismes et les protocoles de sécurité pour trouver des meilleur solutions et améliorer cette sécurité pour avoir une bonne qualité de service de réseau avec moins de risque.

III.2) **Généralités sur la sécurité**

III.2.1) **Les objectifs de base de la sécurité**

Garantir la sécurité Wi-Fi est essentiel dans les réseaux sans fil en raison des caractéristiques décrites ci-dessus. Cependant, selon les objectifs de sécurité, il est possible de protéger plus ou moins le réseau. La sécurité informatique totale n'existe pas, il faut parler plus modestement de niveau de sécurité. Avec la technologie Wi-Fi, le niveau de sécurité par défaut est généralement faible. Il est donc nécessaire de l'augmenter lors de l'installation. La sécurité d'un réseau sans fil repose sur ces éléments fondamentaux :

- **Confidentialité :**

Elle vise à assurer que seuls les sujets (les personnes, les machines ou les logiciels) autorisés aient accès aux ressources et aux informations auxquelles ils ont droit. La confidentialité a pour objectif d'empêcher que des informations secrètes soient divulguées à des sujets non autorisés.

- **Intégrité :**

L'intégrité vise à assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des sujets non autorisés.

L'objectif des attaques sur l'intégrité est de changer, d'ajouter ou de supprimer des informations ou des ressources.

- **Authenticité :**

L'authenticité est l'assurance qu'un message, un ordre ou une information provient bien de la source (une personne, une machine, ou un programme) dont il prétend venir. L'authenticité induit une preuve d'identité, elle est vérifiée à travers le processus d'authentification ou de signature.

- **Disponibilité :**

La disponibilité vise à assurer que le système soit bien prêt à l'emploi, que les ressources et les informations soient en quelque sorte consommables, que les ressources ne soient pas saturées, que les informations, les services soient accessibles et que l'accès au système par des sujets non autorisés soit prohibé. L'objectif des attaques sur la disponibilité est de rendre le système inexploitable ou inutilisable.

- **Non-répudiation :**

Le service de non-répudiation consiste à prévenir le refus, le démenti qu'un message ait été émis ou reçu ou qu'une action, transaction ait eu lieu. Cela permet de prouver par exemple qu'une entité est liée à une action ou à un événement.

La non-répudiation est basée sur une signature unique ou sur une identification qui prouve qui a créé le message. Pour assurer ce service, on peut faire appel à un algorithme de chiffrement à clé publique.

- **Traçabilité :**

C'est Un fonction qui consiste à repérer l'histoire des entités et leur mouvement. La traçabilité peut localiser par intermittence la position d'une personne ou d'un objet, peut dater des transactions, peut noter des renseignements sur des situations, le tout avec des attributs de sécurité. Cette fonction s'avère irremplaçable pour contrôler un objet, pour pister un suspect ou pour reconstituer un scénario lors d'une enquête informatique

III.2.2) **Les risque en matière de sécurité [17]**

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

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

III.2.2.1) L'interception de données

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

III.2.2.2) L'intrusion réseau

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

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

III.2.2.3) Le brouillage radio

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

III.2.2.4) Les dénis de service

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connus, il est facile pour un pirate d'envoyer des paquets demandant de dissocier la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

III.2.3) Les attaques d'un réseau Wi-Fi

III.2.3.1) C'est quoi une attaque ?

Une attaque est l'exploitation d'une faille d'un système informatique soit un système d'exploitation, un logiciel pour des fins non connues par l'exploitant du système .Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Afin d'empêcher ces attaques il est indispensable de connaître les principaux types d'attaques pour mettre en œuvre des dispositions préventives.

III.2.3.2) Motivation et objectif de l'attaquant

Les motivations des agresseurs, souvent qualifiés de « pirates », peuvent être multiples :

- Attrait interdit, désir d'argent (par exemple, violation du système bancaire), besoin d'argent.
- Renommée (pour impressionner des amis) ou désir de nuire (pour détruire des données, empêcher le système de fonctionner).
- Les pirates peuvent être des employés malveillants, des journalistes, des concurrents (espions de l'industrie), la police ou les services de renseignement de l'État, les terroristes ou juste des criminels solitaires.

Le but de l'attaquant est généralement de prendre le contrôle d'une machine afin de pouvoir exécuter l'action qu'ils souhaitent. Pour cela, il existe différents types de moyens :

- Obtenez des informations utiles pour attaquer

- Exploitation des failles du système

- Utiliser la force pour perturber le système

III.2.3.3) Différentes attaques d'un réseau Wi-Fi

III.2.3.3.1) 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.

III.2.3.3.2) 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.

III.2.3.3.3) 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 [18].

III.2.3.3.4) 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 œuvre l'intrusion est triviale, il suffit de s'associer à l'un des points d'accès du réseau [18].

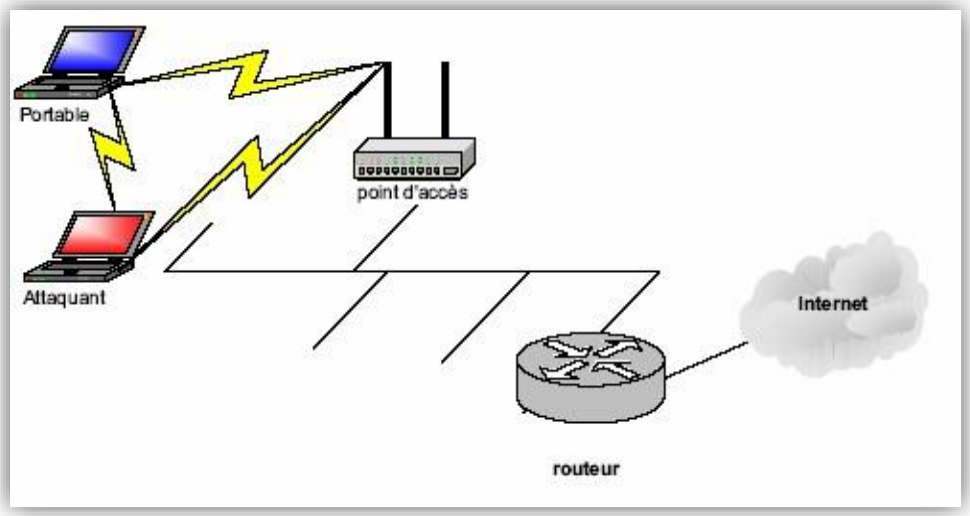


Figure III-1.L'attaque de l'intrusion

III.2.3.3.5) **Attaque de dictionnaire [19]**

Pour la première option, le pirate doit parvenir à tromper le mécanisme d'identification, il suffit de trouver le mot de passe valable soit dans un échange 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 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.
- **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 [19].

III.2.3.3.6) **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 [18].

III.2.3.3.7) **L'espionnage (sniffing)**

C'est 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.

III.3) Les mécanismes de cryptographie

III.3.1) Cryptographie (chiffrement)

La cryptographie consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelée clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire. La cryptanalyse consiste à déchiffrer un texte codé en l'effectuant sur ce texte avec une clé. Il existe trois méthodes de cryptographie : à clé symétrique, à clé asymétrique (ou clé publique), à clé mixte (utilisation des deux précédentes).

III.3.1.1) Chiffrement symétrique ou à clé secrète

- **Clé symétrique** : L'expéditeur et le destinataire utilisent la même clé (pour le codage et le décodage), toutes les personnes voulant se transmettre des données doivent partager la même clé. Les algorithmes utilisant ce système sont rapides et fiables, par contre la faille de ce système réside dans la transmission de cette clé partagée.
    - Types d'algorithmes à clé symétriques :
        - DES (Data Encryption Standard) : a été le plus utilisé, mais n'est plus utilisé depuis 1998 considéré peu sûr. Clé de 40 à 56 bits.

- IDEA (International Data Encryption Algorithm) : est utilisé par PGP (Pretty Good Privacy), le logiciel de cryptographie le plus utilisé au monde. Clé de 128 bits.
- Série RC (Ron's Code) RC2 à RC 6 : algorithme développé par Ron Rivest, la version RC4 est utilisé dans le protocole WEP d'IEEE 802.11.
- AES (Advanced Encryption Standard) : remplaçant du DES dans l'administration américaine et du RC4 dans la norme 802.11 avec 802.11i. Fondé sur l'algorithme de Rijndael, est considéré comme étant incassable.

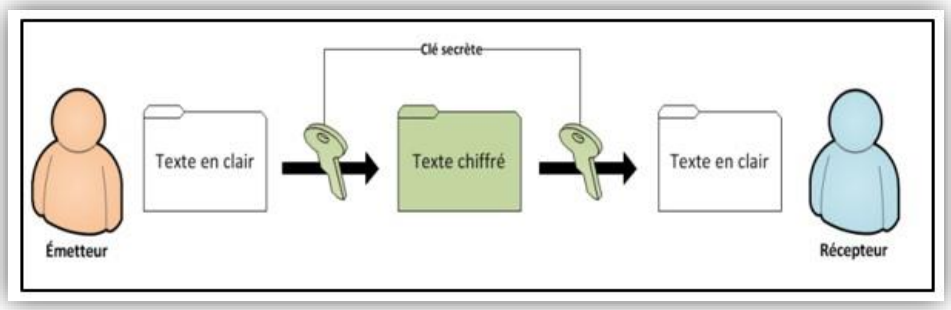


Figure III-2 Chiffrement Symétrique

III.3.1.2) Chiffrement asymétrique ou à clé publique

III.3.1.2.1) Clé asymétrique ou clé publique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire; l'autre est publique et donc accessible par tout le monde.

Les clés publiques et privées sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés sont générées en même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Il est plus lent que la plupart des cryptages à clé privée mais il reste préférable pour 3 raisons :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Permet de signer le message donc garantir l'authentification et le non répudiation

- Supporte les signatures numériques.

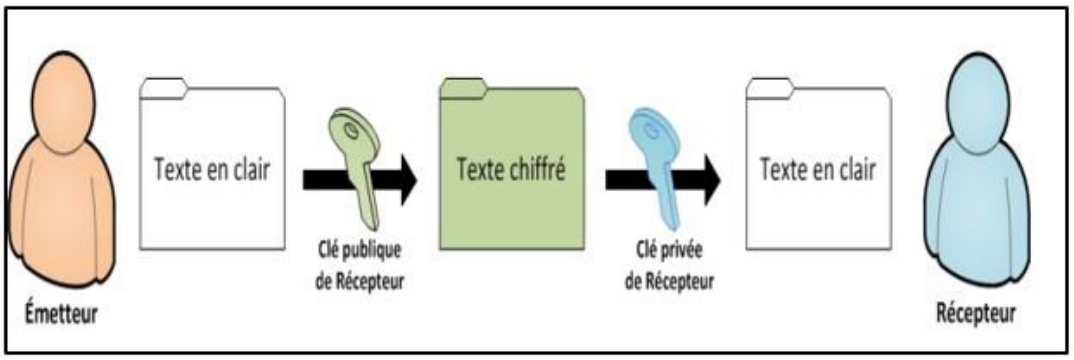


Figure III-3. Chiffrement asymétrique

Finalement comme nous avons pu le voir précédemment, les deux systèmes de base de la cryptographie souffrent de problèmes complémentaires. Ainsi l'intérêt pour augmenter la sécurité des systèmes de cryptage passe certainement par l'utilisation combinée de ces deux techniques, ce que l'on nomme la cryptographie mixte.

III.3.1.3) Clé mixte

Ce principe fait appel aux deux techniques précédentes, à clé symétrique et à clé publique, combinant les avantages des deux tout en évitant leurs inconvénients. Le principe général consiste à effectuer le chiffrement des données avec des clés symétriques, mais en ayant effectué au départ l'envoi de la clé symétrique par un algorithme à clé publique.

III.3.2) **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.

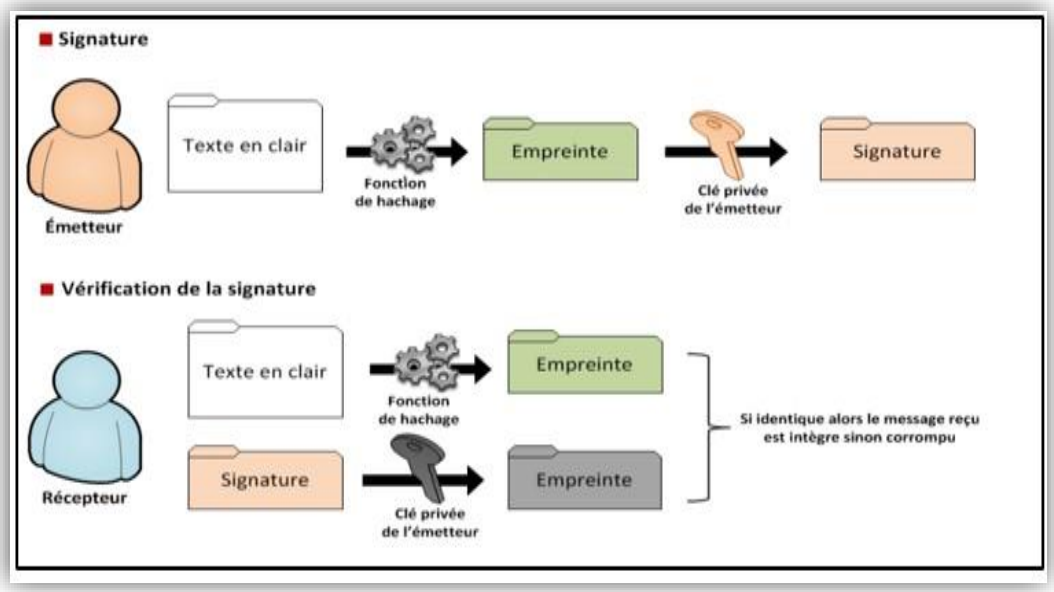


Figure III-4 – Signature numérique

III.3.3) **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 **[20].**

III.4) **Différentes solutions de sécurité réseau WiFi :**

III.4.1) **Sécurités des points d'accès**

III.4.1.1) **Une infrastructure adaptée**

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir et de configurer leur puissance de manière à limiter la propagation du signal dans des zones publiques. Le contrôle du réseau dans sa globalité permettra également de détecter les déploiements pirates.

III.4.1.2) **Eviter les valeurs par défaut**

Les configurations par défaut des équipements Wi -Fi sont d'une manière générale très peu sécurisées et dont les pirates peuvent avoir accès plus facilement. Le changement de cette

configuration est l'une des étapes essentielles dans la sécurisation d'un réseau sans fil. Pour cela il est nécessaire de :

- **Changer les mots de passe administrateurs :** Les mots de passe par défaut des points d'accès sont connus de tous, souvent, il n'y en a même pas. Il faut le modifier dès que le point d'accès est sous tension par un mot de passe plus fort. Bien entendu, le choix du mot de passe doit respecter les règles élémentaires de sécurité, c'est-à-dire au moins huit caractères de type alphanumérique et il ne doit pas être issu d'un dictionnaire (car c'est plus facile à deviner).
- **Changer le nom du réseau (SSID)** : Tout réseau Wi-Fi a un nom (le SSID), changer et cacher ce dernier à la vue des utilisateurs malintentionnés est une bonne pratique, et cela se fait comme suit :
- Eviter l'utilisation d'un SSID trop simple.
- Désactiver la diffusion automatique «broadcast» du nom SSID du réseau sans fil en cochant la case du type «disable SSID», pour qu'il n'apparaisse pas dans la liste des connexions possibles.

III.4.1.3) Le filtrage des adresses MAC

Chaque équipement informatique possède une adresse physique qui lui est propre, appelée adresse MAC (Media Access Control). C'est un identifiant matériel unique inscrit dans chaque carte réseau. Contrairement à une adresse IP qui peut changer, l'adresse MAC est définie une fois pour toute en usine par le fabricant de la carte. Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. (Ex. 44-6F-D5-00-A 1).

Le filtrage par adresse MAC est une fonctionnalité de sécurité que l'on trouve dans certains points d'accès, elle est basée sur la technique **ACL** (Access Control List), elle consiste à utiliser des listes d'accès. En effet, chaque point d'accès dispose d'une liste où sont inscrites toutes les adresses MAC des stations mobiles autorisées à l'accès. Le point d'accès procède alors à un filtrage sur la base des adresses MAC répertoriées. Chaque liste doit être continuellement mise à jour, manuellement ou par un logiciel spécialisé, afin d'ajouter ou de supprimer des utilisateurs.

Cette précaution, un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines, mais il ne faut pas compter dessus pour arrêter un pirate déterminer. Il existe, bien évidemment, des techniques permettant d'usurper une adresse MAC et ainsi de pouvoir se

connecter au point d'accès. Elle est aussi, assez difficile à mettre en œuvre pour les réseaux d'une grande taille où l'administrateur doit au minimum saisir toutes les adresses MAC autorisées dans un fichier de référence. [21].

III.4.2) **Etude des protocoles de sécurité liés aux Wi-Fi**

De nombreuses évaluations protocolaires ont rythmé la sécurité des réseaux WiFi. Les objectifs sont les suivants :

- Assurer la confidentialité des données.
- Permettre l'authentification des clients.
- Garantir l'intégrité des données.

III.4.2.1) Le protocole WEP (Wired Equivalent Privacy)

III.4.2.1.1) Qu'est ce que le WEP ? [22]

Le protocole WEP (Wired Equivalent Privacy) fait partie de la norme internationale IEEE 802.11 ratifiée en septembre 1999 .Il constitue le premier mécanisme de chiffrement mis en place dans un réseau sans fil pour assurer la sécurité des échanges radio.

Le protocole WEP protège le corps principal de la trame de données transmise sur la base de la clé K partagée entre les différentes parties communicantes.

Le principe du protocole WEP est d'utiliser l'algorithme RC4, un algorithme de chiffrement en mode flux. Ainsi, à partir d'une clé (PSK) de longueur comprise entre 40 et 104 bits (une version améliorée de WEP) et d'un vecteur d'initialisation (IV) 24 bits transmis en clair dans chaque paquet, WEP génère un flux de clé nommé KeyStream (Ks) (séquence d'octets pseudo-aléatoire). Cette série d'octets est utilisée pour chiffrer le message M en effectuant un ou exclusif (XOR) bit à bit entre Ks et M :

$$\mathbf{C = Ks \bullet XOR\ M}$$

Équation III-1 equation de chifferemet

, où C est le message chiffré.

III.4.2.1.2) Présentation de l'algorithme RC4 et PSK

- RC4 :

RC4 est un algorithme de chiffrement symétrique par flot (à la volée) utilisant le mode OFB (Output Feedback). Cette méthode est extrêmement rapide, 10 fois plus que DES. De plus, les S

Boxes évoluent avec l'exécution : le même bit ne donne pas toujours le même résultat. RC4 est donc très efficace.

RC4 est un algorithme de génération de bits pseudo aléatoires. Il permet, à partir d'une clé secrète d'obtenir une séquence binaire aléatoire et unique de même longueur du texte clair. Ensuite, il procède à faire un XOR bit par bit pour obtenir la forme chiffrée.

Le destinataire va faire un XOR entre la séquence reçue et la séquence aléatoire originale pour retrouver le message en clair [23].

- **Une clé pré-partagée (PSK – Pre-shared key)** :

  Est une clé secrète partagée qui était auparavant partagé entre les deux parties en utilisant un canal sécurisé avant de devoir être utilisé.

La Figure III.5 montre le mécanisme de chiffrement :

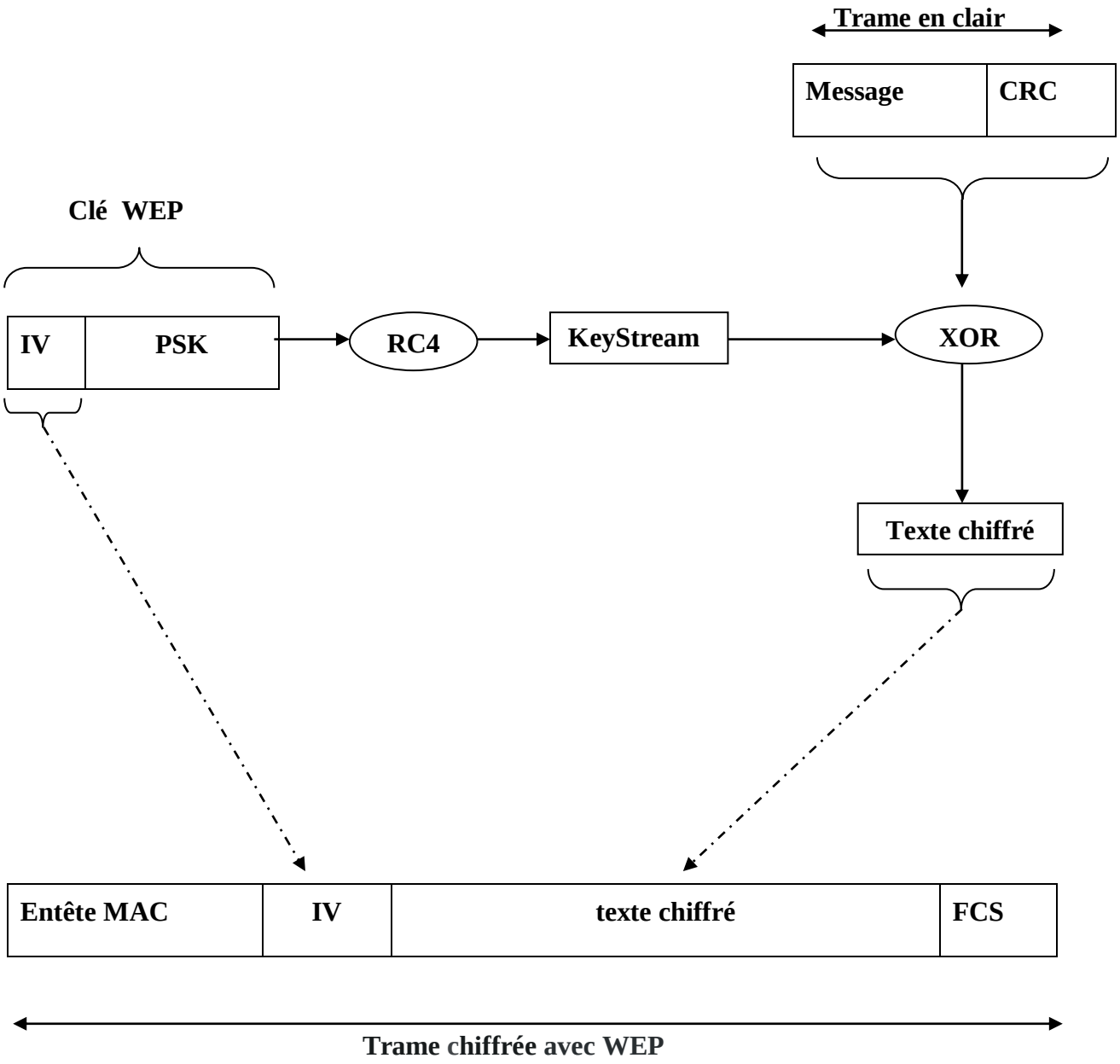


Figure III-5 .Le chiffrement WEP

III.4.2.1.3) **Les failles du WEP**

Les principales failles du WEP sont essentiellement les suivantes :

- Les algorithmes de vérification d'intégrité et d'authentification sont très facilement contournables.

- Possibilité de construire des dictionnaires fournissant en fonction d'un IV, le keystream.

- L'algorithme de chiffrement RC4 présente des clés faibles et l'espace disponible pour les IV est trop petit.

- Une même clé est utilisée pour tout le réseau et les clés de chiffrement sont statiques.

- Clés courtes 40 bits (5 caractères) ou 104 bits et/ou trop simples (attaque par dictionnaire).

III.4.2.2) Le protocole WPA (Wi-Fi Protected Access) [24]

WPA a été proposé en Octobre 2002 en réponse aux failles mises à jour dans WEP. C'est une version « allégée » du protocole 802.11i, reposant sur des protocoles d'authentification et un algorithme de cryptage robuste, TKIP (Temporary Key Integrity Protocol).

Ces propriétés sont :

- **Authentification :**Deux modes de fonctionnements existent :
  - WPA est conçu pour fonctionner avec un serveur d'authentification 802.1X (un serveur radius en général) qui se charge de la distribution des clés à chaque utilisateur.
  - WPA propose aussi un mode moins sécurisé (PSK) basé sur un secret partagé commun à tous les utilisateurs.
- **Gestion des clés :** Utilisation d'un protocole (TKIP) pour pallier les failles de WEP (changement de clé de chiffrement de manière périodique).
- **Intégrité des messages :** Utilisation d'un code de vérification d'intégrité (MIC) en remplacement de CRC.

III.4.2.2.1) Le protocole TKIP

Il permet la génération de clé aléatoire et offre la possibilité de modifier la clé de chiffrement plusieurs fois par seconde pour une sécurité accrue. Ainsi, le WPA permet d'utiliser une clé pour chaque poste connecté au réseau sans fil, tandis que le WEP utilise la même clé pour l'ensemble du réseau sans fil. Si WPA est compatible, la clé WPA est en effet automatiquement générée et distribuée par l'AP. De plus, les validateurs de données peuvent vérifier l'intégrité des informations reçues pour s'assurer que personne ne les a modifiées. Les avantages de TKIP liés aux clés WEP sont les suivants :

• Vecteur d'initialisation 48 bits au lieu du 24 bits de WEP.

• Génération et distribution de clés : WPA génère et distribue périodiquement des clés de chiffrement à chaque client. En fait, chaque trame utilise une nouvelle clé, évitant ainsi des semaines voire des mois d'utilisation de la même clé WEP.

- Code d'intégrité du message : Ce code, appelé MIC (message integrity Code), permet de vérifier l'intégrité de la trame. Le WEP utilise une valeur de vérification d'intégrité ICV (integrity Check Value) de 4 octets, tandis que le WPA rajoute un MIC de 8 octets.

III.4.2.2.2) **Architectures WPA [25]**

Le WPA peut fonctionner selon deux modes :

- **WPA Enterprise** : Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification qui permet d'identifier les utilisateurs sur le réseau et de définir leurs droits d'accès, généralement un serveur RADIUS (Remote Authentification Dial In User Service], et d'un contrôleur réseau (le point d'accès). Cela signifie un ordinateur serveur dédié, d'où un coût certain.
- **WPA Personal** : Le mode WPA « personnel » permet de mettre en œuvre une infrastructure sécurisée basée sur un WPA restreint au WPA-PSK (Pre-Shared Key] sans mettre en œuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelée PSK, en déployant une même clé de chiffrement dans l'ensemble des équipements (vous la renseignez sur le point d'accès ainsi sur les postes clients). Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage.

Cette première version du WPA ne prend en charge que les réseaux en mode infrastructure, ce qui signifie qu'il ne permet pas de sécuriser des réseaux sans fil d'égal à égal (mode ad hoc).

III.4.2.2.3) **Fonctionnement du WPA**

WPA, lui est plus évolué avec un nombre IV de 48 bits: ce qui veut dire qu'il prendra beaucoup plus de temps avant que le nombre IV ne soit recyclé. Il faut également noter que dans la manière, WPA est supérieur dans sa méthode de connexion lorsque des utilisateurs sont connectés, ils sont authentifiés par des clés pré-partagées, ou bien par des configurations plus sophistiquées, par une authentification (LDAR, RADIUS).

Une fois qu'un utilisateur est membre d'un réseau, une clef WPA est crée.

Périodiquement, WPA va générer une nouvelle clé par utilisateur. Combiné la longueur du nombre IV, ceci rend très difficile le piratage. Sur la transmission de chaque paquet, WPA ajoute un code de vérification d'intégrité de 4 bits (ICV) afin de les vérifier. On peut donc conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP. Néanmoins un problème ici reste évident : un attaquant peut intercepter la transmission, modifier le payload, recalculer le code d'intégrité, et le retransmettre sans que personne ne s'en aperçoive. WPA résout ce problème avec un message d'intégrité 8 bits : un payload crypté et des facteurs dans le calcul de l'ICV réduise fortement les possibilités de forge de paquets (l'usurpation d'adresses IP sources).

III.4.2.2.4) **Les failles de WPA**

Ce protocole possède toutefois quelques faiblesses, dont sa sensibilité aux attaques de type déni de service.

En effet, si quelqu'un envoie au moins deux paquets chaque seconde utilisant une clé de cryptage incorrecte, le point d'accès sans fil tuera toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non autorisés à un réseau protégé, mais susceptible de bloquer tout un réseau sans fil.

D'autre ce problème, il manquerait au WPA pour fournir une meilleure sécurité :

- un SSID (Service Set Identifier) sécurisé, c'est-à-dire une chaîne de caractères alphanumériques sécurisée permettant d'identifier un réseau sans fil.
- une déconnexion rapide et sécurisée.
- une dé-authentification et une dé-association sécurisées.
- un meilleur protocole de cryptage tel que AES (Advanced Encryption Standard).

III.4.2.3) Le protocole WPA2 /802.11i

III.4.2.3.1) **Qu'est-ce que l'AES et CCMP ? [26]**

AES qui signifie Advanced Encryption Standard est une forme de cryptage populaire qui est utilisée depuis un certain temps maintenant pour garantir que les données sont conservées en toute sécurité, à distance des regards indiscrets

L'AES comprend trois chiffrements par bloc, et chacun de ces chiffrements par bloc a un nombre différent de combinaisons de touches possibles, comme suit :

AES-128 : longueur de clé de 128 bits=3,4 x 1038

AES-192 : longueur de clé 192 bits=6,2 x 1057

AES-256 : longueur de clé de 256 bits=1,1 x 1077

- **CCMP (*Counter Mode CBC-MAC Protocol*)**

Il est la standard de chiffrement pour la norme IEEE 802.11i.

Il se base sur AES mais évite que chaque message utilise le même bloc d'initialisation. On trouve donc l'option de sécurité **WPA2-AES-CCMP** qui offre une protection efficace de votre réseau sans fil.

III.4.2.3.2) **Présentation WPA2 [27]**

Le WPA-2, tout comme son prédécesseur le WPA, assure le cryptage ainsi que l'intégrité des données mais offre de nouvelles fonctionnalités de sécurité telles que le « *Key Caching* » et la « *Pré-Authentification* ».

III.4.2.3.3) **Le Key Caching**

Il permet à un utilisateur de conserver la clé PMK (Pairwise Master Key) - variante de PSK (Pre-Shared Key) du protocole WPA lorsqu'une identification s'est terminée avec succès afin de pouvoir la réutiliser lors de ses prochaines transactions avec le même point d'accès. Cela signifie qu'un utilisateur mobile n'a besoin de s'identifier qu'une seule fois avec un point d'accès spécifique. En effet, celui-ci n'a plus qu'à conserver la clé PMK, ce qui est géré par le PMKID (Pairwise Master Key IDentifier) qui n'est autre qu'un hachage de la clé PMK, l'adresse MAC du point d'accès et du client mobile, et une chaîne de caractère. Ainsi, le PMKID identifie de façon unique la clé PMK.

III.4.2.3.4) **La Pré-Authentification**

Cette fonction permet à un utilisateur mobile de s'identifier avec un autre point d'accès sur lequel il risque de se connecter dans le futur. Ce processus est réalisé en redirigeant les trames d'authentification générées par le client envoyé au point d'accès actuel vers son futur point d'accès par l'intermédiaire du réseau filaire. Cependant, le fait qu'une station puisse se connecter à plusieurs points d'accès en même temps accroît de manière significative le temps de charge.

Pour résumer, le WPA-2 offre par rapport au WPA :

- Une sécurité et une mobilité plus efficaces grâce à l'authentification du client indépendamment du lieu où il se trouve.
- Une intégrité et une confidentialité fortes garanties par un mécanisme de distribution dynamique de clés.
- Une flexibilité grâce à une ré-authentification rapide et sécurisée.
- Toutefois, pour profiter du WPA-2, les entreprises devront avoir un équipement spécifique tel qu'une puce cryptographique dédiée pour les calculs exigés par l'AES

III.4.2.3.5) **Les failles du WPA2**

WPA2 présente pourtant des inconvénients. Le protocole est par exemple vulnérable aux attaques de réinstallation de clé (KRACK). Cette attaque exploite une faiblesse dans WPA2, qui permet aux attaquants de créer un réseau clone et forcer la victime à s'y connecter. Les hackers peuvent ainsi déchiffrer un petit paquet de données agrégées pour craquer la clé de chiffrement. Toutefois, les dispositifs peuvent être corrigés et WPA2 est toujours considéré comme étant plus sûr que WEP ou WPA.

III.4.2.4) Le protocole WPA3 [28]

WPA3 fournit des protocoles de sécurité de pointe sur le marché. S'appuyant sur le succès généralisé et l'adoption de la sécurité Wi-Fi, WPA3 ajoute de nouvelles fonctionnalités pour simplifier la sécurité Wi-Fi, permet une authentification plus robuste, offre une force cryptographique accrue pour les marchés de données hautement sensibles et maintient la résilience des réseaux critiques. Tous les réseaux WPA3 :

- Utilisent les dernières méthodes de sécurité.
- Interdirent les anciens protocoles obsolètes.
- Exigent l'utilisation de cadres de gestion protégés (PMF).

Étant donné que les réseaux Wi-Fi diffèrent par leur objectif d'utilisation et leurs besoins de sécurité, WPA3 inclut des fonctionnalités supplémentaires spécifiquement pour les réseaux personnels et d'entreprise. Les utilisateurs de WPA3-Personal bénéficient d'une protection accrue contre les tentatives de deviner le mot de passe, tandis que les utilisateurs de WPA3-Enterprise peuvent désormais profiter de protocoles de sécurité de niveau supérieur pour les réseaux de données sensibles.

III.4.2.4.1) **Architectures WPA 3**

- **WPA3-Personnel**

WPA3-Personal apporte de meilleures protections aux utilisateurs individuels en fournissant une authentification basée sur un mot de passe plus robuste, même lorsque les utilisateurs choisissent des mots de passe qui ne répondent pas aux recommandations de complexité typiques. Cette fonctionnalité est activée via l'authentification simultanée d'égal à égal (SAE). La technologie résiste aux attaques par dictionnaire hors ligne où un adversaire tente de déterminer un mot de passe réseau en essayant des mots de passe possibles sans autre interaction avec le réseau.

- **Sélection naturelle du mot de passe** : permet aux utilisateurs de choisir des mots de passe plus faciles à retenir.
- **Facilité d'utilisation** : fournit des protections améliorées sans modifier la façon dont les utilisateurs se connectent à un réseau.
- **Confidentialité de transmission** : protège le trafic de données même si un mot de passe est compromis après la transmission des données.

- **WPA3-Entreprise**

WPA3-Enterprise s'appuie sur la base de WPA2-Enterprise avec l'exigence supplémentaire d'utiliser des cadres de gestion protégés sur toutes les connexions WPA3.

Authentification : plusieurs méthodes EAP (Extensible Authentication Protocol)

Cryptage authentifié : 128 bits minimum Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128).

Dérivation et confirmation de clé : mode d'authentification de message haché (HMAC) 256 bits minimum avec algorithme de hachage sécurisé (HMAC-SHA256).

Protection robuste des trames de gestion : code d'authentification de message basé sur le chiffrement du protocole d'intégrité de diffusion/multidiffusion 128 bits minimum (BIP-CMAC-128).

- **WPA3-Enterprise avec mode 192 bits**

WPA3-Enterprise propose également un mode optionnel utilisant des protocoles de sécurité de niveau minimum de 192 bits et des outils cryptographiques pour mieux protéger les données sensibles.

Le mode de sécurité 192 bits offert par WPA3-Enterprise garantit l'utilisation de la bonne combinaison d'outils cryptographiques et définit une base de sécurité cohérente au sein d'un réseau WPA3.

III.5) L'authentification dans les WLAN [29]

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:

- 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.

III.5.1) Protocoles d'authentification pour les réseaux WiFi [30]

III.5.1.1) PAP :

Le protocole PAP (Password Athentication Protocol), utilisé avec le Protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau.

Après une phase de synchronisation entre le client et le serveur pour définir l'utilisation du protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

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

PAP est le plus simple des protocoles d'authentification, il est donc très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé, il est donc fortement déconseillé. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification et la réutiliser pour s'authentifier, c'est ce qu'on appelle : attaque par rejeu.

III.5.1.2) CHAP

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

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

Ce mécanisme d'authentification procure à CHAP deux avantages :

Tout d'abord, si la requête d'authentification envoyée par le client est interceptée, elle ne pourra pas être rejouée. En effet chaque empreinte calculée par le client est uniquement par le serveur.

D'autre part, lors d'une session établie par le protocole CHAP, le serveur envoie régulièrement des challenges au client de façon à identifier son identité. Cette mesure de TACACS supplémentaire permet donc de se prémunir des détournements de session.

III.5.1.3) MS-CHAP

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

Ainsi, en travaillant uniquement avec ce hash intermédiaire au lieu du mot de passe, le client et le serveur peuvent réaliser le même type de procédure que celle du CHAP, ainsi, le mot de passe clair n'a plus besoin d'être stocké sur le serveur.

Puis malgré l'avancée du protocole MS-CHAP par rapport à CHAP, Microsoft créa une seconde version du protocole (MS-CHAP-v2) pour résoudre deux principales faiblesses de MS-CHAP-v1, d'une part le fait que le client ne puisse pas vérifier l'authenticité du serveur sur lequel il veut se connecter et d'autre part que l'algorithme de hachage propriétaire utilisé soit très vulnérable à des attaques par brute-force.

Voici le fonctionnement du processus d'authentification mutuelle fournit par MS-CHAP-v2 :

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

III.5.1.4) EAP

EAP (Extensible Authentification Protocol) n'est pas directement un mécanisme d'authentification comme le sont PAP ou CHAP, il s'agit en réalité d'une extension du protocole PPP qui a permis d'universaliser et de simplifier l'utilisation des différents protocoles dans le cadre des réseaux sans fils et les liaisons Point-A-Point. EAP contient une douzaine de méthodes d'authentification, les plus utilisées étant EAP-MD5, EAP-TLS, EAP-TTLS, LEAP.

Il faut distinguer des types de trafics EAP, celui entre le client et le point d'accès : EAP over LAN (utilisant un média 802.11a, b ou g) et celui entre le point d'accès et le serveur d'authentification, EAP over RADIUS.

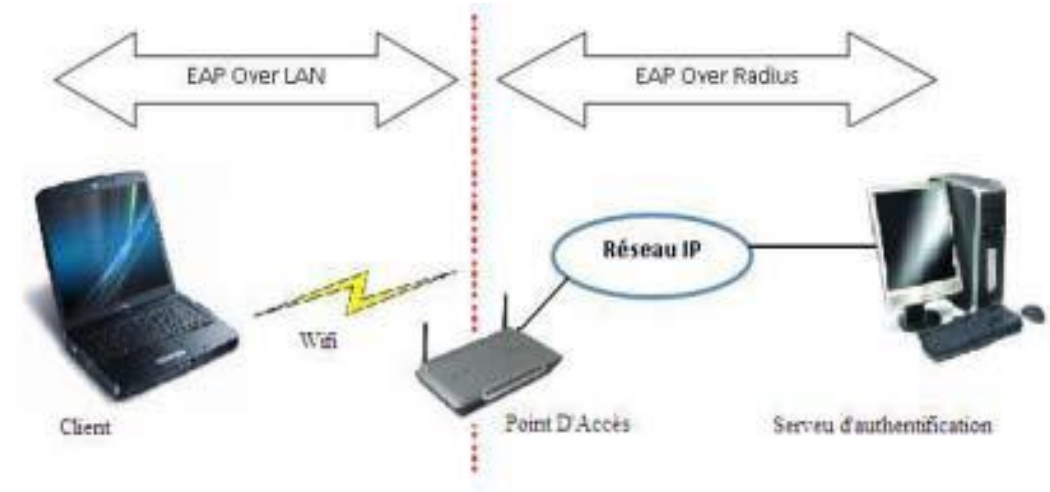


Figure III-6 Types de trafic EAP

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

III.5.1.4.1) LEAP

LEAP signifie « Light Extensible Authentication Protocol », qui se traduit par : version allégée de EAP. C'est une implémentation propriétaire d'EAP développée par Cisco. Lorsque que les mots de passes utilisés sont complexes, il est également très sûr, ce qui a été mis en doute en cas d'utilisation d'un mot de passe faible. On préfèrera donc à sa place PEAP, EAP-TLS ou EAP-FAST pour l'aspect plus sécurisé de ces implémentations. LEAP n'est d'ailleurs pas supporté sur

Windows sans l'ajout d'un client spécifique. Il est cependant largement supporté sur les points d'accès WiFi.

III.5.1.4.2) **PEAP**

PEAP signifie « Protected Extensible Authentication Protocol ». PEAP est une des implémentations d'EAP les plus utilisées. Elle utilise le protocole CHAP15 pour authentifier de façon sécurisée un client grâce au challenge request/response. Windows Server utilise cette version d'EAP.

III.5.1.4.3) **EAP-TLS**

EAP-TLS utilise un système d'authentification avec certificats. C'est donc l'un des meilleurs en termes de sécurité. Son désavantage réside dans le fait qu'un certificat doit être obligatoirement installé chez le client.

III.5.1.4.4) **EAP-TTLS**

EAP-TTLS fonctionne sur le même principe que la version ci-dessus, à la différence que le client ne nécessite pas de certificat de son côté. Un tunnel encrypté est créé à l'aide du certificat du serveur afin d'échanger les informations d'authentification.

III.5.1.4.5) **EAP-FAST**

FAST veut dire « Flexible Authentication via Secure Tunneling ». C'est une version améliorée de LEAP qui utilise PAC (Protected Access Credential), un set d'informations d'authentification qui ne peut pas être copié d'une machine à une autre. Il corrige le manque de sécurité qu'on attribue souvent à LEAP.

III.5.1.5) Comparaison entre différents type de EAP

Type d'EAP	Méthode d'authentification	Caractéristiques
EAP-MD5	Login/password	•Facile à implémenter •Supporté par la plupart des serveurs •Attaquable par dictionnaire hors-ligne •Pas d'authentification mutuelle
EAP-TLS	Certificat	•Utilisation de certificats par le client et le serveur, de ce fait création d'un tunnel sur. •Authentification mutuelle entre le client et serveur •Lourd à mettre en place à cause des certificats coté client.
EAP-PEAP EAP-TTLS	Login/password Et certificat	•Création d'un tunnel TLS •Moins lourd que EAP-TLS, car pas de certificat du coté client. •Moins sur que EAP-TLS, car pas de certificat du côté client.

Tableau III-1 comparaison entre les type de EAP

On remarque que le type **EAP –TLS** est le plus sécurisé

III.6) Services d'authentification applicatif

III.6.1) Le protocole RADIUS [29]

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.

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

- **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 :

- **Les clients 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 demandes d'authentification, l'authentification des utilisateurs et les réponses contenant toutes les informations de configuration nécessaires aux NAS.

On distingue deux sortes d'authentifications RADIUS [29] :

III.6.1.1) 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 œuvre mais est également la moins sûre.

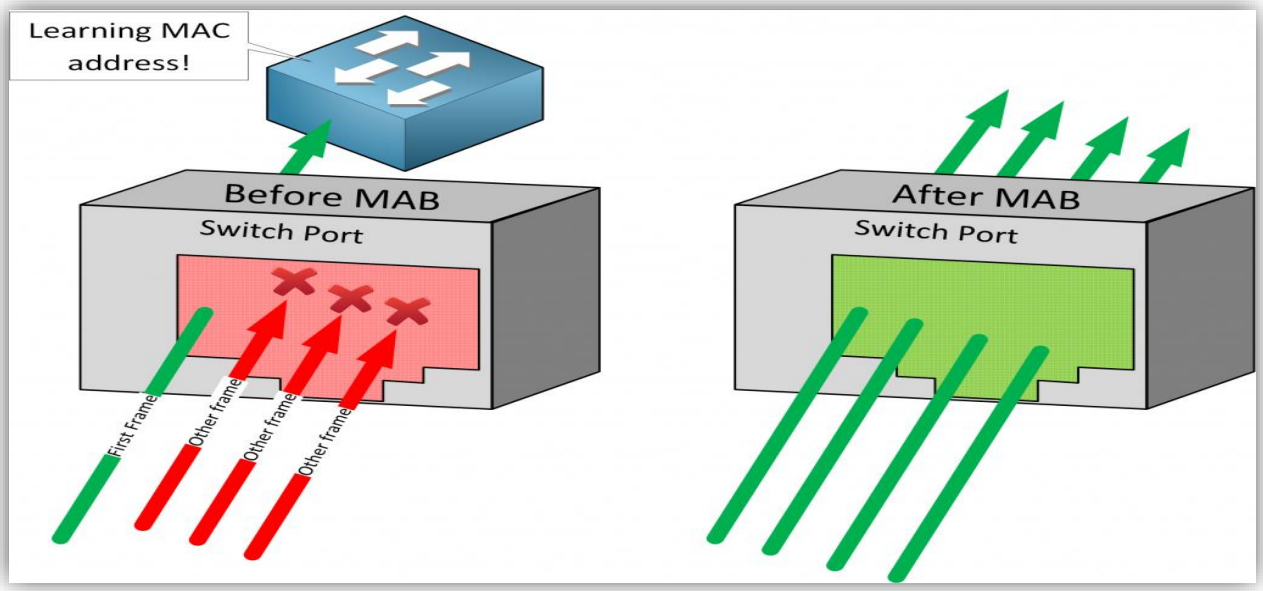


Figure III-7 Authentification RADIUS-MAC

III.6.1.2) L'authentification 802.1X

Cette solution est basée sur le protocole 802.1x et sera détaillée dans ce qui suit.

III.6.2) La technologie 802.1x

Jusqu'ici, nous avons décrit des mesures de sécurité assez faibles : éviter le débordement radio, détecter les AP pirates, masquer le SSID, filtrer par adresse MAC, utiliser le cryptage WEP, etc. Chacune apporte sa pierre à l'édifice, mais aucune ne constitue une véritable muraille contre un pirate motivé et compétent. Il est donc temps d'aborder le protocole EAP : il est à la base du 802.1x avec l'utilisation de serveur Radius.

III.6.2.1) De quoi parle-t-on ?

Le 802.1X est un mécanisme d'authentification au standard international pour des terminaux dans un LAN (réseau interne câblé) ou un WLAN (réseau interne sans fil). Il est typiquement appliqué au sein d'une entreprise pour sécuriser l'accès à son réseau et ainsi aux données lui appartenant. L'objectif de 802.1X est de délivrer, ou non, un droit d'accès au réseau, ceci sans se soucier du support physique utilisé. En effet, 802.1X travaille au niveau de la couche 2 du modèle OSI et ne requiert pas l'utilisation de la couche 3 (couche IP).

IEEE 802.1x utilise le protocole EAP pour mettre en communication le client et le serveur d'authentification via le contrôleur.

Trois éléments indispensables doivent être présents pour permettre le bon fonctionnement de ce processus :

- **Demandeur : C'est** le système à authentifier (le client).
- **Port Access Entity (PAE) :** C'est le point d'accès au réseau**.**
- **point d'accès au réseau (PAE) :** Le système authentificateur contrôle une ressource disponible via PAE qu'il s'agit d'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 :
  - **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 suppliant. Ainsi avant l'authentification du suppliant, seul le mode non contrôlé est possible, permettant les échanges d'information d'authentification. Ces flux sont appelés flux EAPOL (EAP Over Lan).

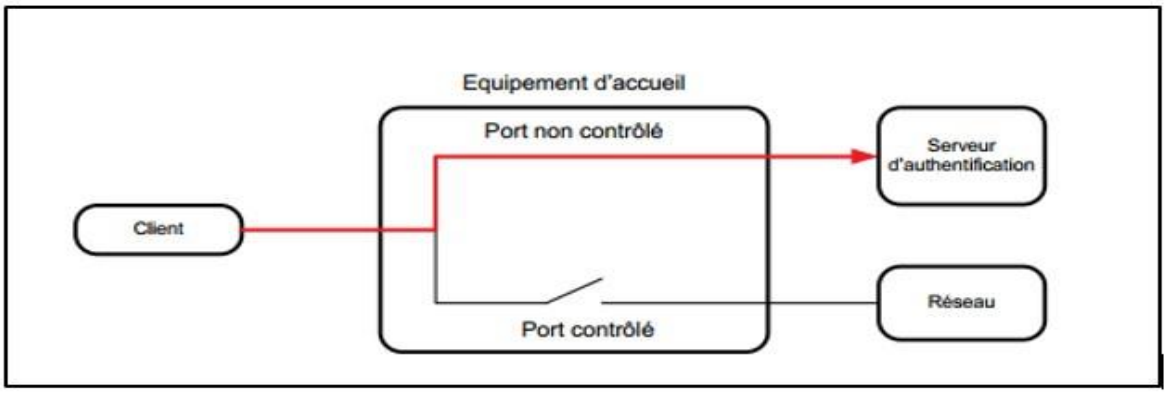


Figure III-8 État du PAE avant la phase d'authentification

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.

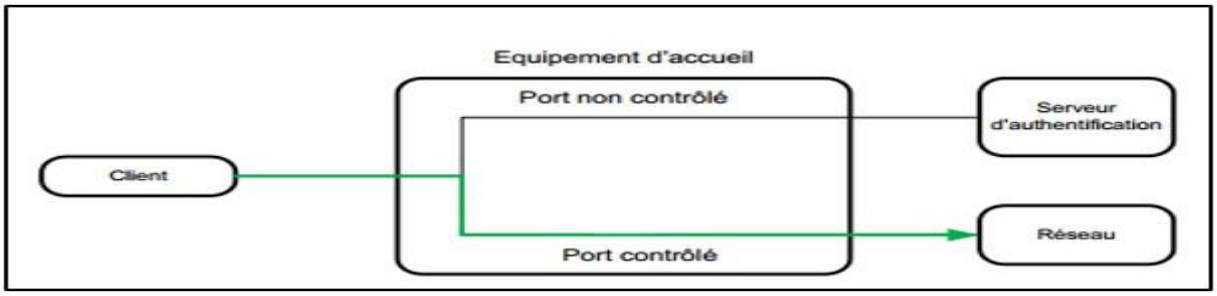


Figure III-9 État du PAE après une authentification réussie

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.

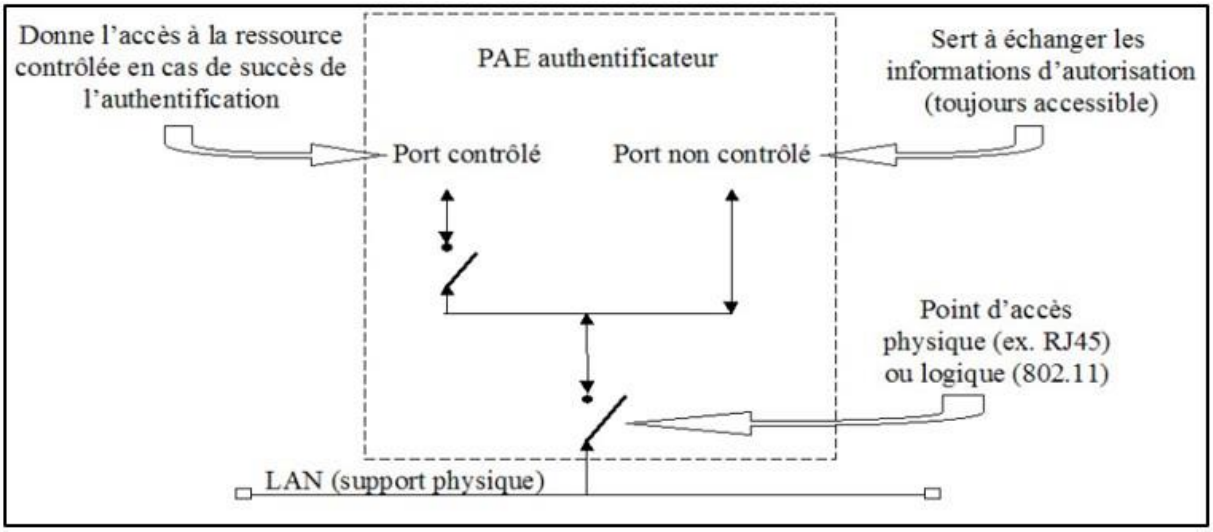


Figure III-10 Le fonctionnement PAE

- **Authenticator System :** C'est système authentificateur qui contrôle les ressources disponibles via le PAE.

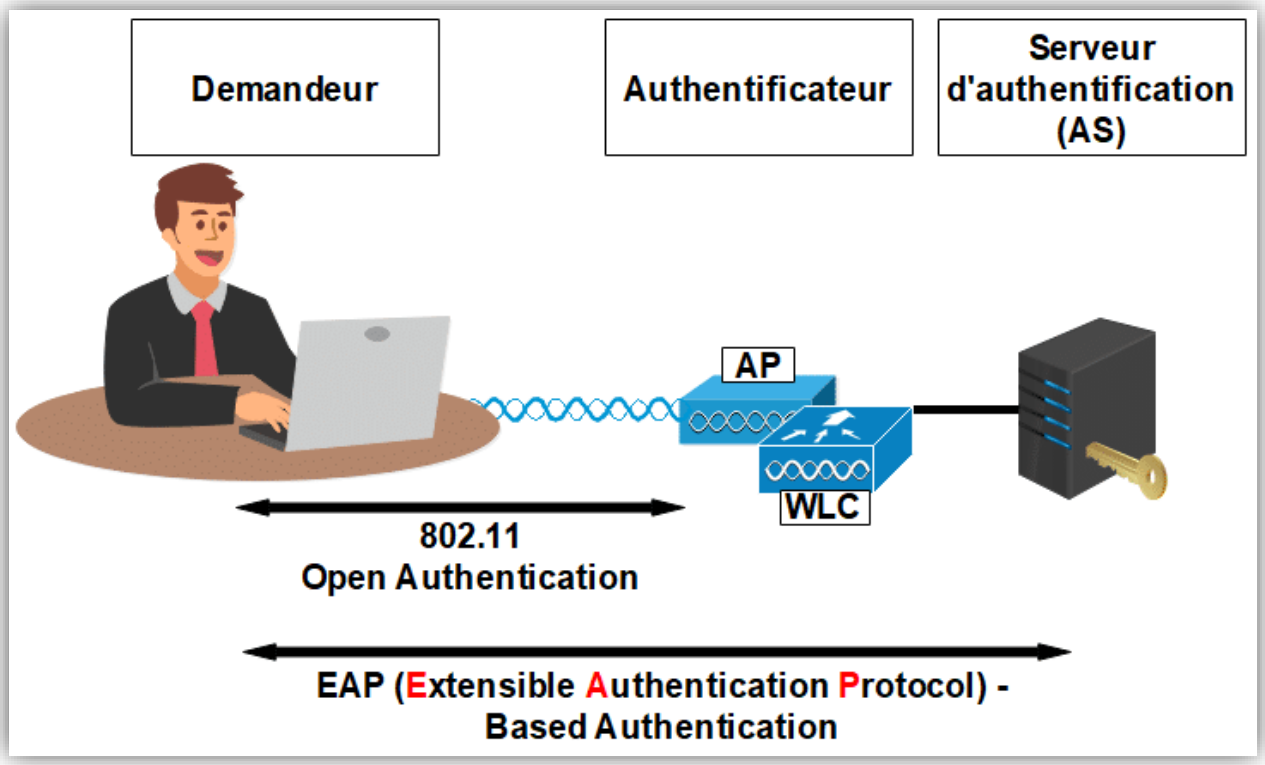


Figure III-11 les différents élément de 802.1x

III.6.2.2) Fonctionnement du protocole 802.1x

La norme 802.1x ne crée pas de nouveau protocole d'authentification, mai s'appuie sur des normes existantes. 802.1x définit plusieurs techniques d'encapsulation pour le transport des paquets d'authentification et de gestion EAP. Cette technique est appelée EAPOL (EAP over LAN) entre le client et le point d'accès et "EAP over RADIUS" entre le point d'accès et le serveur d'authentification RADIUS. Le serveur d'authentification effectue l'action nécessaire (blocage ou déblocage) sur le port contrôlé en fonction des informations d'authentification transportées dans le paquet EAPOL. Ainsi, le système authentificateur agit comme un proxy entre le système authentifié et le serveur d'authentification. Si l'authentification est réussie, le système d'authentification accorde l'accès aux ressources qu'il contrôle (voir la figure ci-dessous)

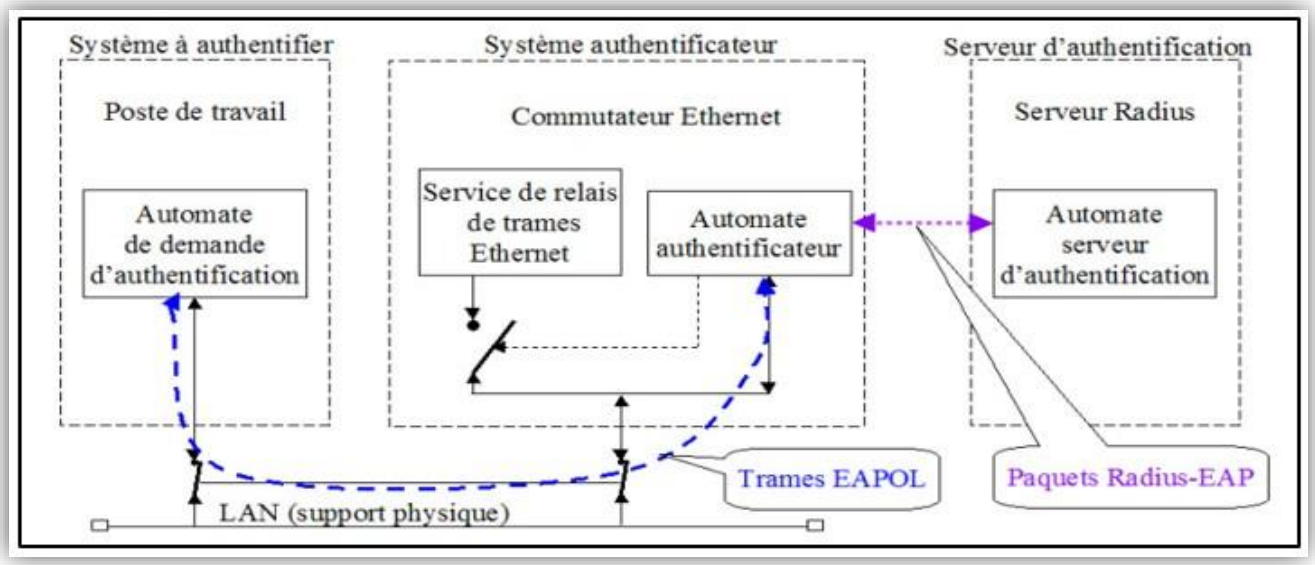


Figure III-12 Les différents protocoles composant le 802.1x [29]

III.6.2.3) Le Procédure d'authentification 802.1x

La première étape est bien sûr une association logique (802.11) avec le port physique du système d'authentification EAP, le port contrôlé de ce dernier est bloqué et seul le port non contrôlé est accessible. Cette étape doit être effectuée avant la phase d'authentification 802.1X. La procédure de certification est la suivante:

1. L'authentificateur envoie un message "EAP-Request/Identity" au suppliant lorsqu'il détecte que le lien est établi.

2. Le demandeur envoie un paquet "EAP-Response/Identity" avec son identité à l'authentificateur et les méthodes d'authentification prises en charge.

3. À ce stade, l'authentificateur envoie un message de réponse/d'identité EAP encapsulé dans une demande RADIUS au serveur d'authentification. L'authentificateur agit comme un simple relais passif lors de l'échange de messages EAP (requêtes et réponses) entre le serveur d'authentification et la station mobile.

4. Le serveur d'authentification décide d'accepter ou de refuser l'accès au réseau et indique le succès ou l'échec du processus d'authentification par un message EAP-Success ou EAP-Failure. Si le serveur d'authentification accepte le client, l'état du port change. Il entre dans l'état autorisé, sinon, le port reste dans l'état non autorisé

À la fin de la connexion (déconnexion logicielle), le demandeur envoie un message de changement d'état de la connexion EAP-Logoff ou physique, et l'authentificateur change l'état du port en non autorisé. 802.1x définit également un minuteur de réauthentification qui peut être utilisé pour forcer le demandeur à se ré-authentifier périodiquement.

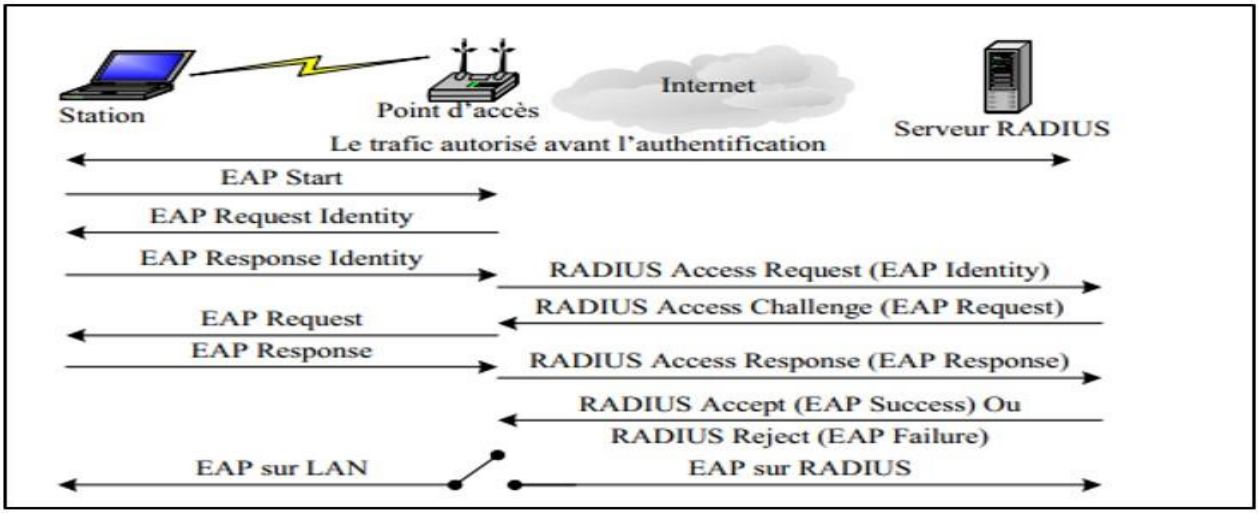


Figure III-13 Procédure standard d'authentification 802.1x

5. Conclusion :

Le WEP avait à sa création pour but avoué (prétention) de proposer une solution de confidentialité équivalente au réseau filaire en s'appuyant uniquement sur un algorithme réputé sûr : RC4. A partir de cette certitude infondée, la simplicité d'utilisation a alors été privilégiée pour promouvoir le développement de ce protocole. Cette « négligence » de la sécurité n'a pas été sans conséquence. Sa conception, on ne l'a constaté pas, a été exemple de failles.

Le développement exponentiel de l'Internet a chamboulé les données du point de vue de la sécurité des réseaux. La découverte constante, au cours de ces dernières années, de ces nombreuses failles devrait mettre un terme à l'utilisation du protocole WEP qui est tout bonnement à proscrire en entreprise et à utiliser avec parcimonie en environnement domestique. C'est pour cela qu'il est progressivement remplacé par des solutions qu'on croyait plus performantes telles que le 802.1x, WPA, WPA2 et WPA3. En fin de compte, on constate que chaque protocole a ses faiblesses.

Dans notre prochain chapitre, on tient à implémenter et tester l'authentification 802.1x dans le réseau Wi-Fi.

chapitre IV. Implémentation et Teste 802.1x

IV.1) Introduction

Après avoir décrit les principes de la sécurité des réseaux et détaillé la mécanique du protocole d'authentification 802.1X, son importance et la nécessité de son déploiement dans les réseaux actuels, nous allons maintenant démontrer ces aspects en pratique à l'aide d'équipements et de solutions réseau des fabricants Cisco.

Tout d'abord, nous construisons une topologie sur laquelle nous implémentons notre solution. Deuxièmement, nous configurons la sécurité 802.1X en détaillant les étapes suivies et en capturant les résultats obtenus.

Notre travail consiste à installer et déployer la solution Cisco ISE, puis à mettre en place la configuration initiale des équipements. Après cela, nous devons ajouter le serveur ISE aux équipements d'authentification et ajouter les équipements dans le serveur ISE (Switch, Access Point), assurer la connectivité entre tous les équipements avec le serveur ISE.

Après ces étapes nous somme besoin de :

- Crée des Policy d'authentification.
- Crée des Rôle.
- Crée des utilisateurs.
- Affecté l'utilisateur a un groupe d'authentification.
- Ajouté une Policy a le groupe d'authentification.

Tout ça dans le serveur ISE on utilise l'interface graphique de celle-ci.

Afin d'atteindre cet objectif, l'entreprise a placé un serveur dans nos mains. Aussi, il a posé sur nous main des équipements réaux (Cisco) deux Switch et point d'accès.

Nous avons mis en œuvre et évalué tous les protocoles EAP qui ne nécessitent pas de licence ISE ou d'AC (autorité de certification). Nous sommes capables de le faire, mais nous n'avons pas les ressources pour le faire.

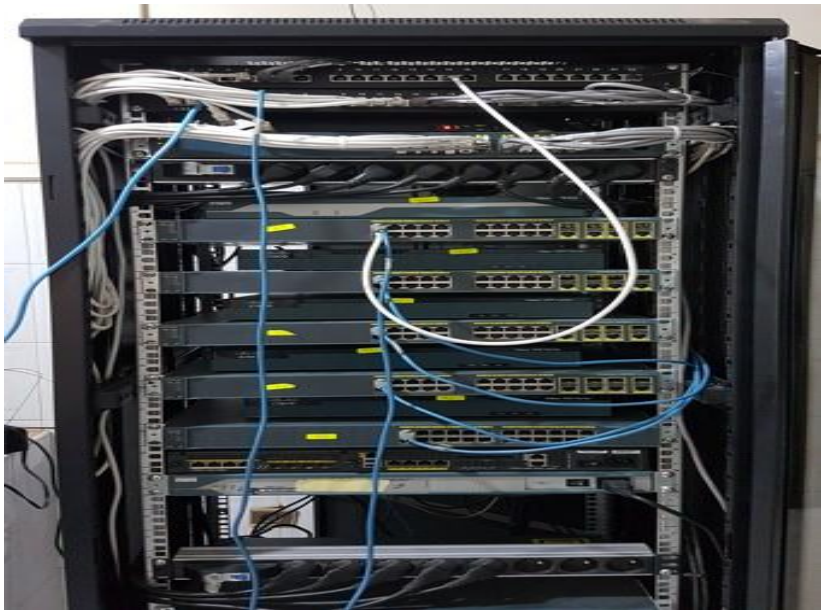


Figure IV-1 le Rack de ICT-TOWERS

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-2 ICT-TOWERS logo

IV.3) **Topologie du réseau :**

Afin de configurer le scénario de test, nous avons représentée la topologie propose dans un enivrement réel de la société **ICT-TOWERS**.

La Figure IV-3 illustre la topologie sur laquelle nous avons travaillé :

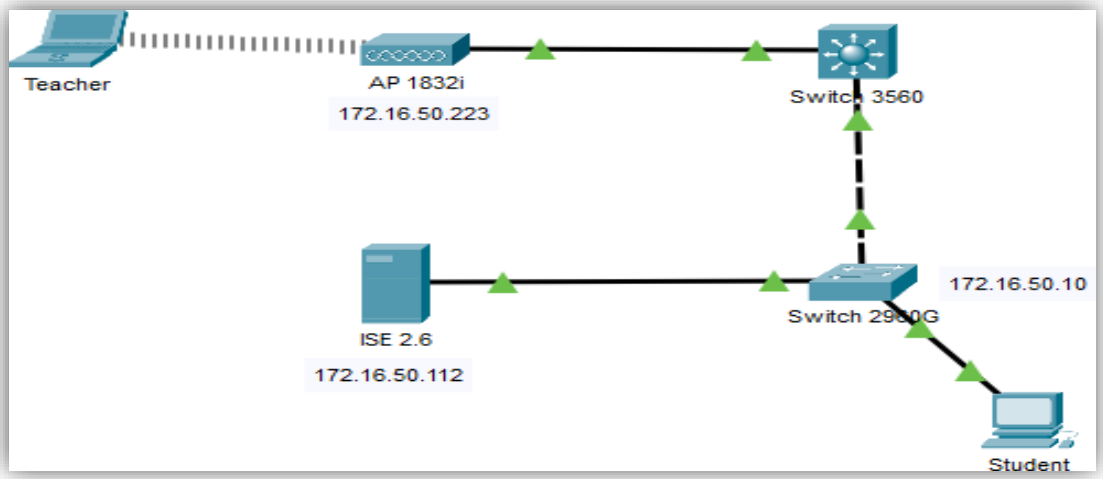


Figure IV-3 topologie préparée à ICT Towers

le tableau IV.1 résume les matériels et les outils utilisés.

ressource matériel (hardware)	Cisco Switch 2960 (WS-C2950G-24-EI)
	Cisco Access Point 1832i (AIR-AP1252AG-E-K9)
	Cisco Switch 3560 (WS-C2950G-24-EI)
	Lenovo Li 3710 (laptop)
	Samsung M32 (phone)
	Microsoft Windows 10
	Dell Serveur ISE
Outils	Wireshark
	VMware Workstation

Tableau IV-1 les matériels et les outils utilisés

Pour des raisons de confidentialité de l'architecteur de l'entreprise et pour simplifier notre topologie. Nous avons utilisé le PC de bureau d'un étudiant connecté au Switch et le PC portable

d'un prof. Après notre implémentation, chaque PC utilisera une identité (nom d'utilisateur et mot de passe) pour se connecter au réseau et aura une adresse IP.

Le client (PC) au droit d'utiliser ou de spécifier une méthode EAP.

Si ce n'est pas le cas, chaque PC dispose de 3 tentatives, s'il les dépasse, il passe en Vlan Filed.

Remarque

On a réalisé se travail avec un autre binôme qu'ils ont le même sujet comme nous juste nous faisons implémentation sur un réseau sans fil et l'autres sur un réseau filaire. C'est pour ca dans cette topologie il y a filaire qu'est relie avec un switch et sans fil avec point accès.

IV.4) Cisco Identity Services Engine (ISE)

IV.4.1) Présentation ISE

ISE est une plate-forme de politique d'identité et de contrôle d'accès de nouvelle génération qui permet aux entreprises d'appliquer la conformité, d'améliorer la sécurité de l'infrastructure et de rationaliser leur service opérations. L'architecture unique de Cisco ISE permet aux entreprises de recueillir des données contextuelles en temps réel informations provenant des réseaux, des utilisateurs et des appareils. L'administrateur peut ensuite utiliser ces informations pour faire décisions de gouvernance proactives en liant l'identité à divers éléments du réseau, y compris les commutateurs d'accès, contrôleurs LAN sans fil (WLC), passerelles de réseau privé virtuel (VPN) et commutateurs de centre de données.

Cisco ISE est un composant clé de la solution Cisco Security Group Access.

Cisco ISE est un système de contrôle d'accès consolidé basé sur des politiques qui intègre un sur-ensemble de fonctionnalités disponibles sur les plates-formes de politique Cisco existantes. Cisco ISE exécute les fonctions suivantes :

• Combine l'authentification, l'autorisation, la comptabilité (AAA), la posture et le profileur dans une seule Appliance

• Fournit une gestion complète de l'accès invité pour l'administrateur Cisco ISE, sanctionné administrateurs parrains, ou les deux

• Applique la conformité des terminaux en fournissant des mesures complètes de provisionnement des clients et évaluer l'état de l'appareil pour tous les terminaux qui accèdent au réseau, y compris les environnements 802.1X

• Fournit une prise en charge pour la découverte, le profilage, le placement basé sur des règles et la surveillance des terminaux appareils sur le réseau

• Permet une politique cohérente dans les déploiements centralisés et distribués qui permet aux services d'être livrés là où ils sont nécessaires

• Prend en charge l'évolutivité pour prendre en charge un certain nombre de scénarios de déploiement, du petit bureau aux grands environnements d'entreprise

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer l'ensemble de votre réseau d'accès. Fournir un accès au réseau basé sur l'identité

La solution Cisco ISE fournit une gestion des identités sensible au contexte dans les domaines suivants :

• Cisco ISE détermine si les utilisateurs accèdent au réseau sur un réseau autorisé et conforme à la politique dispositif.

• Cisco ISE établit l'identité, l'emplacement et l'historique des accès des utilisateurs, qui peuvent être utilisés pour la conformité et rapports.

• Cisco ISE attribue des services en fonction du rôle d'utilisateur, du groupe et de la stratégie associée (rôle de travail, emplacement, type d'appareil, etc.).

• Cisco ISE accorde aux utilisateurs authentifiés l'accès à des segments spécifiques du réseau ou à des applications et services, ou les deux, en fonction des résultats d'authentification.

IV.4.2) Configuration expérimentale

Le dispositif expérimental se compose de trois entités : le suppliant, l'authentificateur et le serveur d'authentification. Le rôle de chaque entité utilisée ainsi que la configuration du système et le système d'exploitation (OS) sont décrits ci-dessous,

IV.4.2.1) Client - Le Supplicant

Un client est un dispositif qui se connecte à un réseau. Afin de se connecter au réseau, un client doit s'authentifier auprès du serveur d'authentification pour établir une connexion sécurisée et utiliser les ressources disponibles.

Dans cette expérience, un ordinateur portable fonctionnant avec le système d'exploitation Linux (Ubuntu) est utilisé comme client. La principale motivation de l'utilisation d'un ordinateur portable au lieu d'un ordinateur personnel est que, comme nous réalisons l'expérience dans des réseaux câblés et sans fil, les ordinateurs portables peuvent être utilisés pour se connecter aux deux réseaux, mais les PC ne peuvent pas être utilisés pour se connecter à un réseau sans fil car les cartes d'interface Wifi ne sont pas disponibles en interne. Une autre raison est que les PC ne sont pas pratiques et ne peuvent pas être transportés partout, généralement les gens qui portent

des ordinateurs portables ont tendance à se connecter à un réseau sans fil. Les spécifications de l'ordinateur portable sont indiquées ci-dessous.

Le Pc portable de client contient :

- Ordinateur portable Lenovo Modèle : PP39I
- Processeur : Intel core i7 CPU : 2GHz
- RAM : 8GB
- Système d'exploitation : Ubuntu 12.04LTS

La raison de l'utilisation d'Ubuntu comme système d'exploitation est qu'il s'agit d'un système open source et que toutes les méthodes EAP sont disponibles en interne et ne nécessitent pas de logiciel supplémentaire, alors que dans le système d'exploitation Windows, de nombreuses méthodes EAP ne sont pas disponibles en interne et nécessitent donc l'installation d'un logiciel externe (Xsupplicant). Ubuntu a été utilisé comme système d'exploitation.

IV.4.2.2) Switch - L'authentificateur

Figure IV-4 le Switch de notre topologie

Le switch est un dispositif utilisé pour transférer les informations d'identification de l'utilisateur entre le suppliant et le serveur d'authentification. Le rôle principal joué par l'authentificateur est qu'il est responsable de l'ouverture ou de la fermeture du port pour que le suppliant puisse accéder/refuser l'utilisation des ressources disponibles dans le serveur.

Dans le réseau câblé, les spécifications de l'authentificateur sont données ci-dessous :

- Nom : Cisco 2960 séries
- Version : 12.4
- Modèle : AIR-LAP1232AG-E-K9

IV.4.2.3) Point d'accès- L'authentificateur 2

Figure IV-5 le point d'accède notre topologie

Ces appareils ont été configurés pour utiliser IEEE 802.1x. Ces périphériques configurés ont été utilisés pour transférer les messages EAP entre le suppliant et le serveur d'authentification.

IV.4.2.4) Serveur RADIUS - Le serveur d'authentification

Le serveur d'authentification on a installé ISE qui est le serveur d'authentification sur le Serveur de ICT-TOWERS sur une virtuelle avec ces paramètres :

- Système : Dell
- CPU : 4GHz
- RAM : 13GB
- Système d'exploitation : Windows 10 / VM
- Logiciel : Cisco ISE 2.6

Il existe de nombreux serveurs RADIUS open source, mais seuls quelques serveurs prennent en charge toutes les méthodes EAP largement utilisées. ISE [30] est un serveur De Cisco qui prend en charge la plupart des protocoles d'authentification, ce qui nous a incités à utiliser ce serveur.

La configuration du serveur RADIUS est présentée dans l'annexe A.

IV.4.3) **Wireshark**

Wireshark est un logiciel open source qui est disponible pour les systèmes d'exploitation Windows et Linux Wireshark est un analyseur de paquets réseau utilisé pour capturer des paquets réseau et afficher les données des paquets de manière détaillée. Il est utilisé pour résoudre les problèmes de réseau, examiner les problèmes de sécurité, déboguer la mise en œuvre du protocole et l'éducation.

Wireshark est utilisé pour surveiller les messages EAP circulant entre le suppliant et le serveur d'authentification.

IV.4.4) **VMware Workstation**

VMware Workstation est un programme de machine virtuelle qui vous permet d'exécuter différents systèmes d'exploitation sur un seul ordinateur hôte physique sur des machines x86 et x86-64. Une seule instance de n'importe quel système d'exploitation (Microsoft, Linux, etc.) peut fonctionner dans chaque machine virtuelle en même temps. Les disques durs, les périphériques USB et les CD-ROM sont tous pris en charge par VMware Workstation, qui agit comme un pont entre l'hôte et la machine virtuelle. L'ordinateur hôte est utilisé pour installer tous les pilotes de périphériques.

IV.5) **Les étapes de Configuration**

Tout d'abord, nous configurons l'équipement (commutateur d'accès et commutateur multicouche) pour transmettre le trafic et activer le protocole 802.1x. Après avoir terminé la configuration initiale de l'équipement et créé (vlan, DHCP, ligne vty, ...), nous pouvons passer au serveur ISE et le configurer.

Remarque : Toute la mise en œuvre de ces étapes se trouve en **annexe A** et en **annexe B**.

IV.5.1) **Installation ISE**

Pour installer ISE nous avons utilisé un serveur de l'entreprise et installé ISE dans une machine virtuelle. ISE requiert une machine virtuelle ayant au minimum les caractéristiques suivantes :

- Mémoire vive de 4 GB
- 4 processeurs (CPUs)
- Mémoire disque de 200 GB
- Deux cartes réseaux (2 NIC)

IV.5.2) Configuration des ports du commutateur

Pour configurer les ports du commutateur, il faut d'abord activer le mode accès et configurer statiquement le VLAN d'accès, puis activer l'authentification 802.1X.

Pour accélérer l'authentification, le demandeur du point final doit envoyer un message périodique EAP over LAN (EAPoL-Start) au port de commutation. En raison de la nature et du calendrier du protocole 802.1X.

IV.5.3) Configuration de serveur RADIUS

Pour que le commutateur puisse communiquer avec Cisco ISE en tant que serveur source ADIUS, il faut lui attribuer l'adresse d'ISE avec une clé. Cette dernière est mentionnée lors de l'ajout du commutateur à la liste des périphériques réseaux au niveau de l'ISE. La commande radius-server vsa send permet au serveur d'accès au réseau de reconnaître et d'utiliser les attributs de comptabilité et d'authentification propres au fournisseur. L'utilisation de paramètre accounting avec la commande radius-server vsa send limite l'ensemble des attributs vsa au seul attribut de comptabilité. L'utilisation de paramètre authentification avec la commande radius-server vsa send limite l'ensemble des attributs vsa au seul attribut d'authentification.

IV.5.4) Résume de la Configuration

Un résumé sur que n'a fait (des point) :

- Configuration initiale.
- Configuration du switch d'accès « authentificateur ».
- Ajout d'un utilisateur d'administration Configuration du routage inter-vlan Création des VLANs.
- Configuration de line vty.
- Configuration de l'interface VLAN 1 de l'interface connectée à l'ordinateur.
- Configuration de l'interface connectée au serveur ISE.
- Configuration de l'interface connectée au switch multi-layer en mode trunk.
- Configuration du switch multi-layer.
- Configuration du routage inter-vlan.
- Création des VLANs Configuration de l'interface VLAN 1.
- Configuration de l'interface connectée au switch d'accès en mode trunk.
- Activation de routage.
- Configuration des SVI (Switch Virtual Interfaces).
- Création des pools DHCP.

- Implémentation de la méthode 802.1X.
- Configuration initiale du modèle AAA.
- Ajout du serveur radius au niveau du switch d'accès.
- Configuration du « Port-Based Authentication ».
- Configuration du « Port-Based Authentication » au niveau de switch.
- Configuration du « Port-Based Authentication » au niveau du serveur ISE.
- Ajout de l'équipement réseau (Switch d'Accès).

On a assuré le routage inter-Vlan et la connectivité entre tous les authentificateurs et le serveur ISE. Après on a autorisé tous les méthodes de authentification dans le Serveur ISE.

IV.5.5)**Déploiement des différents protocoles de l'Authentification dans le réseau sans fil « wireless »**

Après la configuration de l'architecture sans fil ainsi que les machines de chaque architecture et le déploiement des différents protocoles d'authentification, nous allons effectuer des tests de connectivité pour confi mer le bon fonctionnement de chaque approche a part. Les figures suivantes nous affichent les résultats obtenus :

-EAP TTLS (PAP-ASCII)

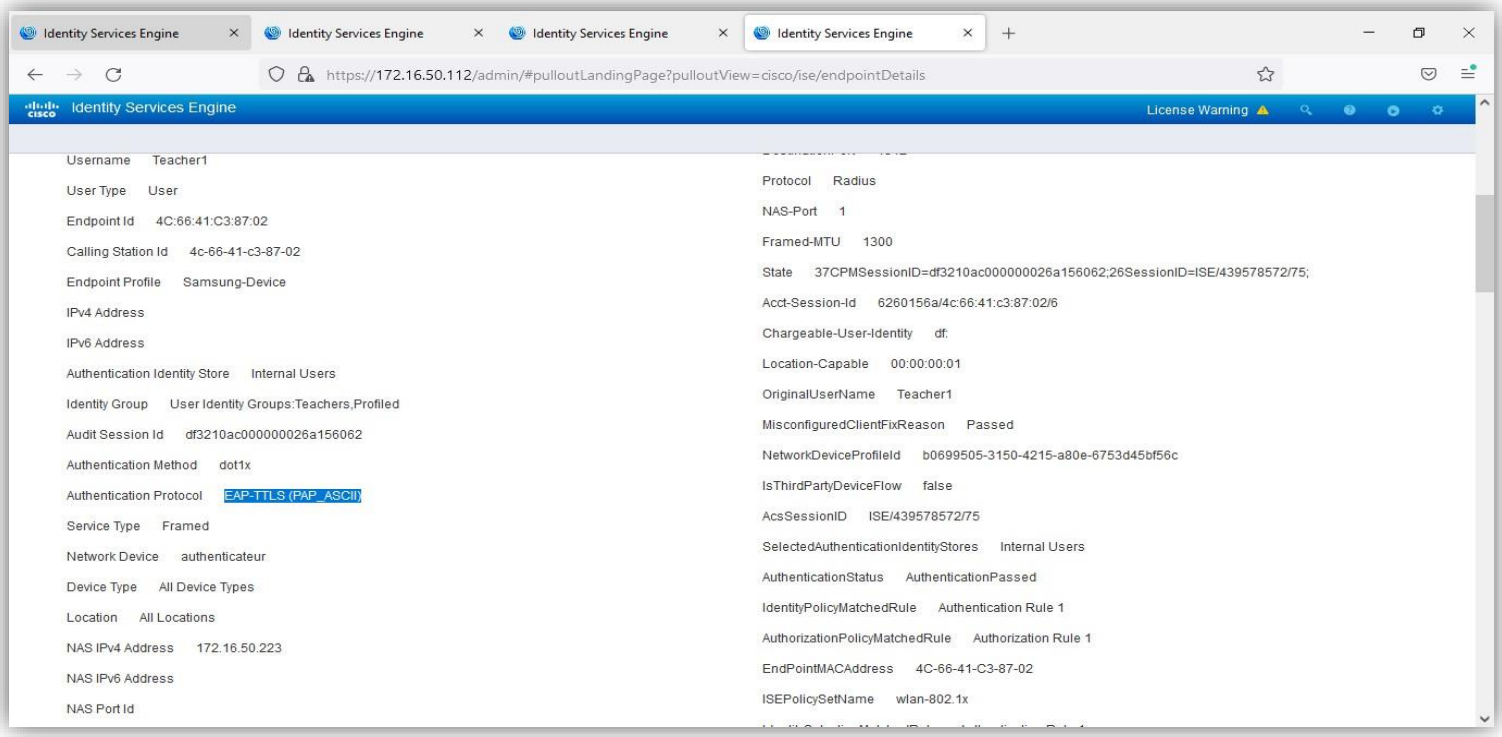


Figure IV-6 Test de connectivite d'EAP TTLS (PAPASCII) WLAN

-PEAP (EAP MSCHAPV2)

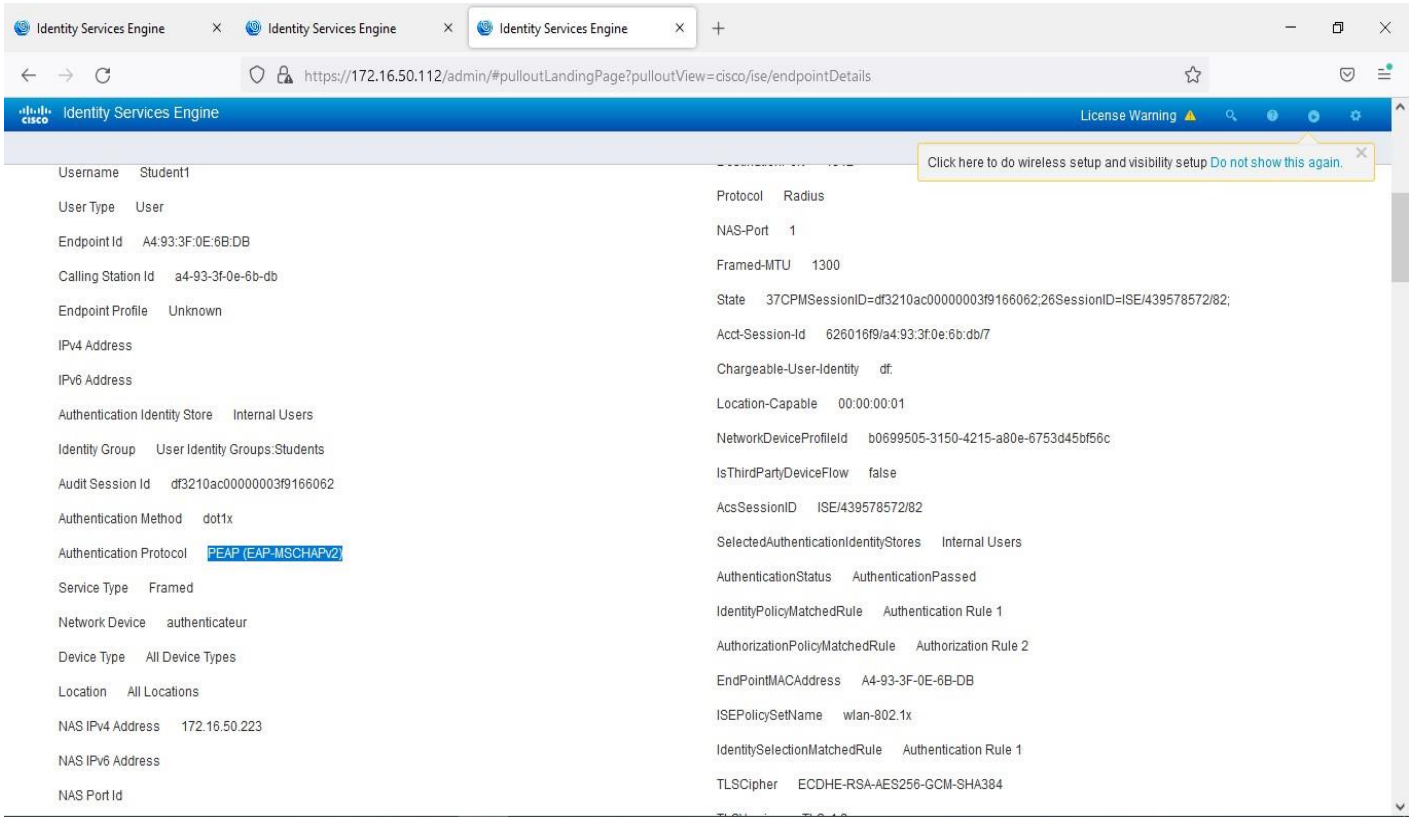


Figure IV-7 Test de connectivite de PEAP (EAP MSCHAPV2) WLAN

-LEAP

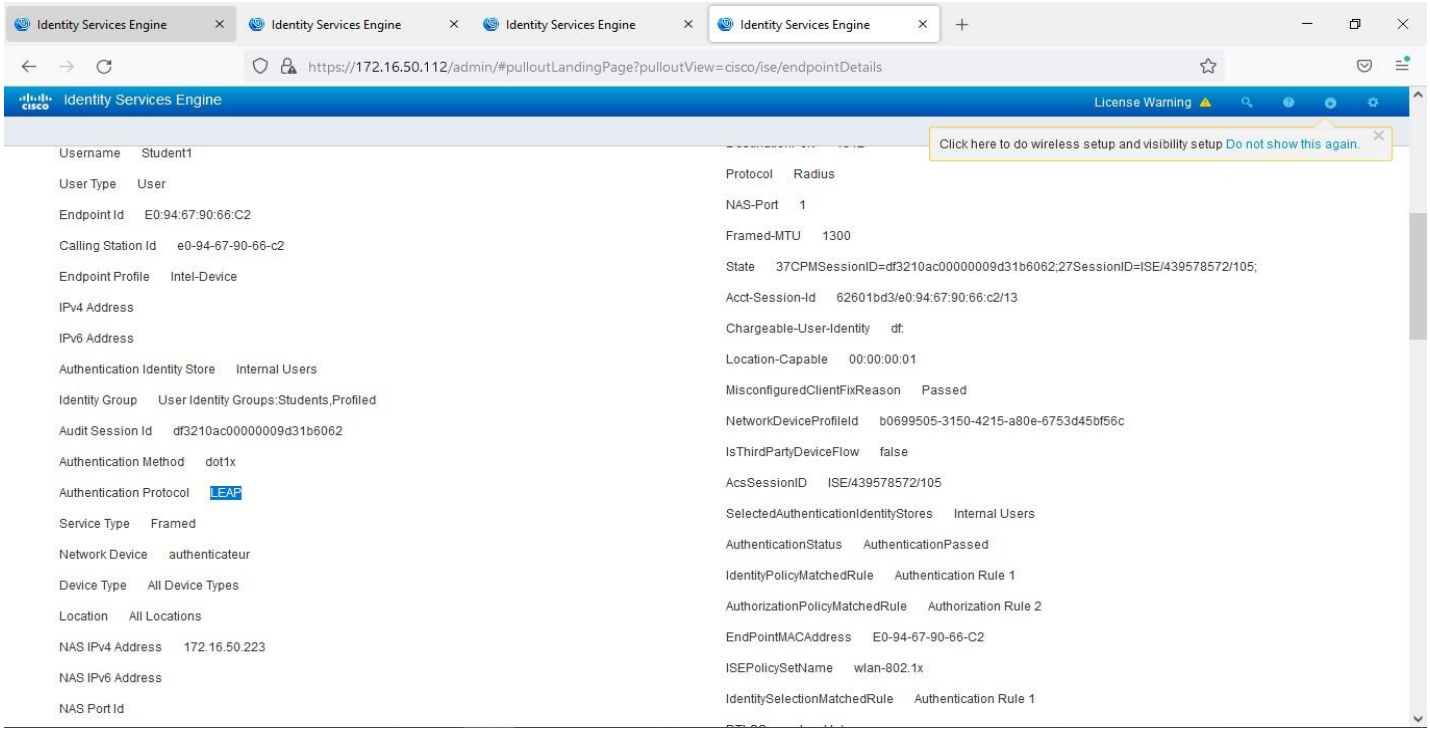


Figure IV-8 Test de connectivite d'EAP LEAP – WLAN

IV.6) **Evaluation les résultats**

Maintenant nous utilisons un outil de capture de paquets (wireshark) pour suivre et faire des statistiques sur les différents protocoles d'authentification mises en place. Le but de la capture de paquets est principalement, le but est le calcul des délais d'authentification de chaque méthode. Ce qui nous permettra de faire une comparaison entre les performances des protocoles d'authentification dans les sans fil.

IV.6.1)**Les résultats du captures de paquet**

Pour chaque figure, un résultat de capture de paquets qui contient les échanges de messages entre l'authentificateur et le client avec le temps réel de chaque message.

LEAP

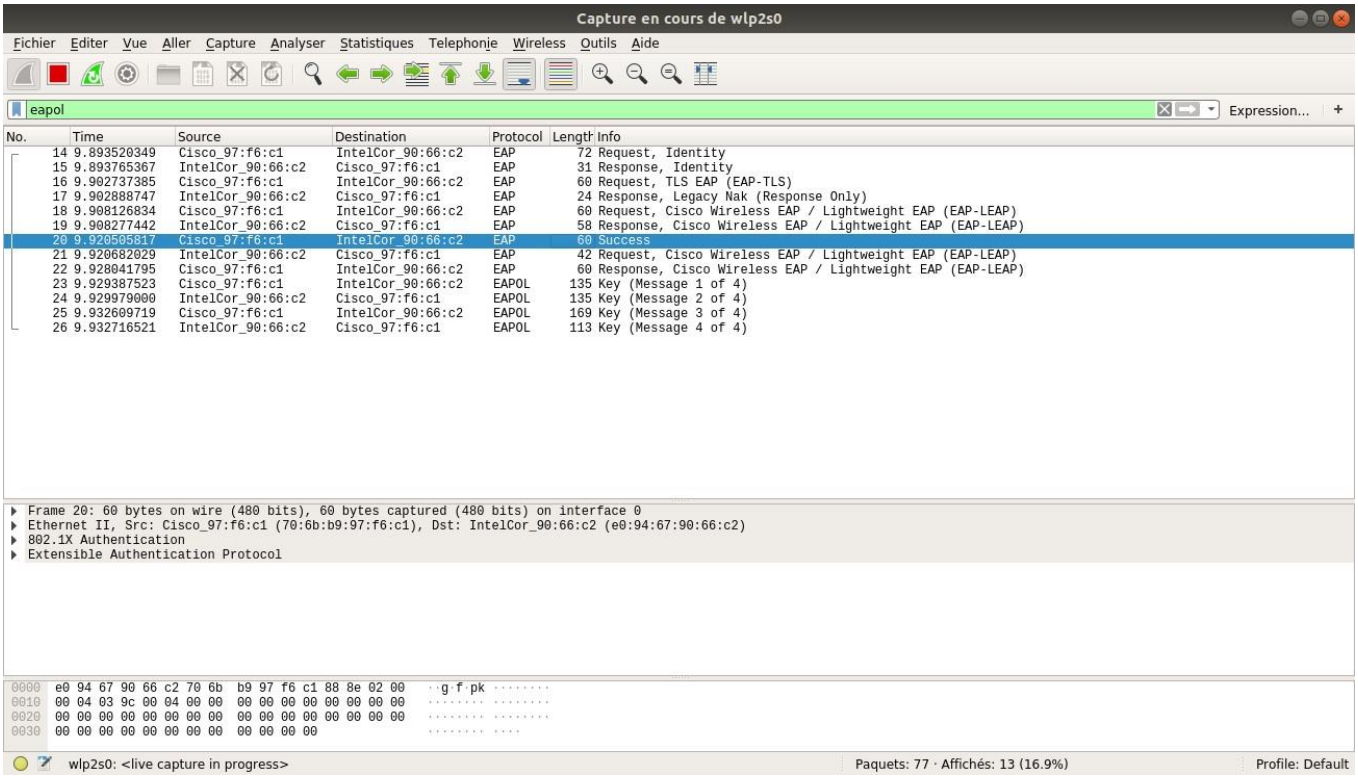


Figure IV-9 Résultat de capture de paquet de LEAP-WIFI

TTLS-PAP

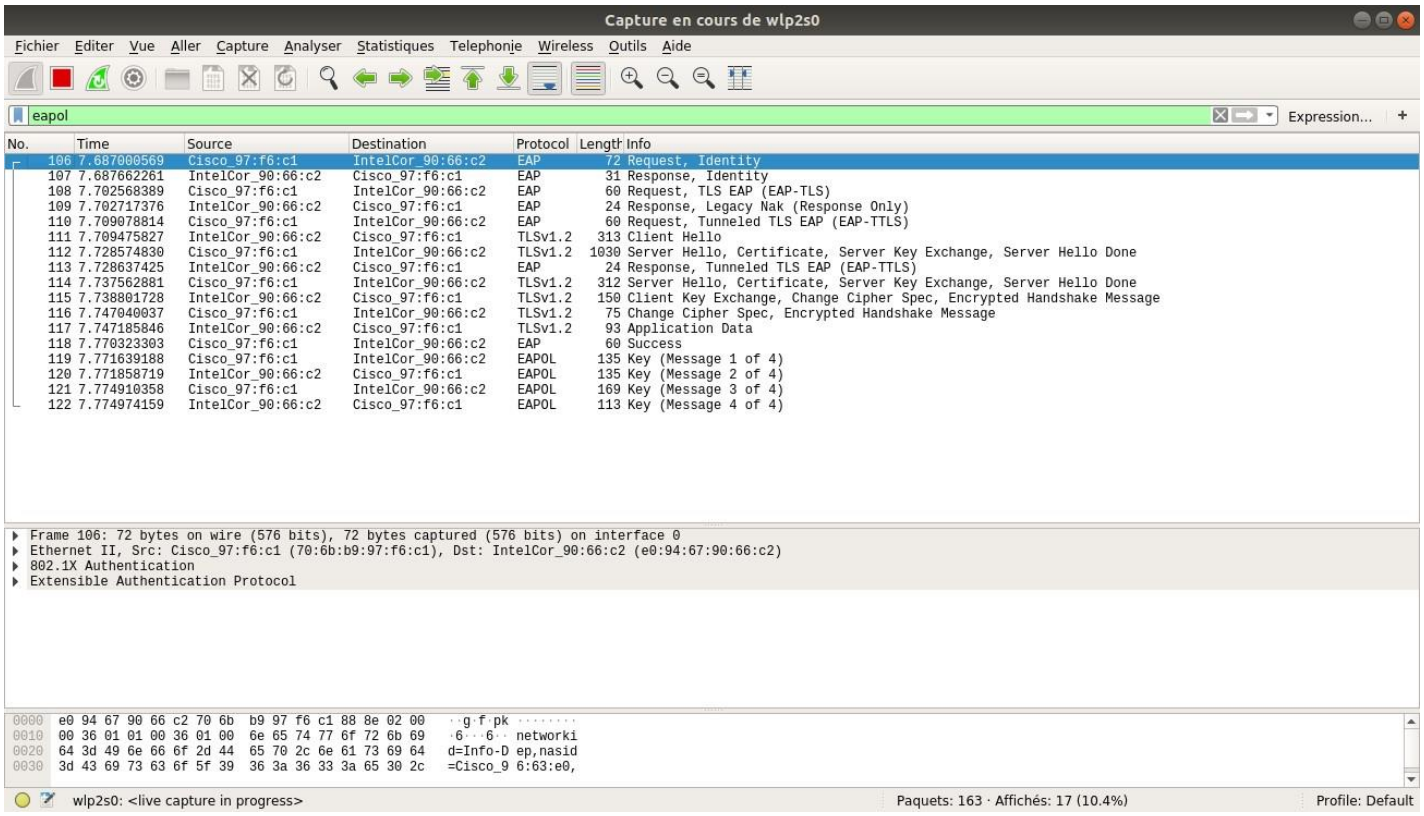


Figure IV-10 Résultat de capture de paquet de TTLS-PAP -WIFI

TTLS-MSCHAP'V2'

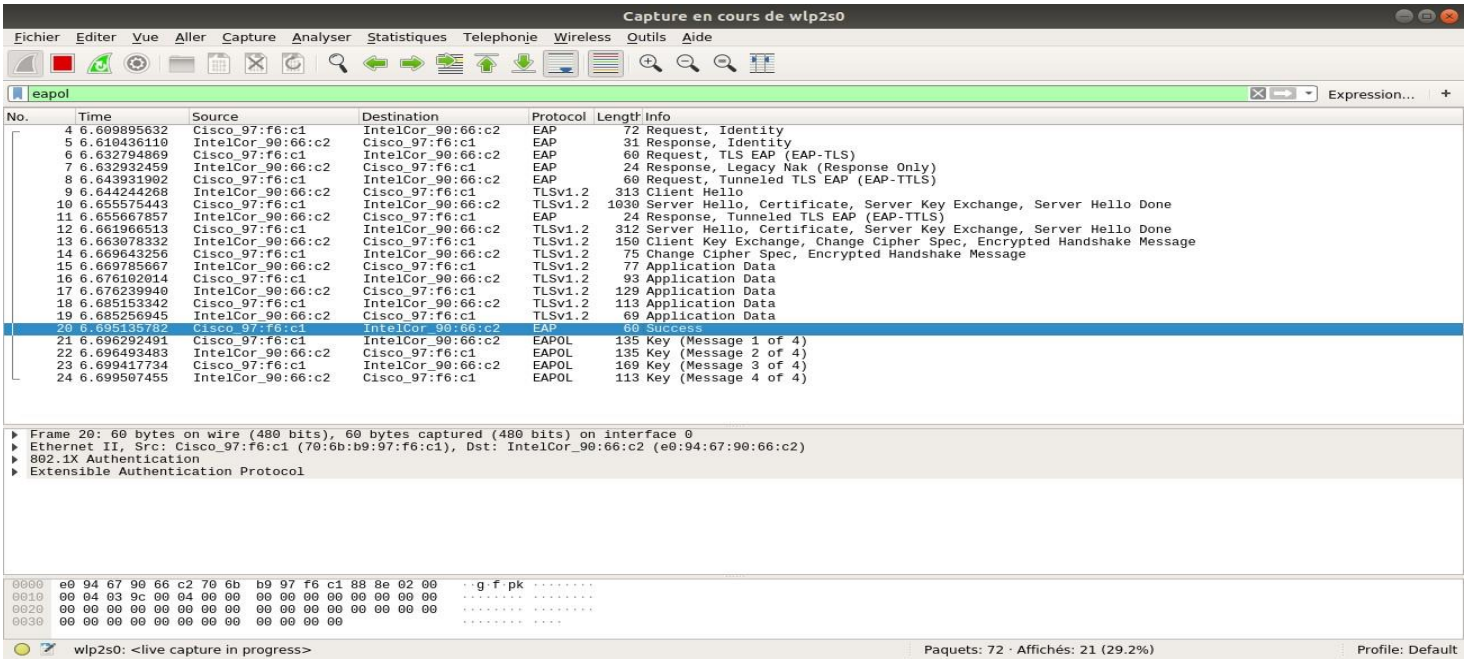


Figure IV-11 Résultat de capture de paquet de TTLS-MSCHAP'V2' -WIFI

PEAP-MSCHAP'V2' :

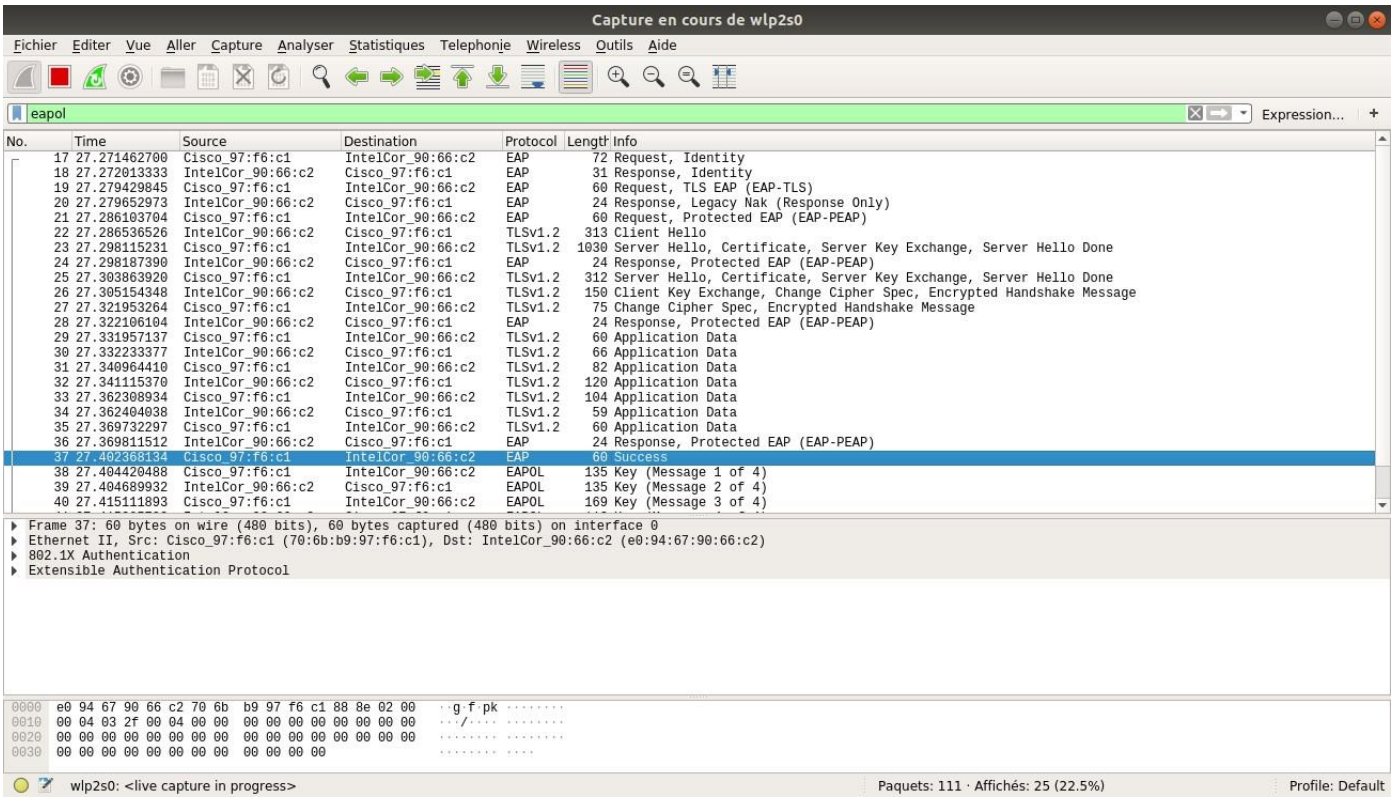


Figure IV-12 Résultat de capture de paquet de PEAP-MSCHAP'V2'-WIFI

IV.6.2)**EVALUATION DES METHODES**

La formule utilisée pour calculer le temps nécessaire à chaque protocole pour effectuer une authentification est la suivante :

$$A_{Total} = A_{fin} - A_{début}$$

A_{fin} =le total temps d'authentification
$A_{début}$ =le temps du 1 ^{er} message EAP
$A_{Début}$ =le temps du dernier message EAP

Équation IV-1 formule de calcule le temps à chaque protocole

Et pour la moyenne de temps d'authentification (5 authentifications) pour
La formule utilisée dans les calculs :

$$\frac{\sum_{n}^{1} At}{n}$$

At = le temps total authentification
N = numéro des essaie

Équation IV-2 formule de calcule le temps à chaque protocole pour 5 authentification

IV.6.3)**Résultats obtenus**

Après la capture du premier paquet d'authentification entre le client et l'authentificateur pour chaque méthode sur le réseau sans fil , nous avons obtenu les résultats suivant :

Méthode EAP	**Le temps d'authentification (s) 1 fois**	**Le temps d'authentification (s) 5 fois**
PEAP-MSCHAP'V2'	0.1309	0.1451
EAP-TTLS-MSCHAP'V2'	0.0852	0.1274
LEAP	0.0269	0.0574
TTLS-PAP	0.0833	0.0268

Tableau IV-2 Le temps d'authentification 1 et 5 fois dans un réseau sans fil

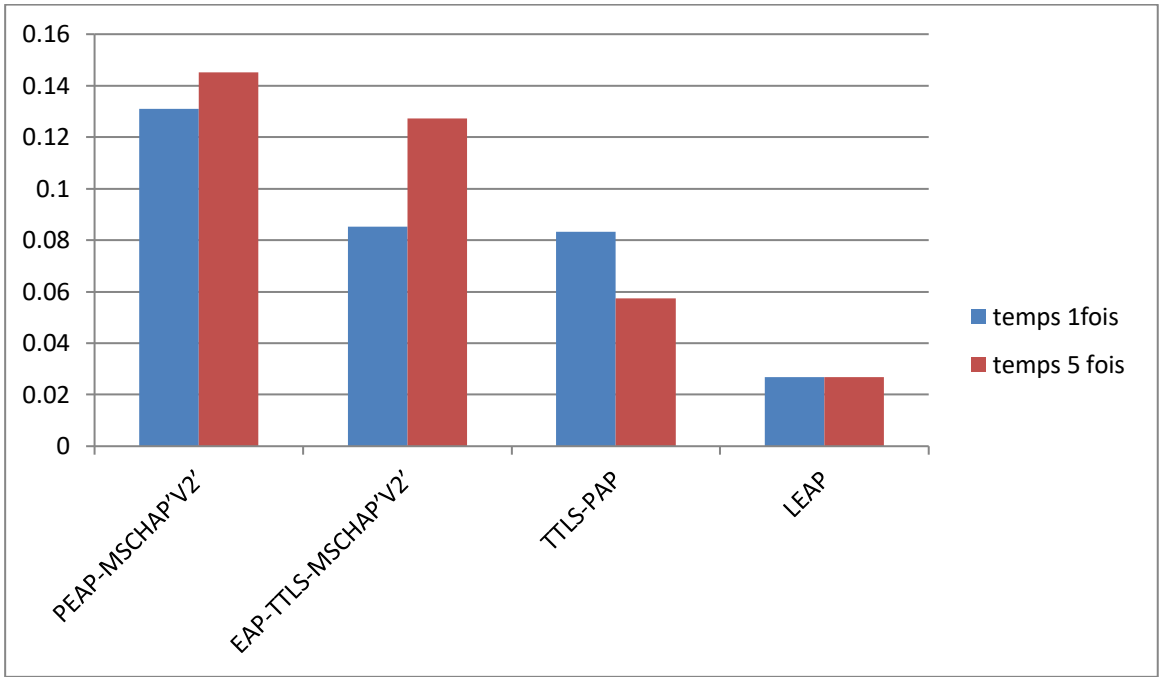


Figure IV-13 comparaison de temps d'authentification entre les types de EAP

IV.7) **Conclusion**

Pour les réseaux sans fil nous consignent d'utiliser LEAP parce que il est le plus rapide, en termes de sécurité TTLS-PAP il est recommandé.

Conclusion Générale

Nous rappelons que l'objectif de notre travail est l'étude l'implémentation et le test de la norme 802.1X dans un réseau sans fil « WiFi ». Avec comme objectif d'assurer la protection de ressource du réseau contre les tentatives de cyber-attaques et d'intrusions. Nous visons aussi une authentification par le protocole 802.1X, centralisé des utilisateurs afin de collecté des informations sur l'utilisations des ressources et mieux identifié les menaces.

Notre implémentation a commencée dans un premier temps par la configuration initiale des équipements de notre topologie, ensuite ,l'implémentation du « Port Based Authentification » puis, l'évaluation du déploiement des différents protocoles de l'authentification dans le réseau sans fil (EAP,PEAP,LEAP) ,enfin , on a assuré l'authentification et l'autorisation de la norme 802.1X dans le serveur ISE Cisco tout on assurons sa fiabilité on la testons .

Cette norme nous a donné des résultats concluants et très prometteurs, donc nous pouvons qualifiés notre protection comme fiable et efficace.

Ce mémoire nous a permis de nous familiarisé avec la notion de communication sans fil de comprendre son fonctionnement et avoir une idée sur ses enjeux expansion futur, et nous a fait prendre conscience de la nécessité d'avoir des réseaux sécurisés.

Annexe A

IV.8) Annexe A

IV.8.1) Configuration initiale

IV.8.1.1) Configuration du switch d'accès « authentificateur »

IV.8.1.1.1) Ajout d'un utilisateur d'administration

```
!
User name Utilisateur1 secret
Admin12 enable secret Admin123@
!
```

IV.8.1.1.2) Création des VLANs

```
!
vlan  1
name
Vlan1
vlan 2
name resVlan
vlan 3
name GuVlan
vlan 10
name
Vlan10 vlan
20 name
Vlan20
!
```

IV.8.1.1.3) Configuration de line vty

```
!
line vty 0 4
transport input all
!
```

IV.8.1.1.4) Configuration de l'interface VLAN 1

```
!
interface vlan 1
IP address 172.16.1.10 255.255.255.0
!
```

IV.8.1.1.5) **Configuration de l'interface connectée à l'ordinateur**

```
!
interface gigabitEthernet
0/11 switchport mode access
switchport access vlan 1
!
```

IV.8.1.1.6) **Configuration de l'interface connectée au serveur ISE**

```
!
interface gigabitEthernet
0/1 switchport mode access
switchport access vlan 1
!
```

IV.8.1.1.7) **Configuration de l'interface connectée au switch multi-layer en mode trunk**

```
!
interface gigabitEthernet 0/2
switchport mode trunk
!
```

IV.8.1.2) Configuration du switch multi-layer

IV.8.1.2.1) **Configuration du routage inter-vlan**

Création des VLANs

```
!
vlan  1
name
Vlan1
vlan 2
name resVlan
vlan 3
name GuVlan
vlan 10
name
Vlan10 vlan
```

Configuration de l'interface VLAN 1

```
!
interface vlan 1
IP address 192.168.1.20 255.255.255.0
!
```

IV.8.1.2.2) **Configuration de l'interface connectée au switch d'accès en mode trunk**

```
!
interface fastEthernet 0/1
switchport trunk encapsulation
dot1q switchport mode trunk
!
```

IV.8.1.2.3) **Activation de routage**

Configuration des SVI (Switch Virtual Interfaces)

```
!
interface vlan 1
IP address 172.16.1.20 255.255.255.0
no shutdown
interface
vlan 2
ip address 172.16.2.1 255.255.255.0
no shutdown
interface
vlan 3
ip address 172.16.3.1 255.255.255.0
no shutdown
interface
vlan 10
ip address 172.16.10.1 255.255.255.0
no shutdown
interface
vlan 20
ip address 172.16.20.1 255.255.255.0
```

Création des pools DHCP

```
!
ip dhcp pool one
network 172.16.1.0 255.255.255.0
default-router 172.16.1.20
ip dhcp pool two
network 172.16.2.0 255.255.255.0
default-router 172.16.2.1
ip dhcp pool three
network 172.16.3.0 255.255.255.0
default-router 172.16.3.1
ip dhcp pool four
network 172.16.10.0 255.255.255.0
default-router 172.16.10.1
ip dhcp pool five
network 172.16.20.0 255.255.255.0
default-router 172.16.20.1
!
```

IV.8.1.3) Les tests de connectivité

Test de connectivité entre le client (172.16.1.50) et le MLS (172.16.50.10)

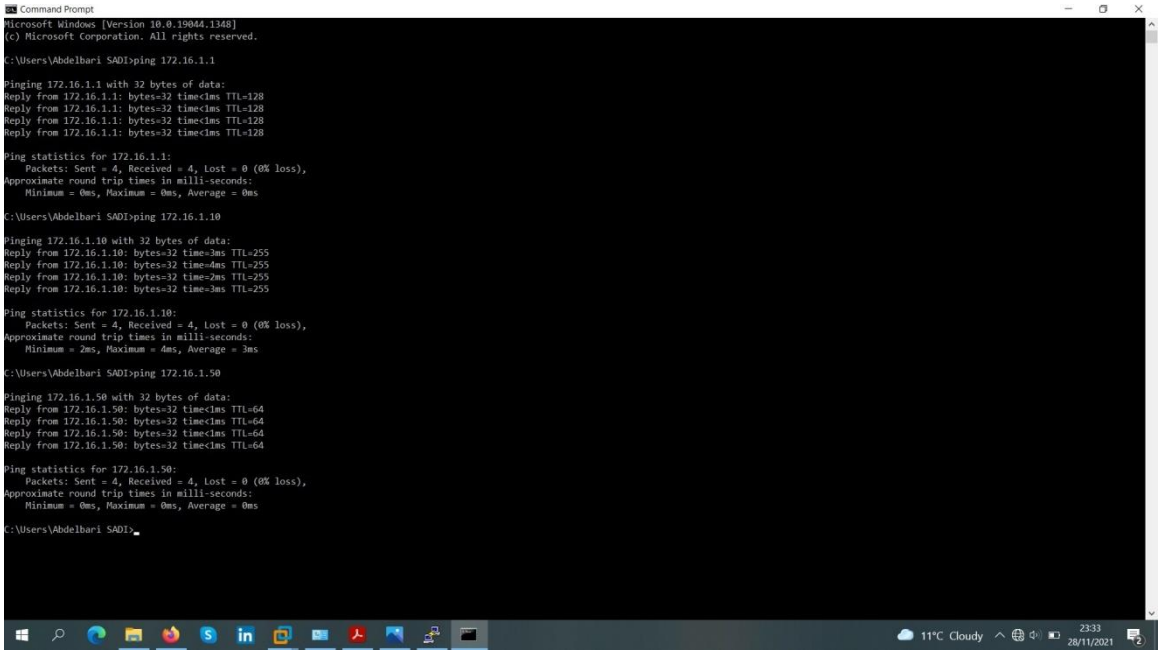


Figure IV-14 Test connectivité

IV.8.1.4) Implémentation de la méthode 802.1X

IV.8.1.4.1) Configuration initiale du modèle AAA

```
!
aaa new-model
aaa authentication login default group radius local aaa
authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
```

IV.8.1.4.2) Ajout du serveur Radius au niveau du switch d'accès

```
!
Radius server Ser-Radius
address ipv4 172.16.1.100 auth-port 1812 acct-port 1813
key cisco123 ip radius source-interface Vlan1 aaa
server radius dynamic-author
client 172.16.1.100 server-key cisco123 radius-server vsa
send authentica- tion
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth radius-server
attribute 8
include-in-access-req
!
```

IV.8.1.5) Configuration du « Port-Based Authentication

IV.8.1.5.1) Configuration du « Port-Based Authentication » au niveau de switch :

```
!
dot1x system-auth-control interface gigabitEthernet 0/11
switchport mode access
spanning-tree portfast spanning-tree bpduguard enable
authentication port-control auto authentication host-
mode multi-auth authentication open
dot1x aep authenticator exit
!
```

IV.8.1.5.2) Configuration du « Port-Based Authentication » au niveau du serveur ISE

En accédant à l'adresse IP de gestion d'ISE, qui est 172.16.50.254, l'écran suivant apparaîtra.

Configuration du « Port-Based Authentication » au niveau du serveurISE

En accédant à l'adresse IP de gestion d'ISE, qui est 172.16.50.112,l'écran suivant apparaîtra.

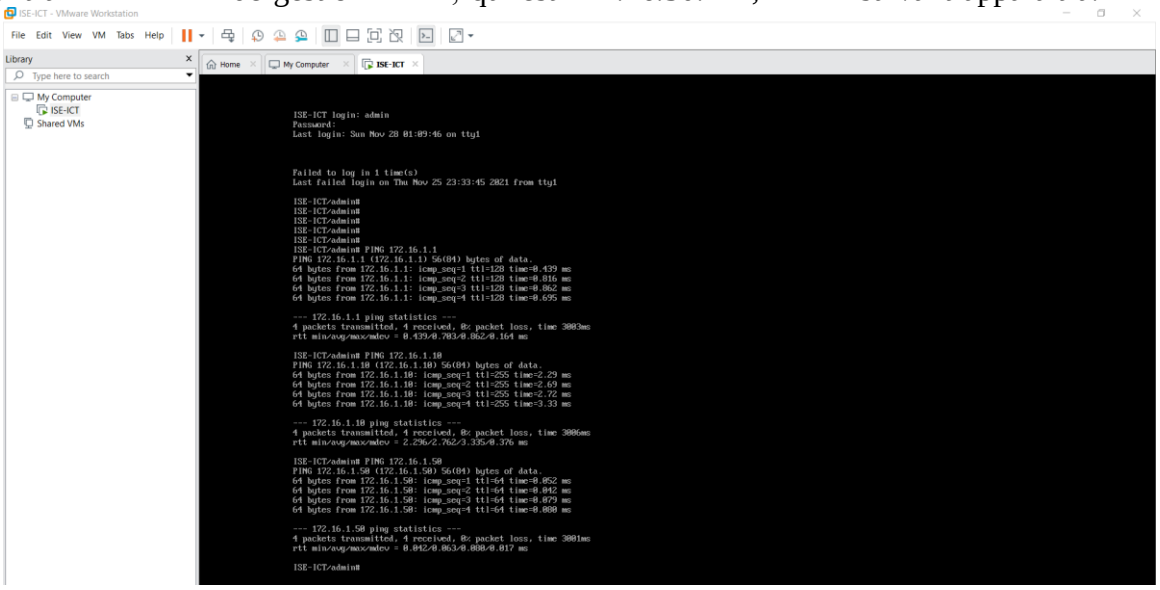


Figure IV-15 test connectivité 2

Annexe A

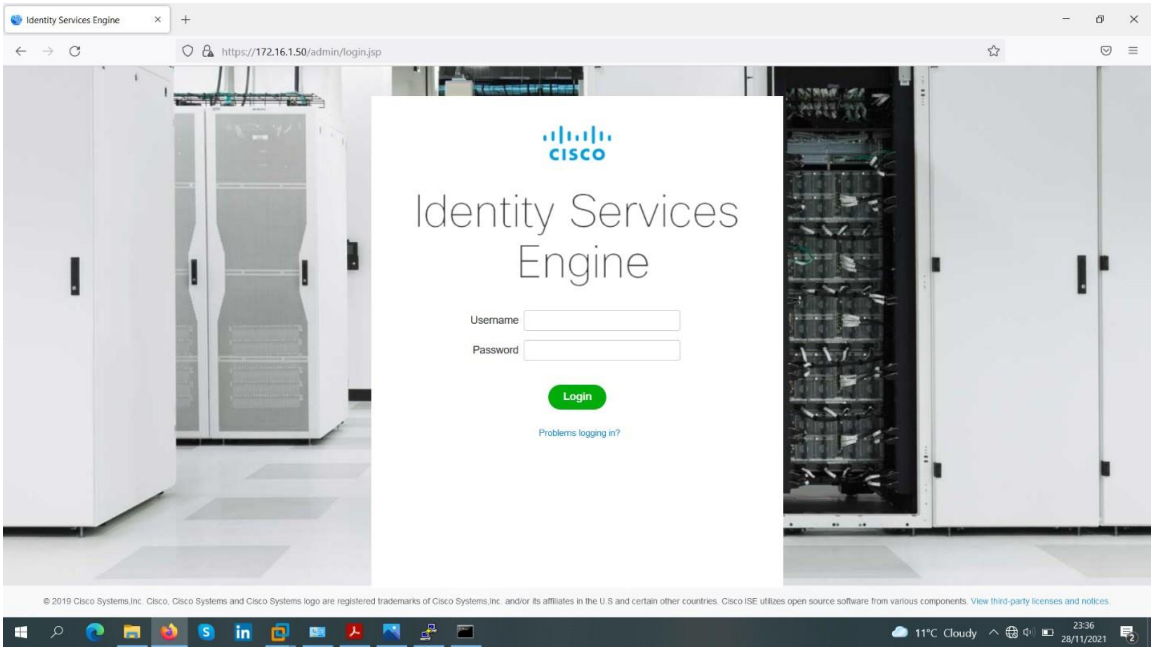


Figure IV-16 Ecran de gestion du serveur ISE

Annexe B

IV.9) Annexe B

IV.9.1) Configuration du « Point d'Accès »

Etape 1 : configuration du protocol

On va sur < Managment > puis sur < Admin Accounts >

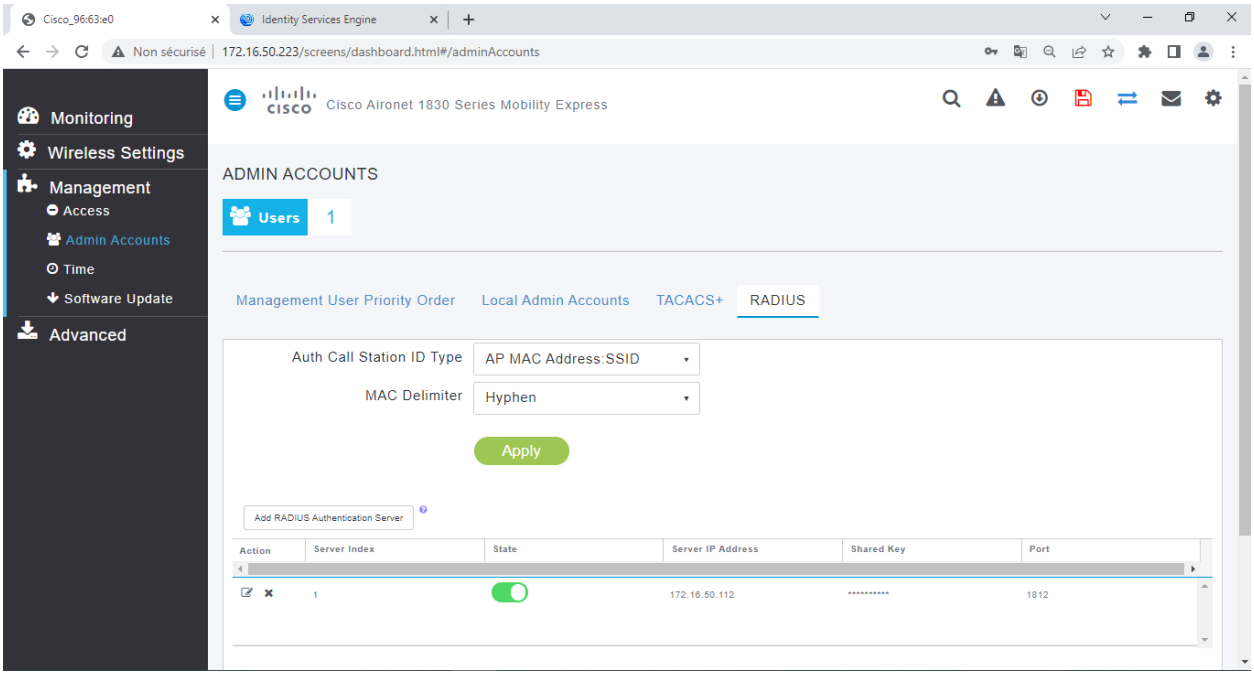


Figure IV-17 configuration du protocol

Etape 2 : On doit activer le Radius sur notre point accès pour que le client se authentifier lorsqu'il veut entrer sur notre réseau, on clique sur ADD radius authentication server comme il est présenté dans la figure suivante

Annexe B

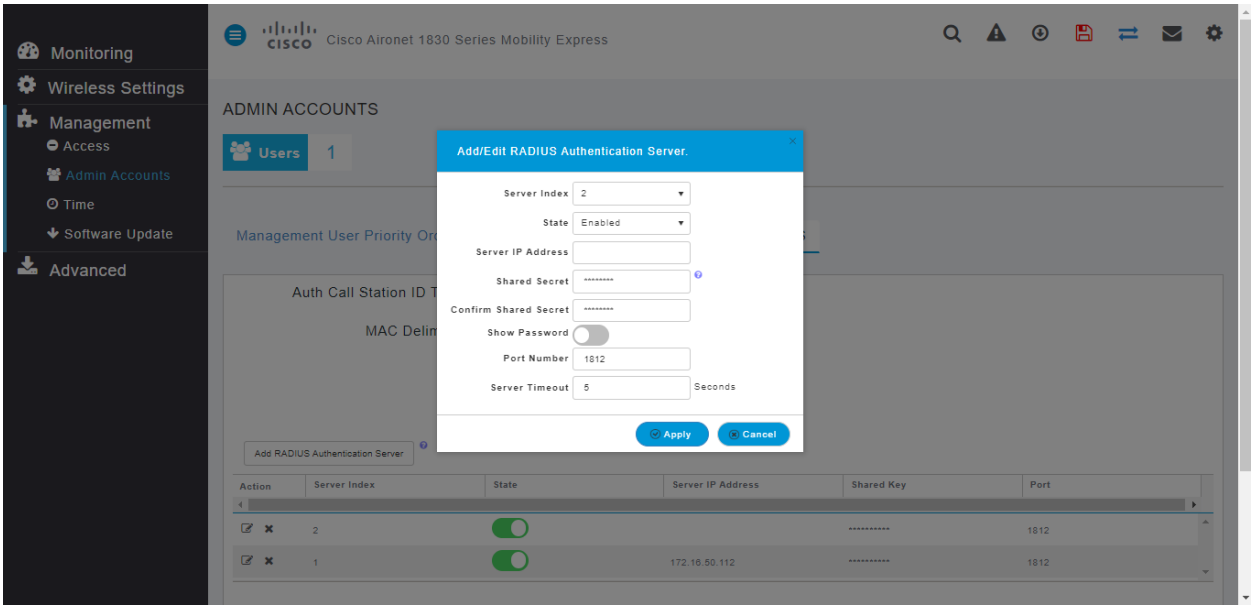


Figure IV-18 activation le Radius sur notre point accès

Etape 3 : On choisie state Enable et on crée un mode passe qui est le même pour accède au serveur ISE.

On va crée un WLANs on clique dans la fenêtre de AP sur Wireless Settings puis sur WLANS comme vous voyez la figure suivante

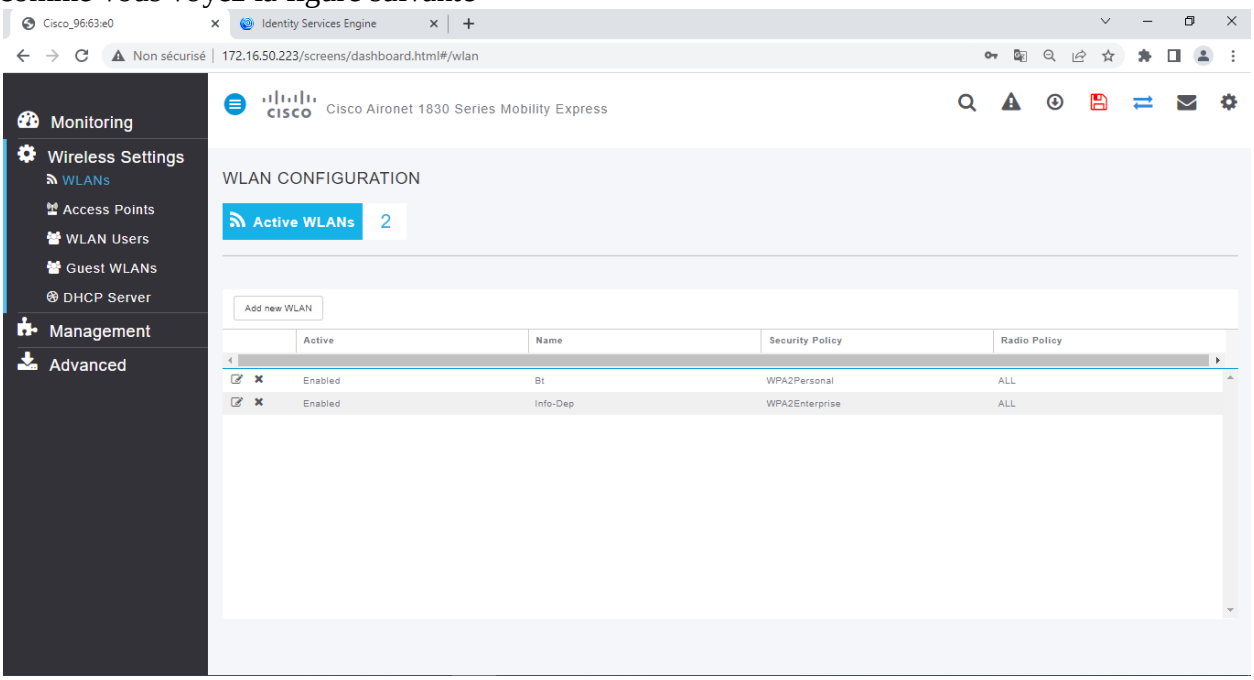


Figure IV-19 création de WLan

Annexe B

ADD new wlans :

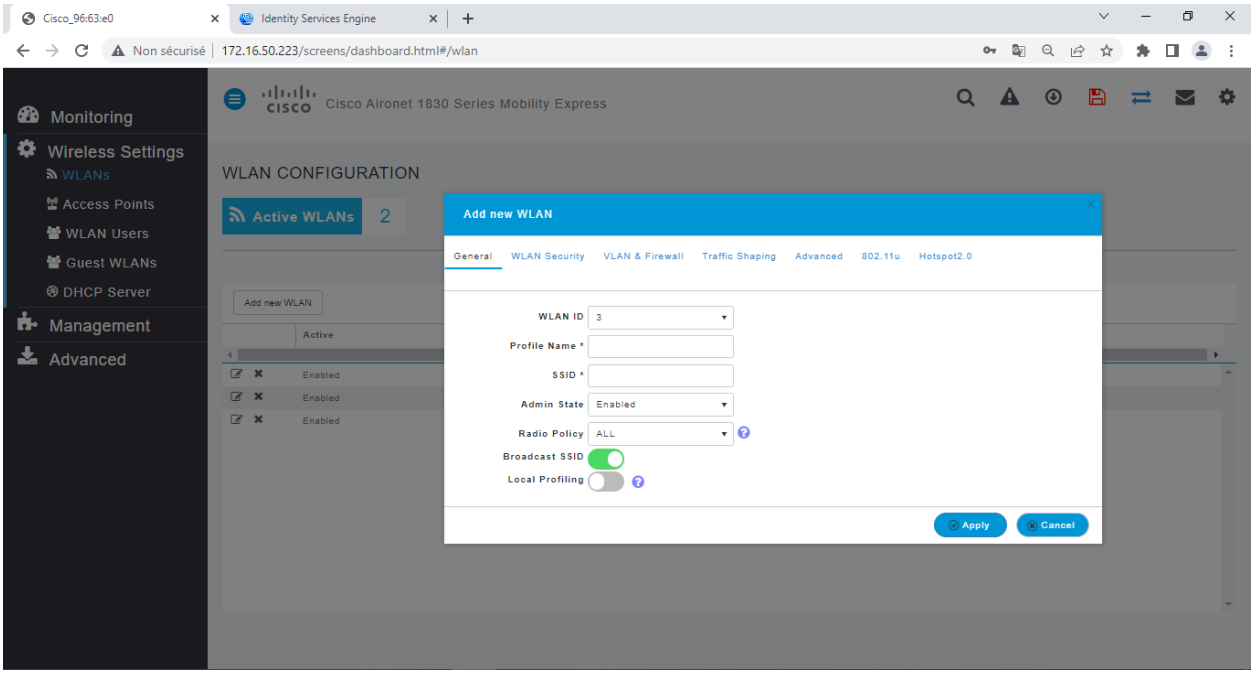
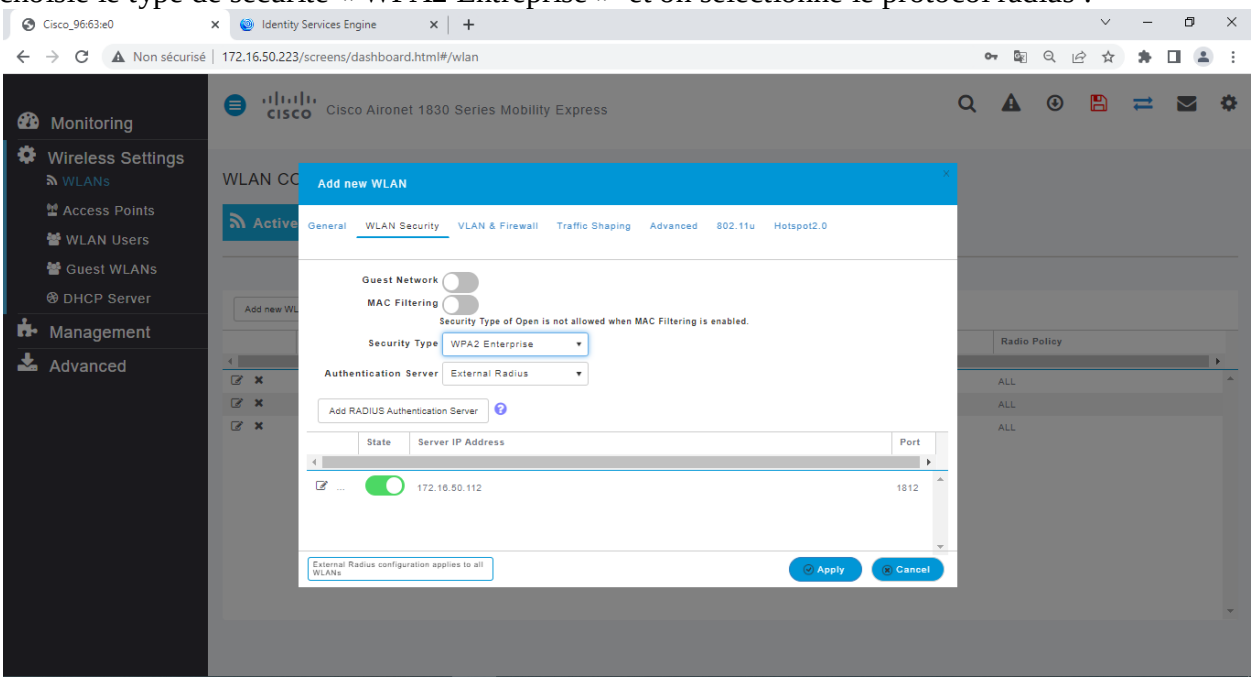


Figure IV-20 add WLan

on remplie les cases par les informations qui conviens ;ensuite on va sur Wlans sécurity et on choisie le type de sécurité « WPA2 Entreprise » et on sélectionné le protocol radius :



Annexe B

IV.9.2) Configuration du « Port-Based au Authentification »au niveau du serveur ISE

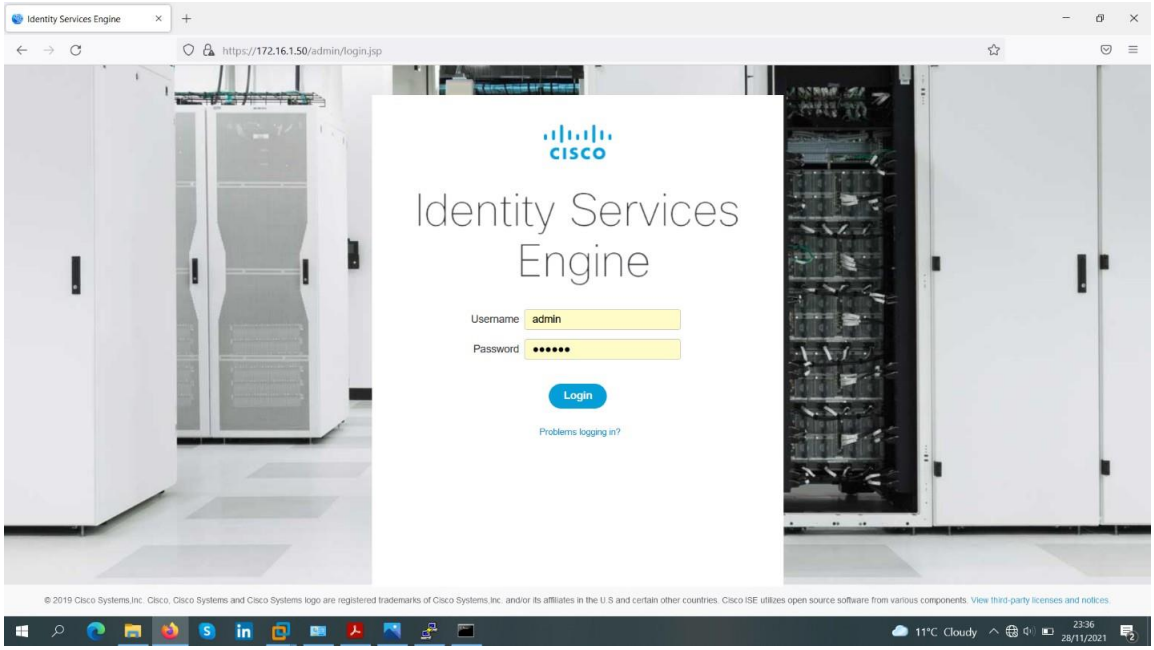


Figure IV-21 Connexion à le serveur ISE

En utilisant le nom d'utilisateur et le mot de passe appropriés, le tableau de bord suivant apparaîtra, après une connexion réussie.

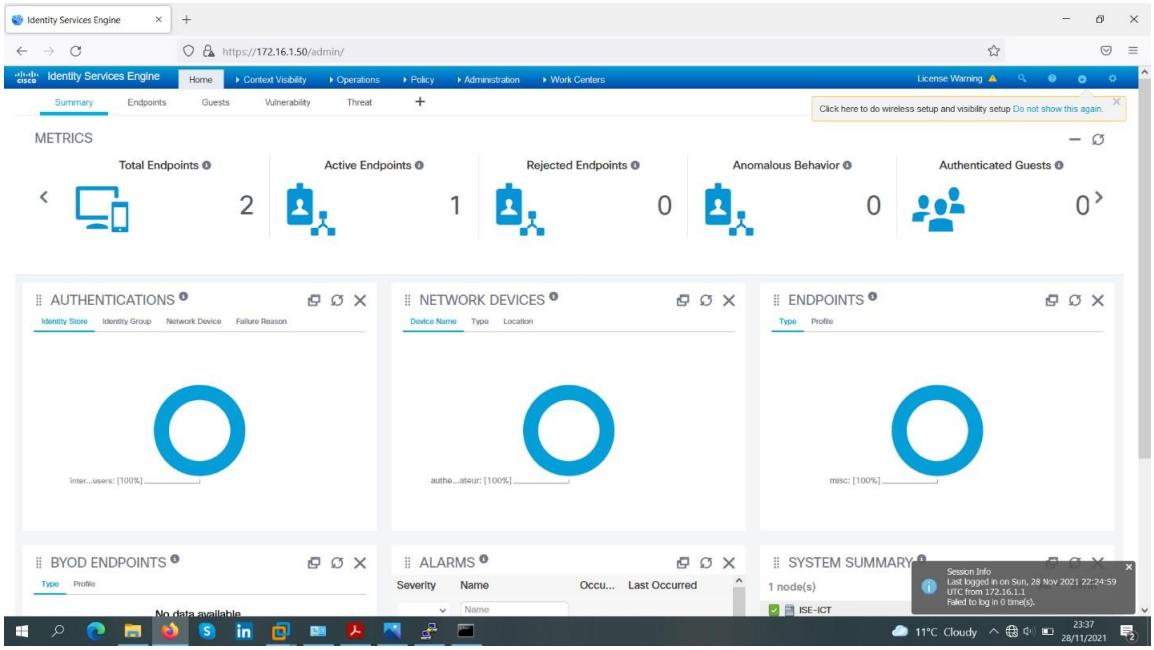


Figure IV-22 Ecran d'accueil du serveur ISE

IV.9.3) **Ajout de l'équipement réseau (switch d'acces)**

Afin d'ajouter un équipement réseau, nous avons suivi les étapes suivantes :

Etape 1 : Nous avons cliqué sur :

"**Administration**" > "**Network Ressource**" > "**Network Devices**" > "**Network Devices**".

L'écran suivant apparaîtra.

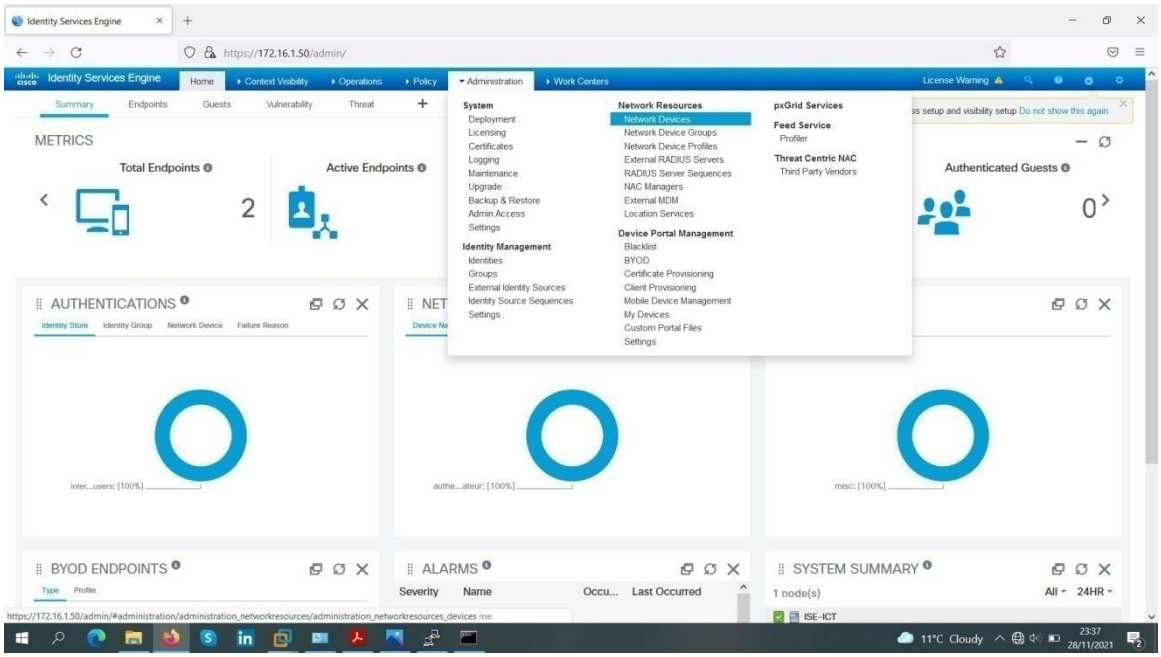


Figure IV-23 Etape 1 de l'ajout de l'équipement réseau.

Etape 2 : Nous avons cliqué sur "ADD"

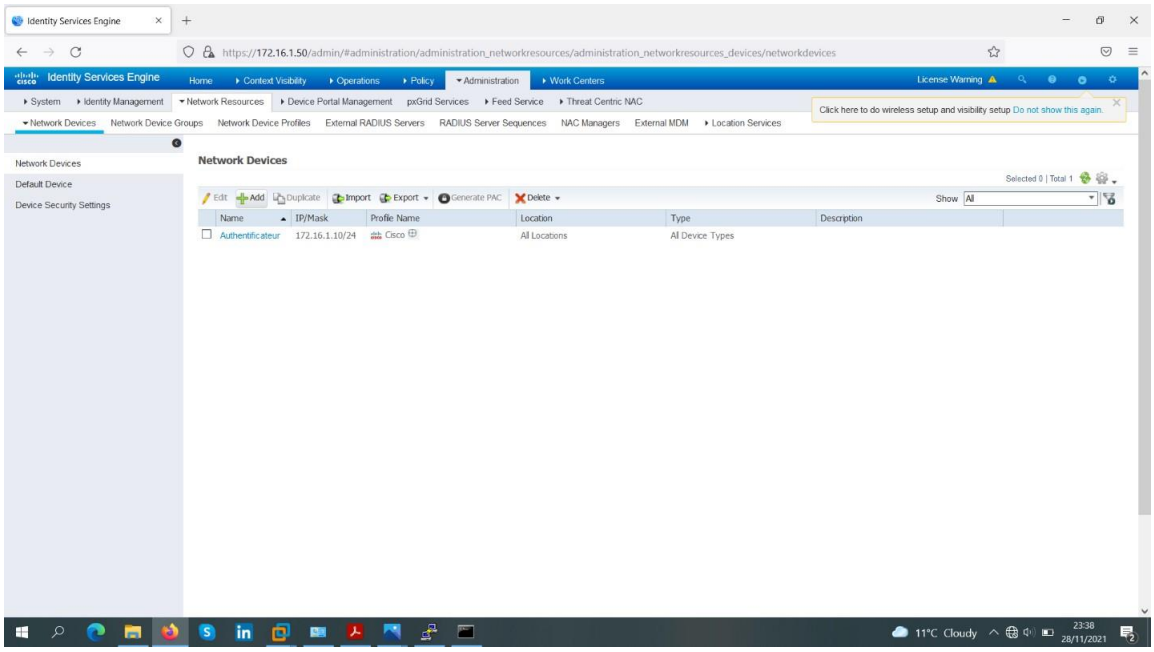


Figure IV-24 Etape 2 .l'ajout de l'équipement réseau.

Etape 3 : Nous avons rempli les champs par les informations suivantes :
Name : Authentificator
IP Address : 172.16.2.10 / 24

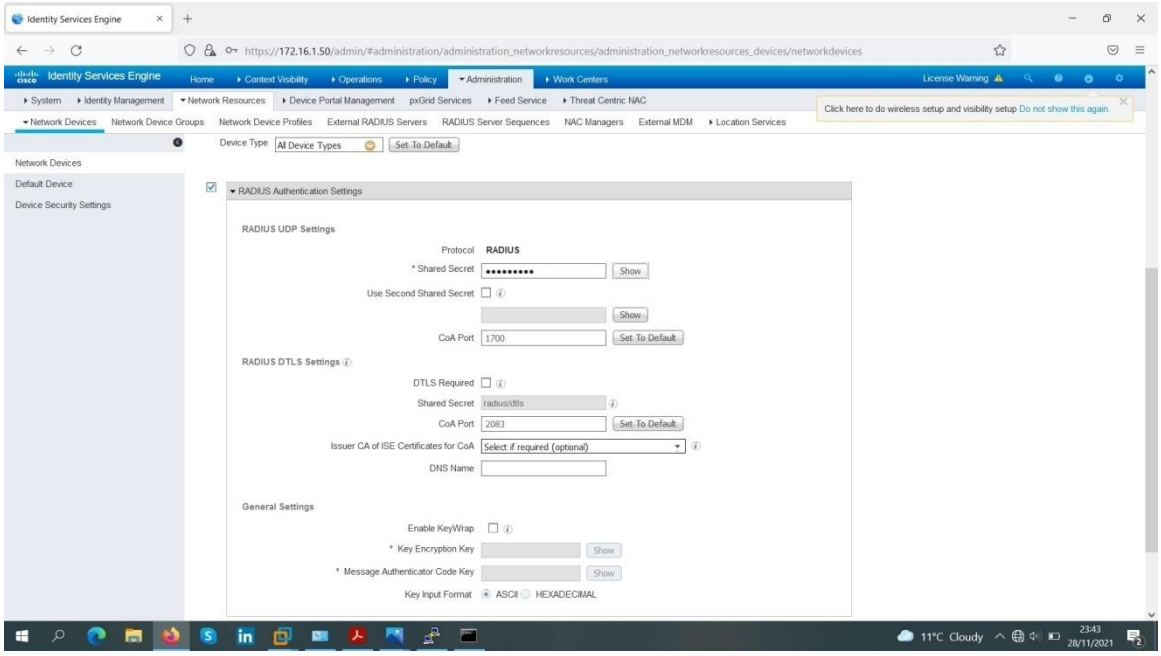


Figure IV-25 Etape 3 de l'ajout de l'équipement réseau.

Etape 4 : Nous avons coché l'option "RADIUS Authentication Settings" et nous avons rempli le champ du "Shared Secret" par la clé secrète partagée, qui est "cisco123", entre le serveur ISE et le switch d'accès (Authentificateur).

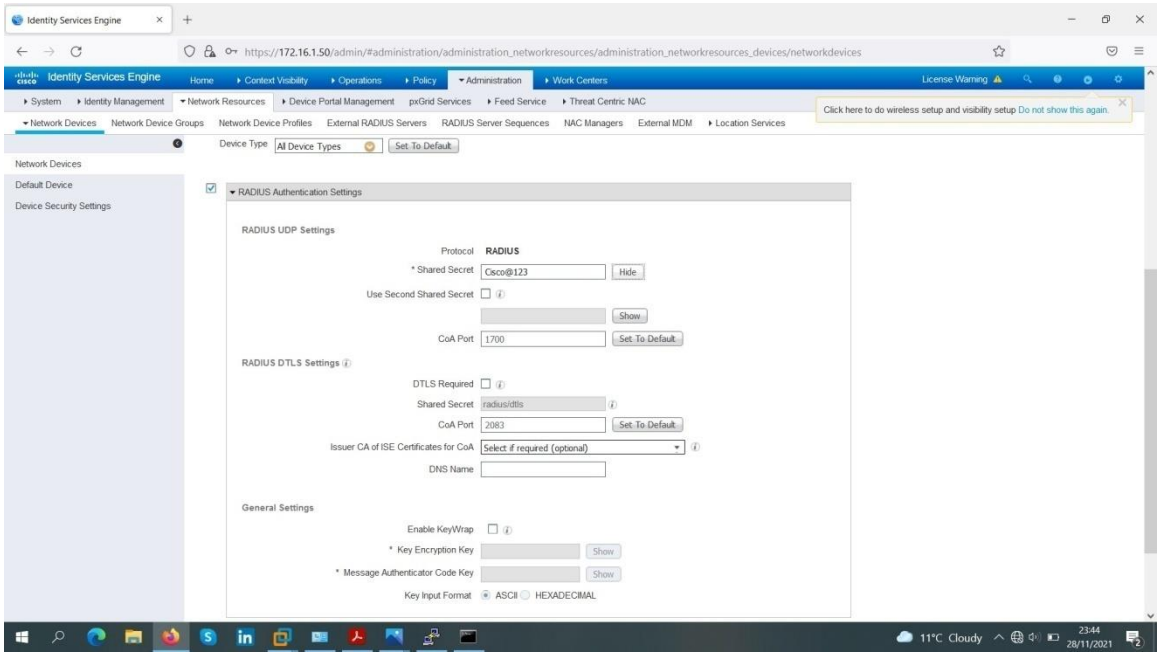


Figure IV-26 Etape 4 de l'ajout de l'équipement réseau.

Etape 5 : Nous avons cliqué sur “Submit” pour appliquer les changements.

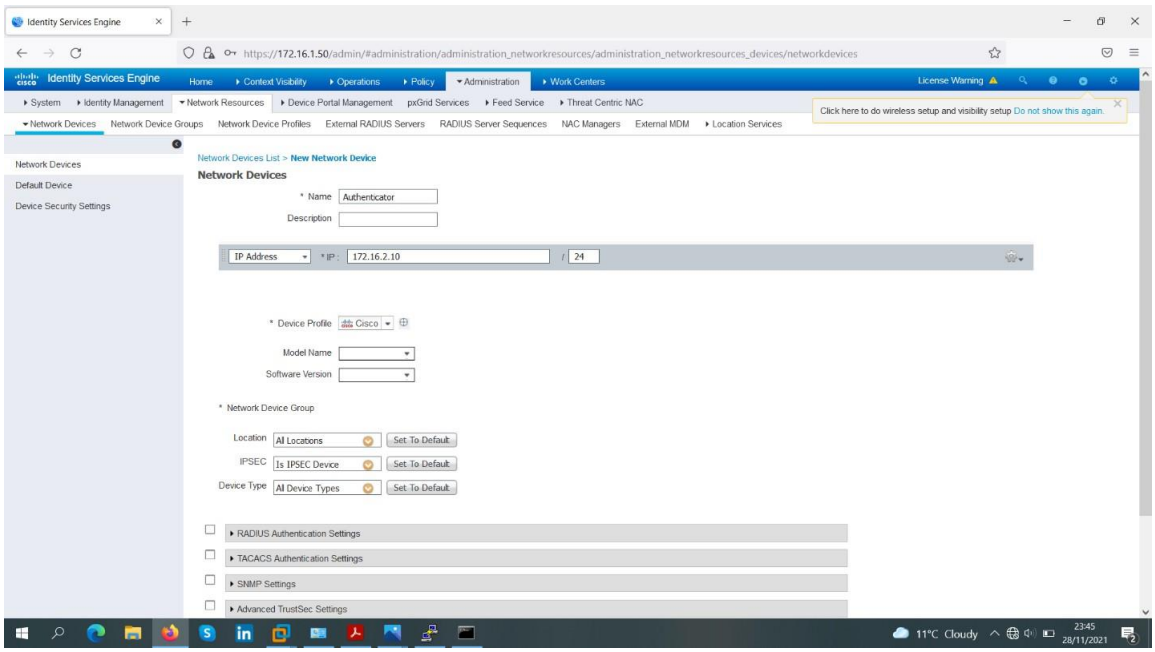


Figure IV-27 Etape 5 :l’ajout de l’équipement réseau.

Enfin, l’écran suivant apparaîtra.

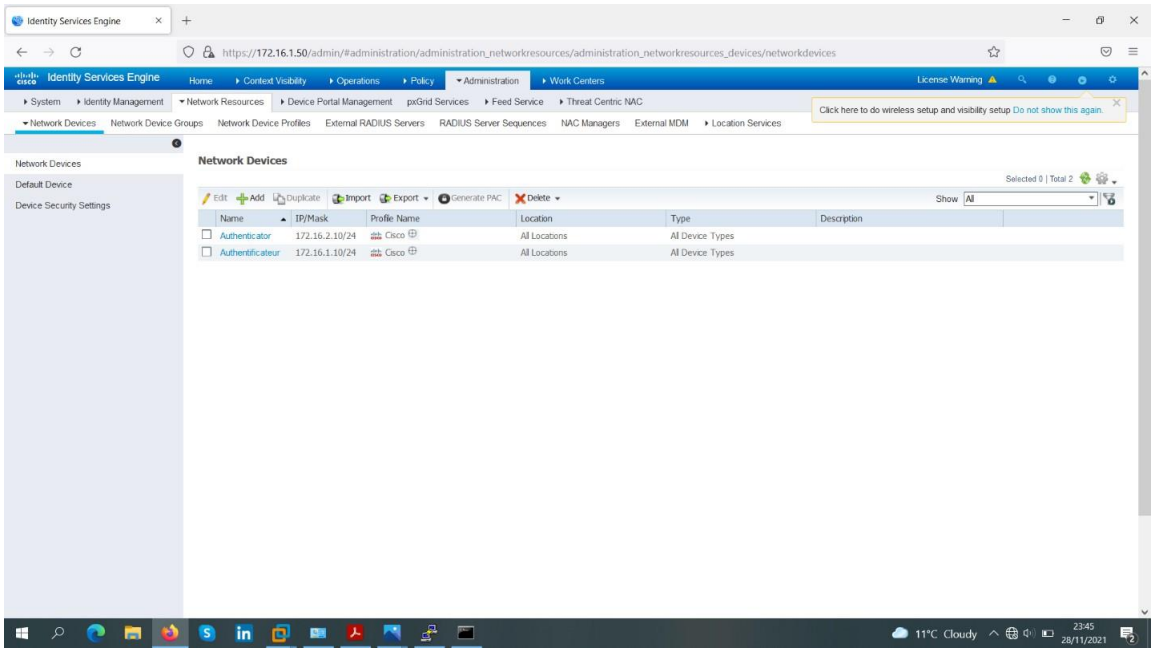


Figure IV-28 vérification l’ajout de l’équipement réseau.

IV.9.4) **Ajout de groupes d’identité d’utilisateurs (User Identity Groups)**

Afin d’ajouter des groupes d’identité d’utilisateurs, Nous avons suiviles étapes suivantes :
Etape 1 : Nous avons cliqué sur : “Administration” > “Identity Management” > “Groups” > “User Identity Groups”, l’écran suivant apparaîtra.

Annexe B

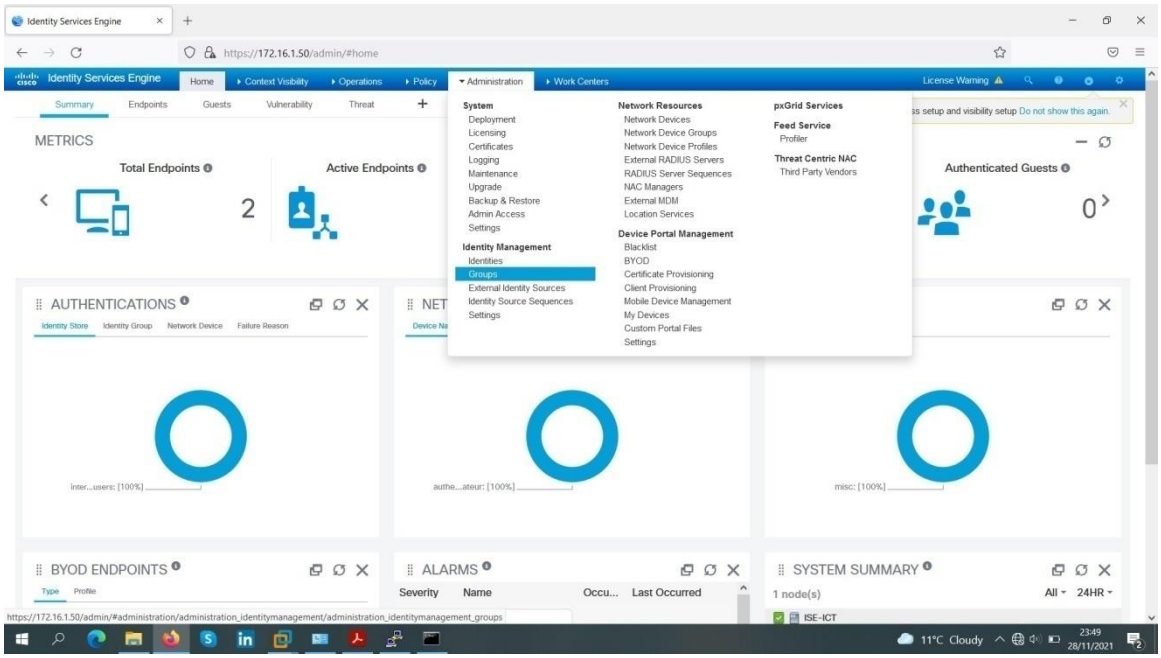


Figure IV- IV-29 confirmation de l'ajout de l'équipement réseau.

Etape 2: Nous avons cliqué sur "ADD".

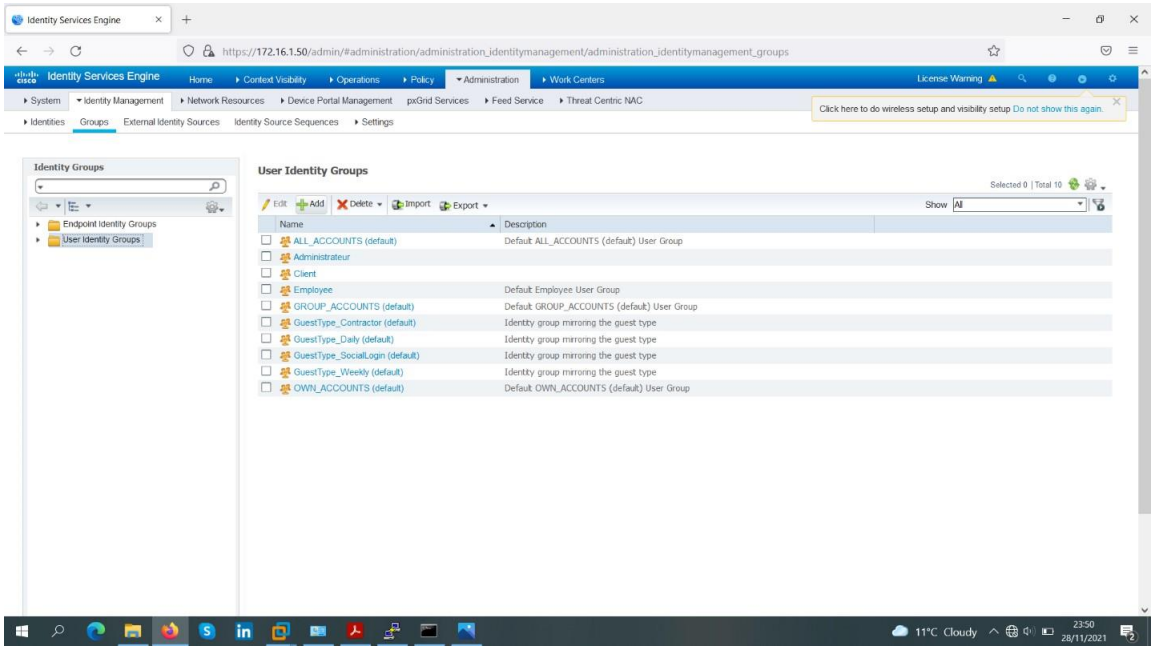


Figure IV-30 Etape 1 de l'ajout de groupes d'identité d'utilisateurs

Etape 3 : Nous avons ajouté un premier groupe en remplissant le champ"Name" par "Student".

Annexe B

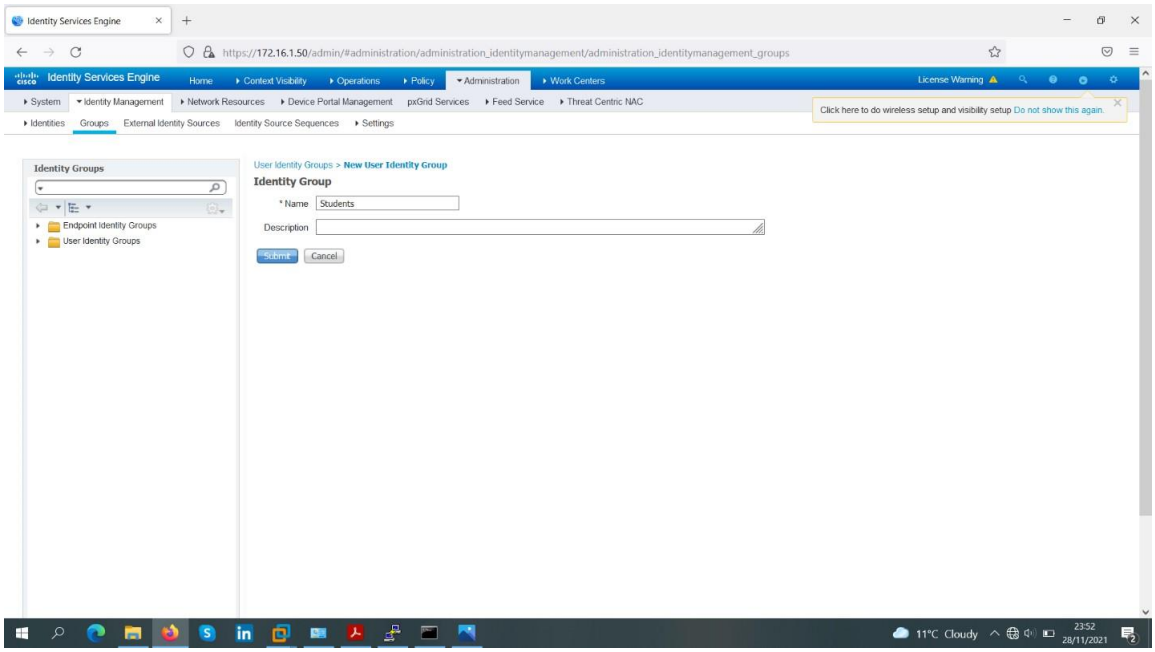


Figure IV-31 Etape 2 de l'ajout de groupes d'identité d'utilisateurs.

Etape 4 : Nous avons cliqué sur "ADD" et nous avons ajouté un deuxième groupe en remplissant le champ "Name" par "Teacher".

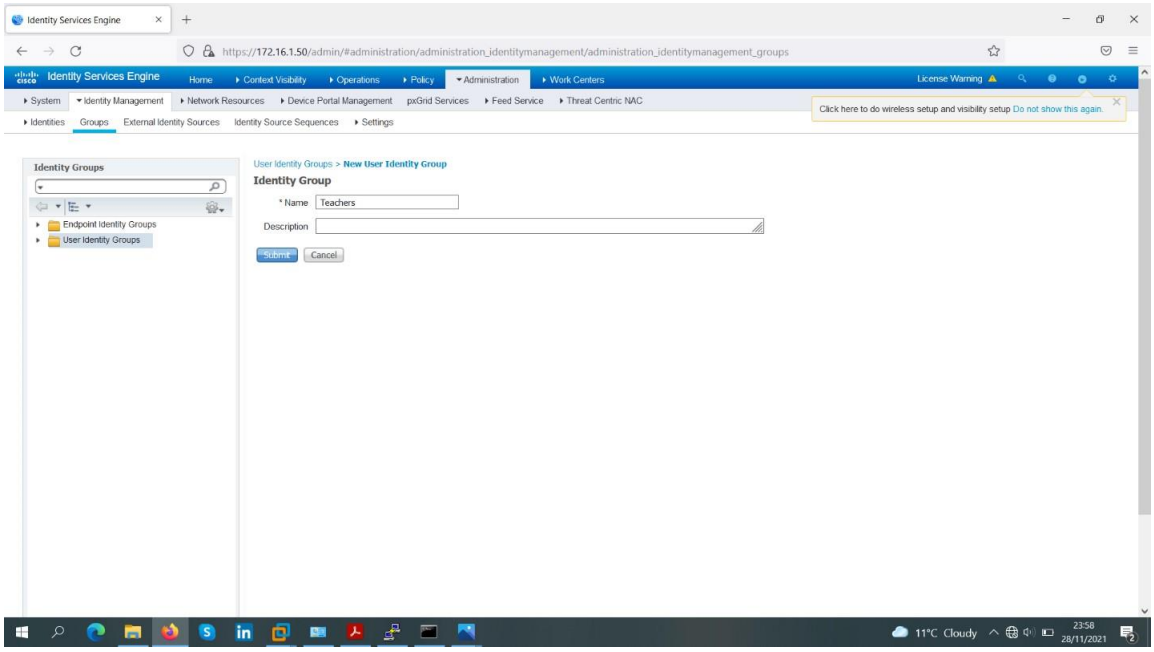


Figure IV-32 Etape 3 de l'ajout de groupes d'identité d'utilisateurs.

Etape 5 : Nous avons cliqué sur "Submit" pour appliquer les changements.

Annexe B

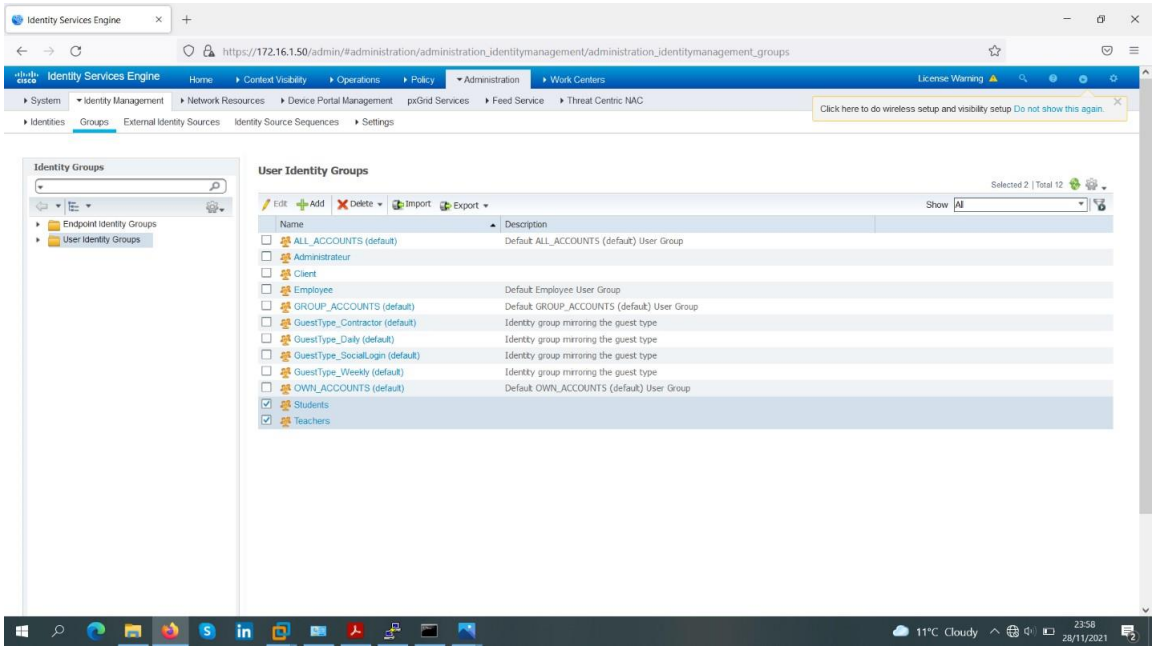


Figure IV-33 Etape 4 de l'ajout de groupes d'identité d'utilisateurs

IV.9.5) **Ajout d'utilisateurs (Users)**

Afin d'ajouter des utilisateurs, nous avons suivi les étapes suivantes :

Etape 1 : Nous avons cliqué sur : "Administration" > "Identity Management" > "Identities" > "Users", l'écran suivant apparaîtra.

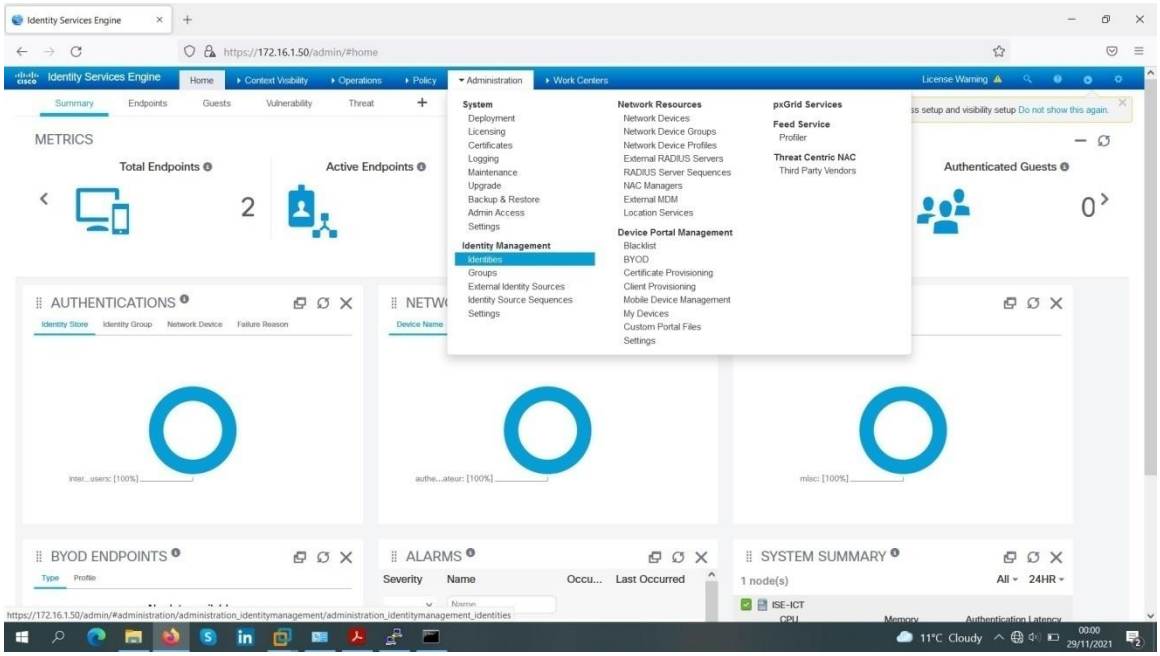


Figure IV-34 Etape 0 de l'ajout d'utilisateurs

Etape 2 : Nous avons cliqué sur "ADD".

Annexe B

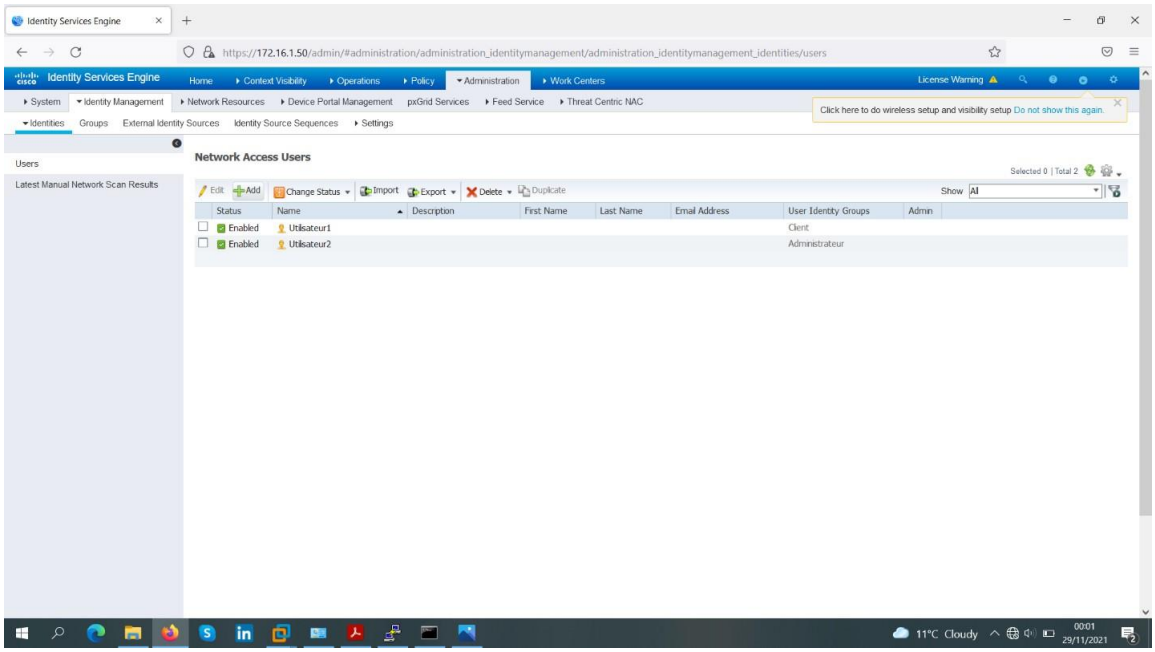


Figure IV-35 Etape 1 de l'ajout d'utilisateurs

Etape 3 : Nous avons ajouté un premier utilisateur en remplissant leschamps "Name" et "Login Password" par les informations suivantes :
- Name: Student1
- Login Password : (Password : kamel@1234)
(Re-enter Password : kamel@1234)

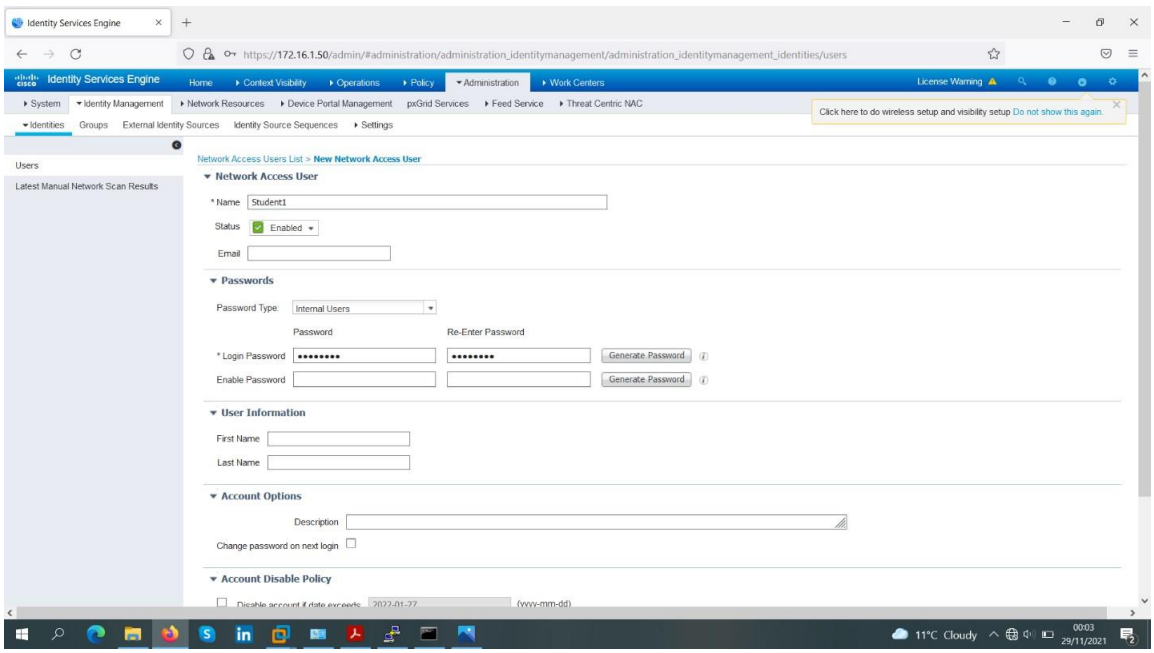


Figure IV-36 Etape 2 de l'ajout d'utilisateurs

Dans la section "User Groups", nous avons cliqué sur "Select an item ". Ensuite, nous avons choisi l'option "User Identity Group" et enfin nous avons choisi le groupe "Student".

Annexe B

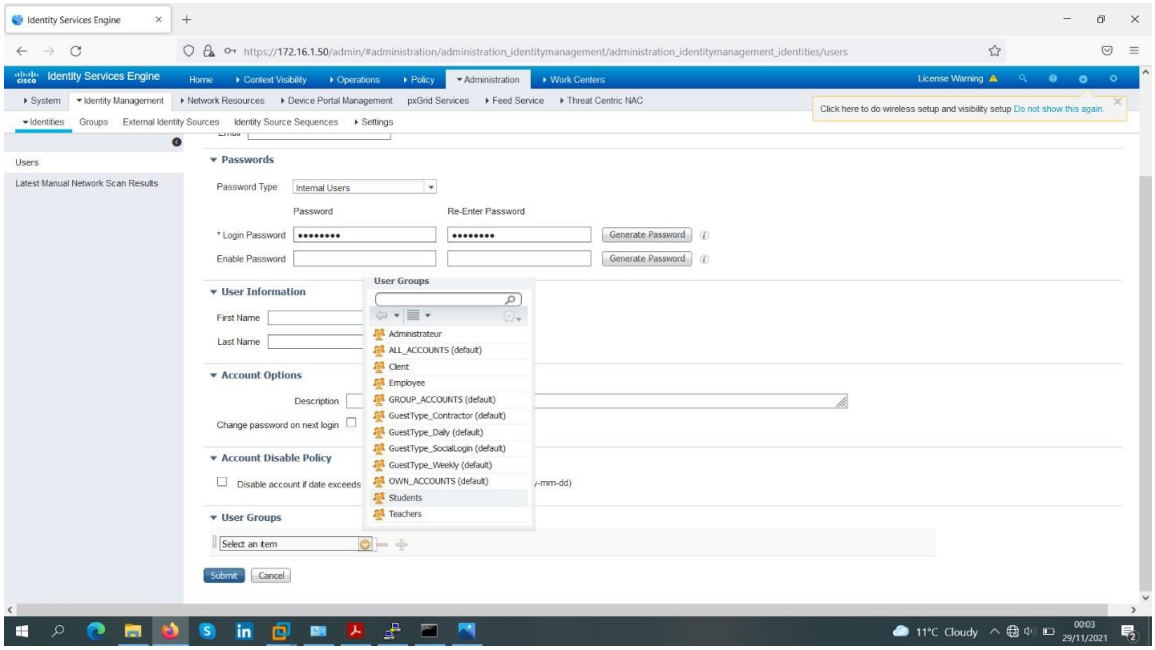


Figure IV-37 Etape 3 de l'ajout d'utilisateurs.

Etape 5 : Nous avons cliqué sur "Submit" pour appliquer les changements.

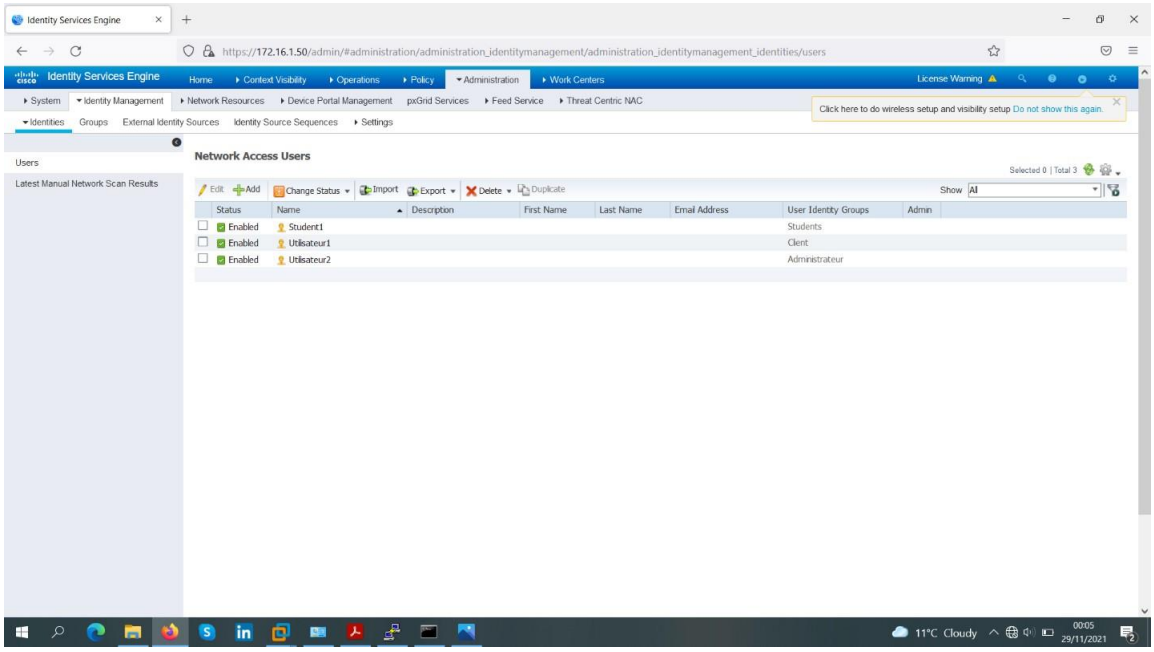


Figure IV-38 vérification de liste d'utilisateurs.

Etape 6 : Nous avons ajouté un deuxième utilisateur en remplissant leschamps "Name" et "Login Password" par les informations suivantes :
- Name : teacher1
- Login Password : (Password : Saadallah@123)
(Re-enter Password : Saadallah@123)

Annexe B

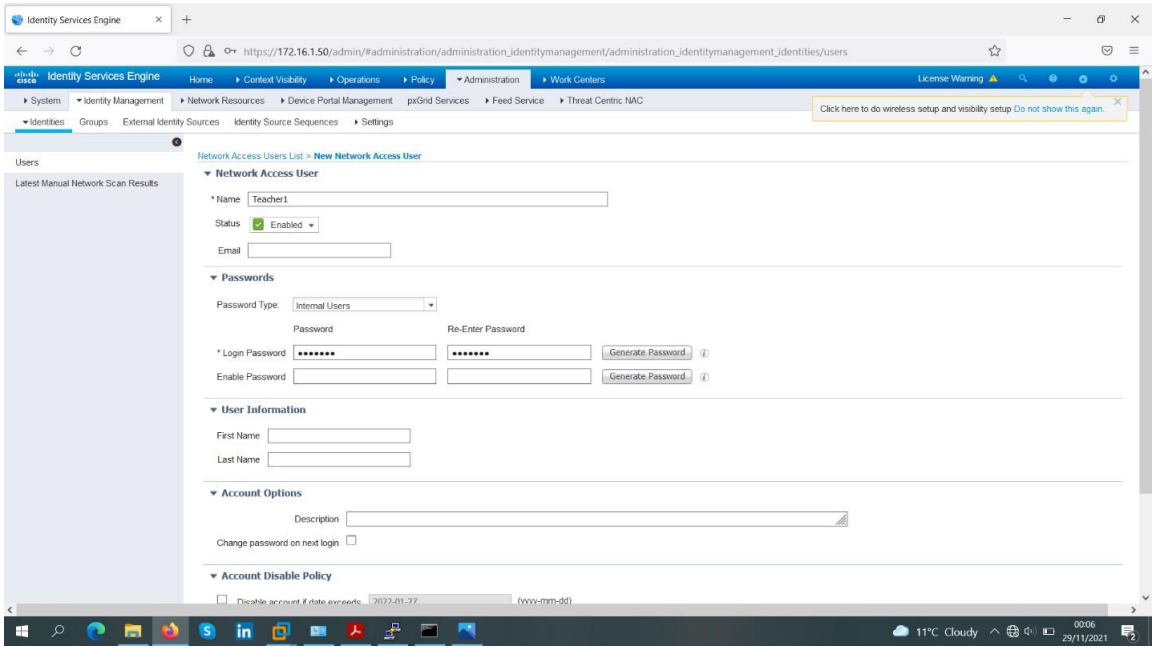


Figure IV-39 Etape 4 de l'ajout d'utilisateurs.(user2)

Etape 7 : Nous avons ajouté le deuxième utilisateur au groupe de 'Teacher '.

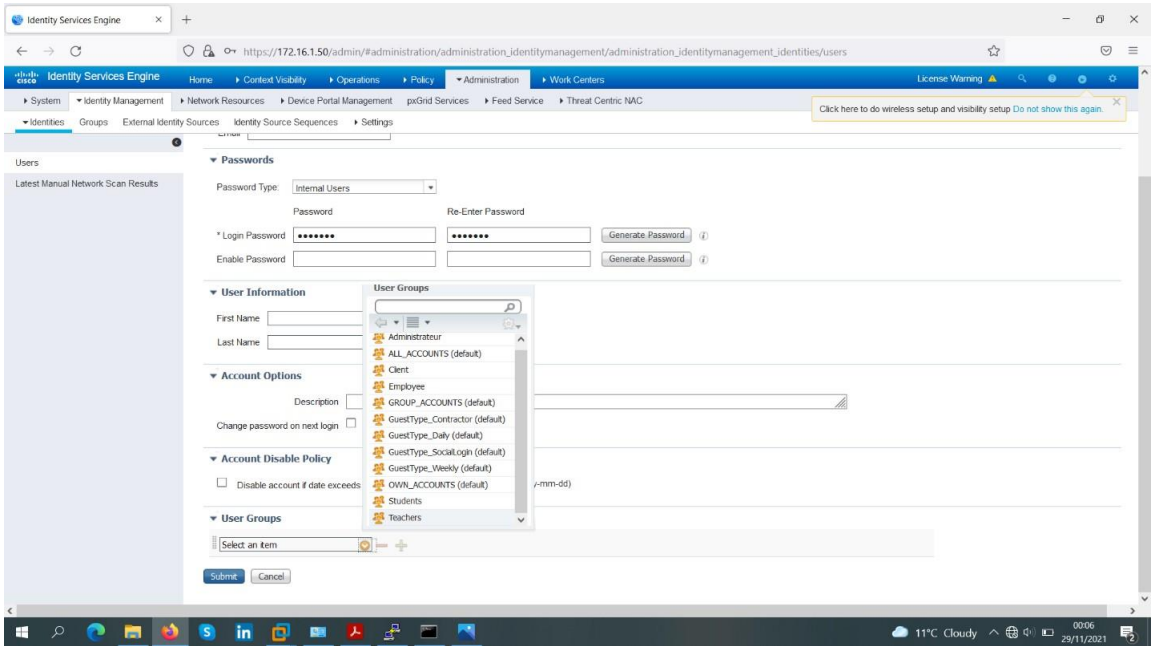


Figure IV-40 Etape 5 de l'ajout d'utilisateurs.

Etape 8 : Nous avons cliqué sur "Submit" pour appliquer les changements.

Annexe B

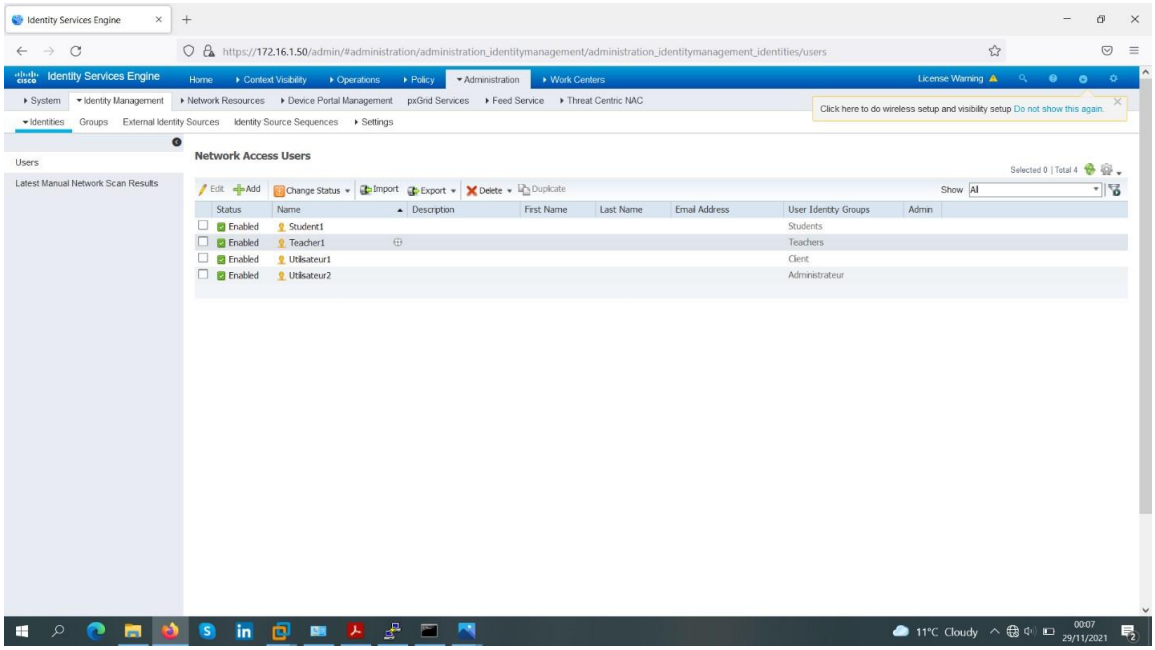


Figure IV-41 l'ajout de l'équipement réseau.

IV.9.6) **Ajout de protocoles d'authentification (Allowed Protocols)**

Afin d'ajouter des protocoles spécifiques d'authentification, nous avons suivi les étapes suivantes :

Etape 1 : Nous avons cliqué sur : "Policy" > "Policy Elements" > "Results" > "Authentication" > "Allowed Protocols", l'écran suivant apparaîtra.

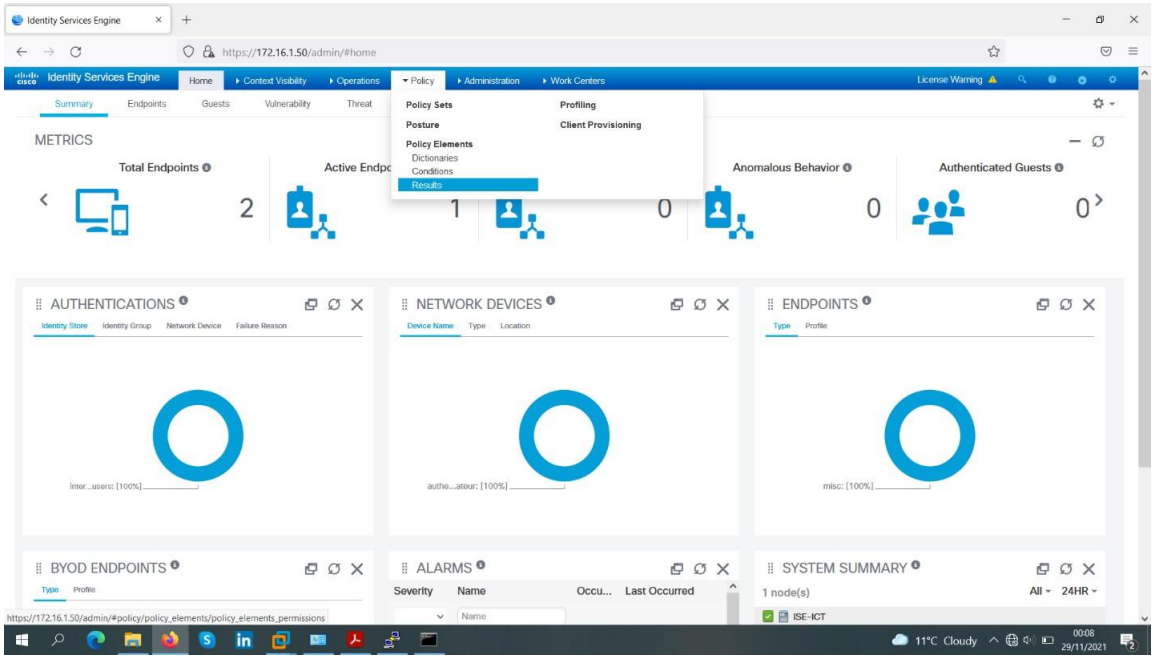


Figure IV-42 Etape 0 de l'ajout de protocoles d'authentification.

Etape 2 : Nous avons cliqué sur "ADD".

Annexe B

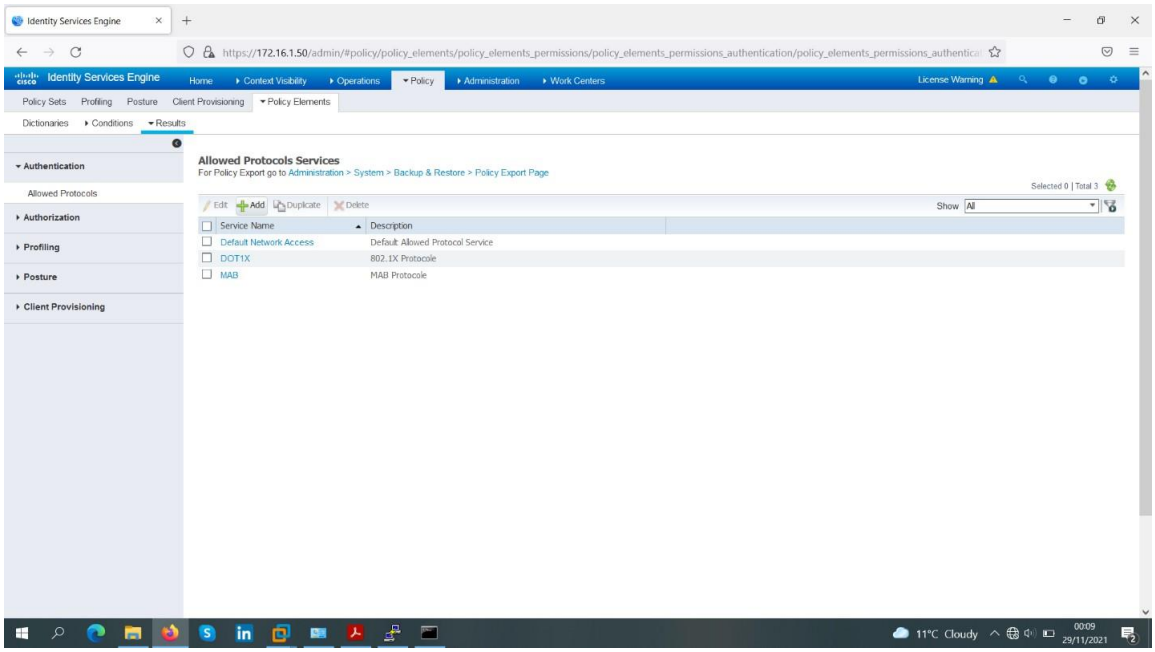


Figure IV-43 Etape 1 de l'ajout de protocoles d'authentification.

Etape 3 : Nous avons ajouté un premier protocole d'authentification 802.1X en remplissant le champ "Name" par "authentication 802.11x".

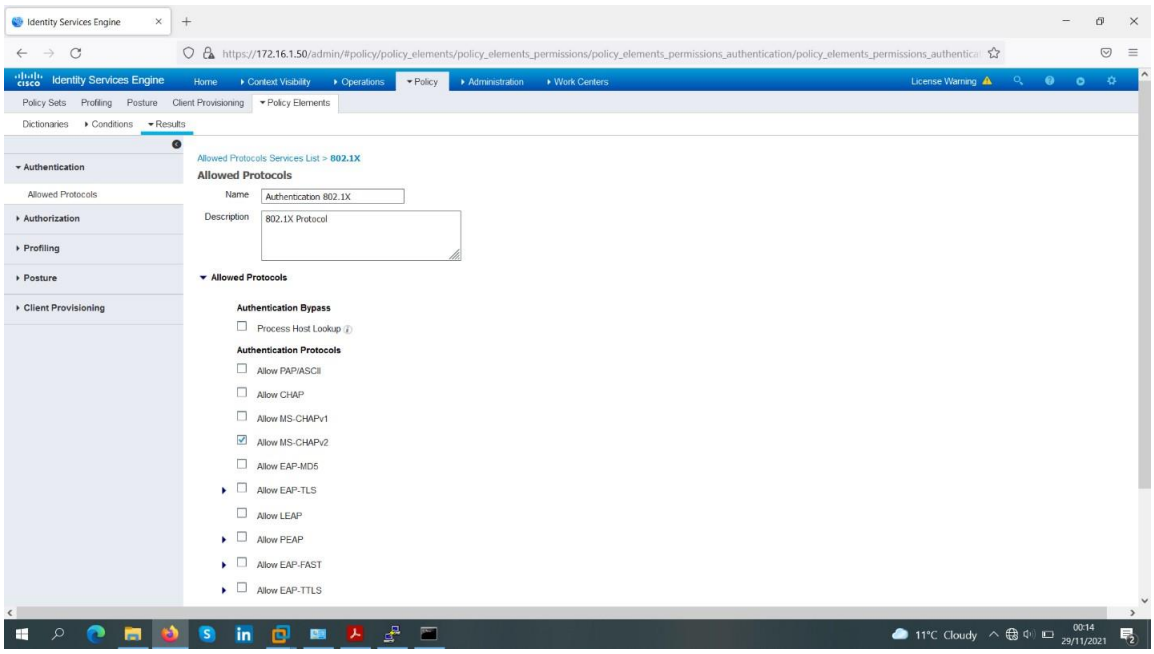


Figure IV-44 Etape 2 de l'ajout de protocoles d'authentification.

Etape 5 : Nous avons cliqué sur "Submit" pour appliquer les changements.

Annexe B

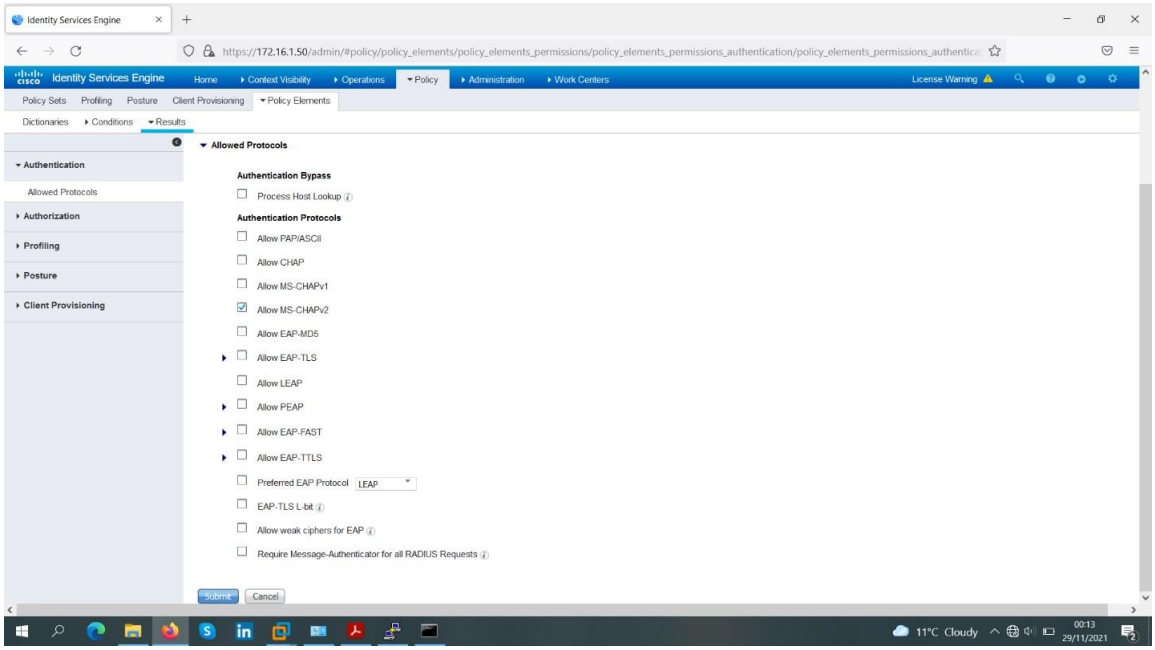


Figure IV-45 Etape 3 de l'ajout de protocoles d'authentification.

IV.9.7) Ajout de politiques d'authentification (Authentication Policy)

Afin d'ajouter des politiques d'authentification, nous avons suivi lesétapes suivantes :
Etape 1 : Nous avons cliqué sur : "Policy" > "Authentication", l'écransuivant apparaîtra.

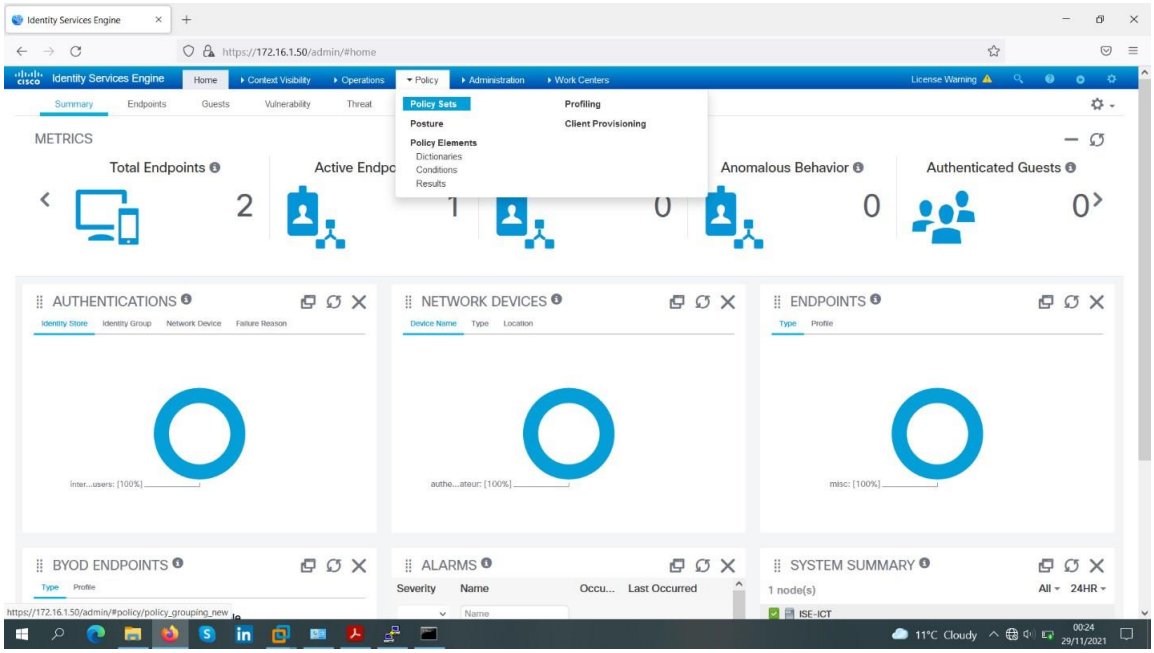


Figure IV-46 Etape 1 de l'ajout de politiques d'authentification

Etape 2 : Nous avons cliqué sur la flèche qui se trouve à côté de l'option "Edit" et nous avons choisi l'option "Insert new row below".

Annexe B

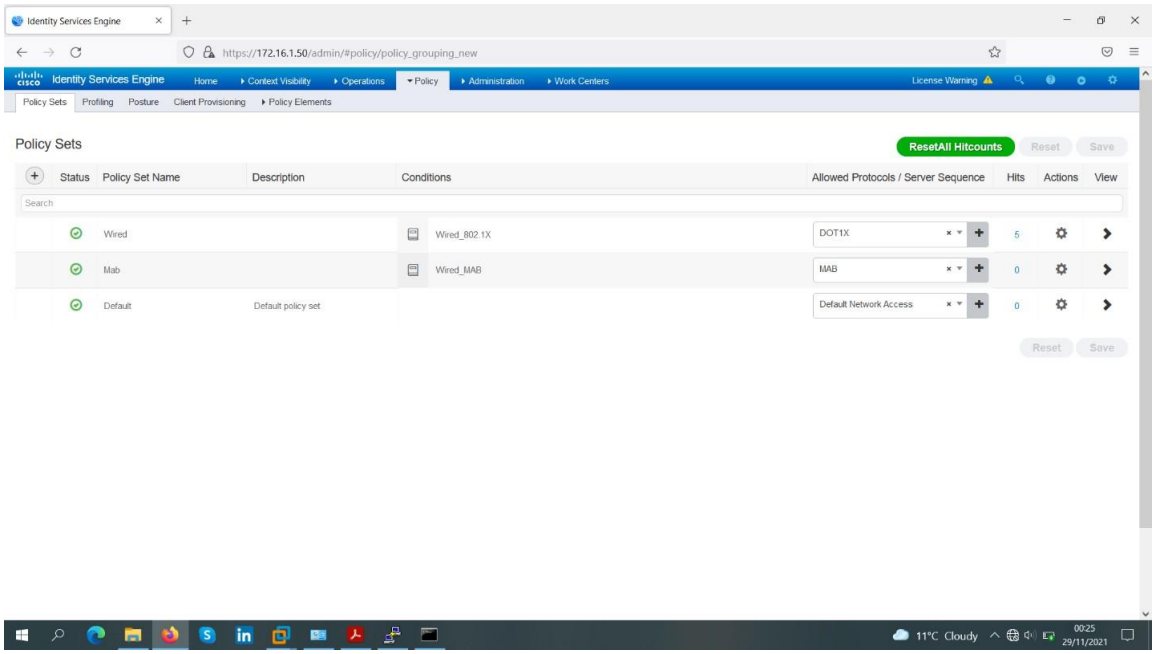


Figure IV-47 Etape 2 de l'ajout de politiques d'authentification.

Etape 3 : Nous avons changé le nom de la règle par "802.1X".
Etape 4 : Nous avons choisi la condition associée à l'authentifica- tion 802.1X en cliquant sur "Condition(s)" > "Select Existing Condition from Library" > "Select Condition" > "Compound Condition" > "Wired- 802.1X".
Etape 5 : Nous avons choisi le protocole d'authentification en cliquantsur "Select Network Access" > "Allowed Protocols" > "DOT1X".

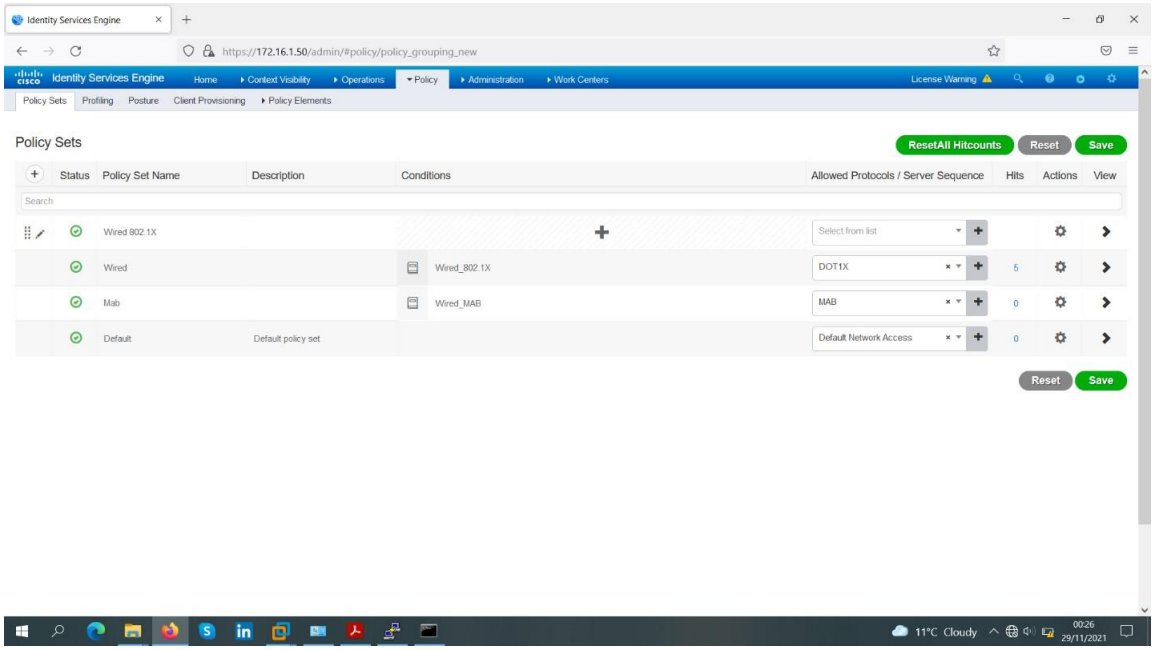


Figure IV-48 Etape 2 de l'ajout de politiques d'authentification.

Etape 6 : Nous avons cliqué sur "Done".

Annexe B

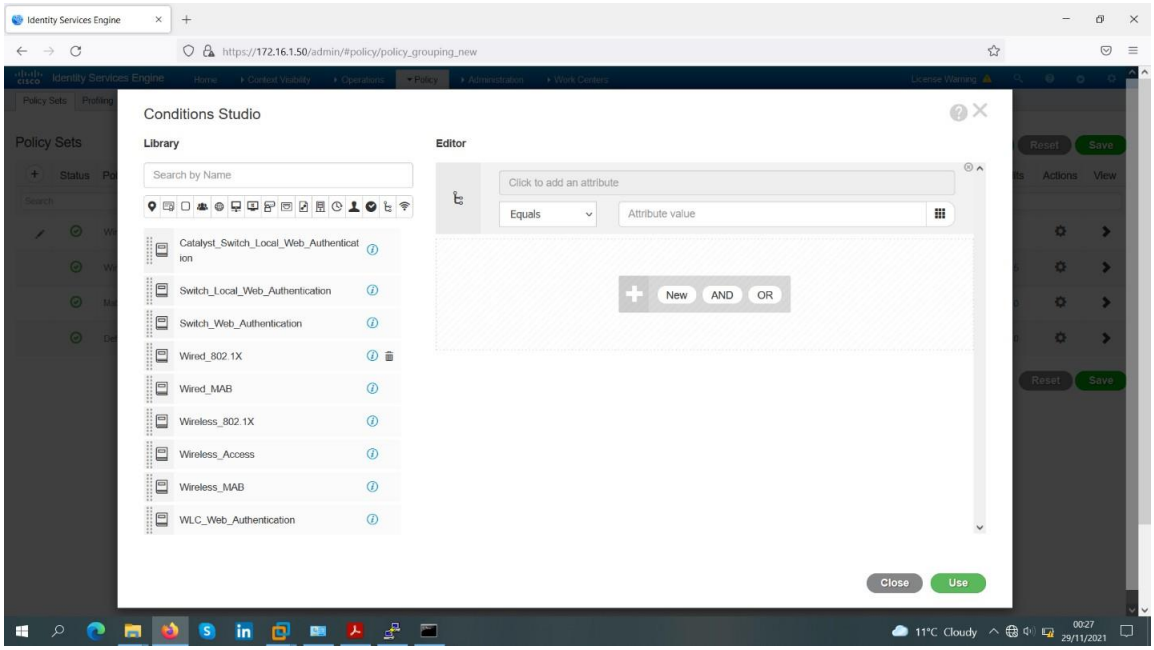


Figure IV-49 Etape 3 de l'ajout de politiques d'authentification.

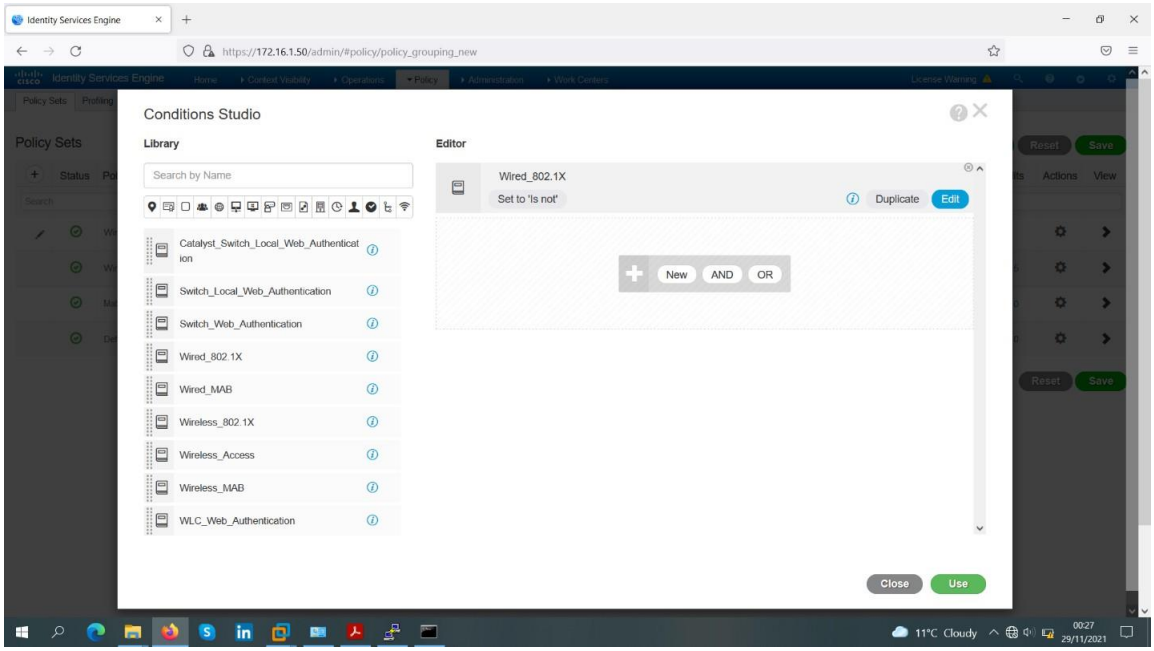


Figure IV-50 Etape 4 de l'ajout de politiques d'authentification.

Annexe B

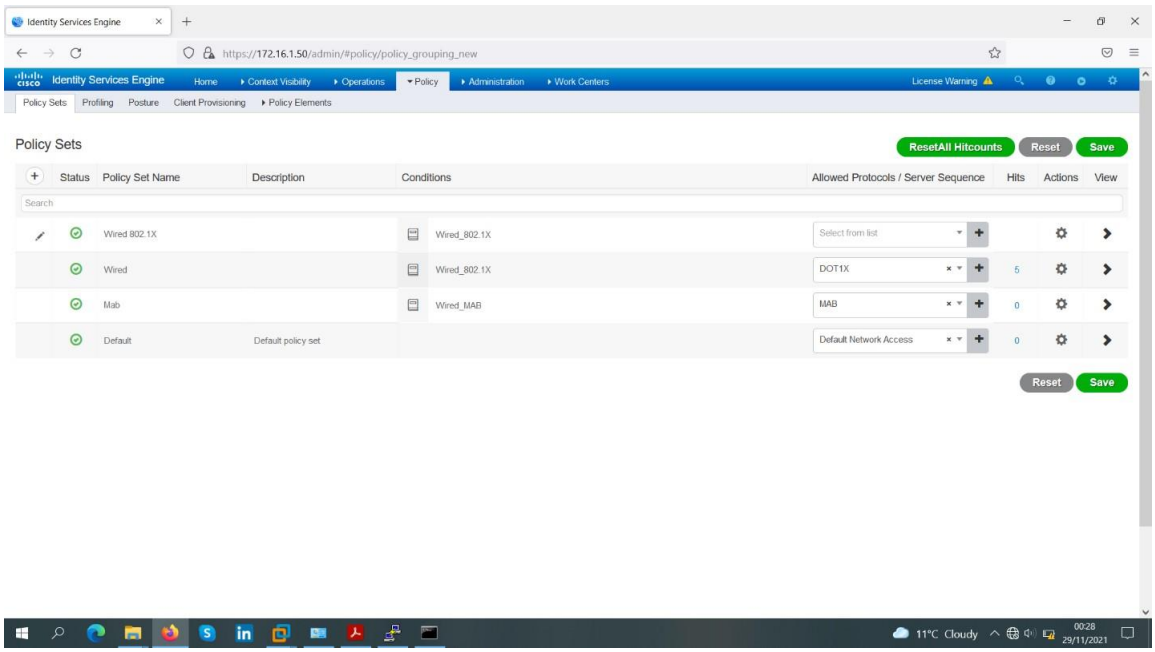


Figure IV-51 Etape 5 de l'ajout de politiques d'authentification.

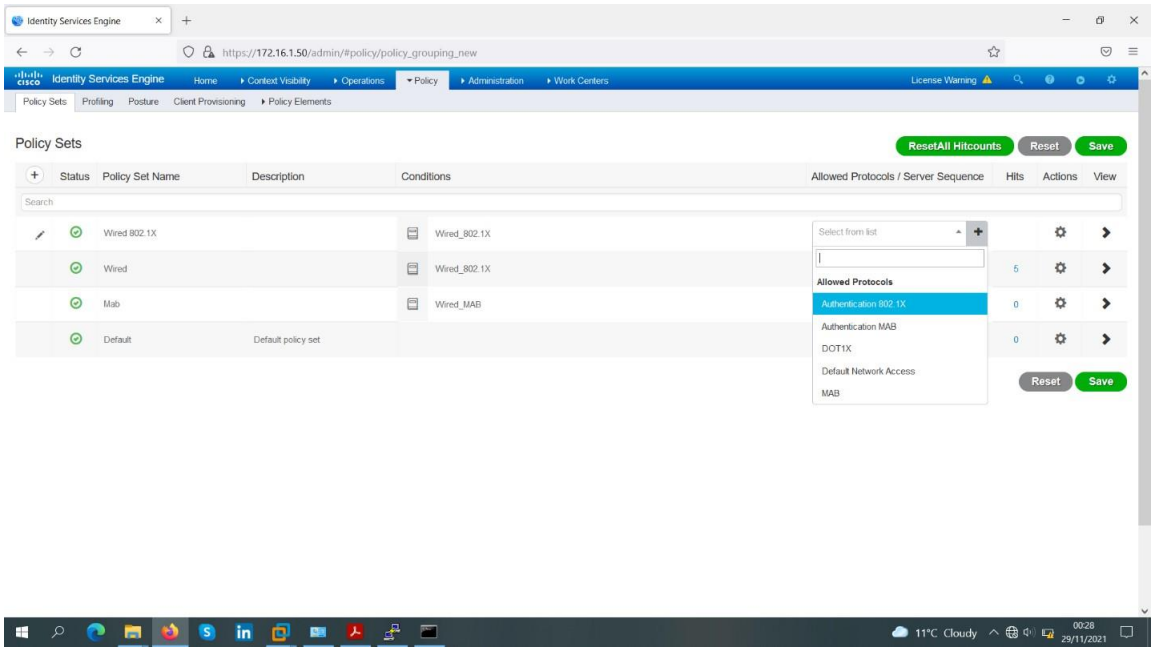


Figure IV-52 Etape 6 de l'ajout de politiques d'authentification.

Annexe B

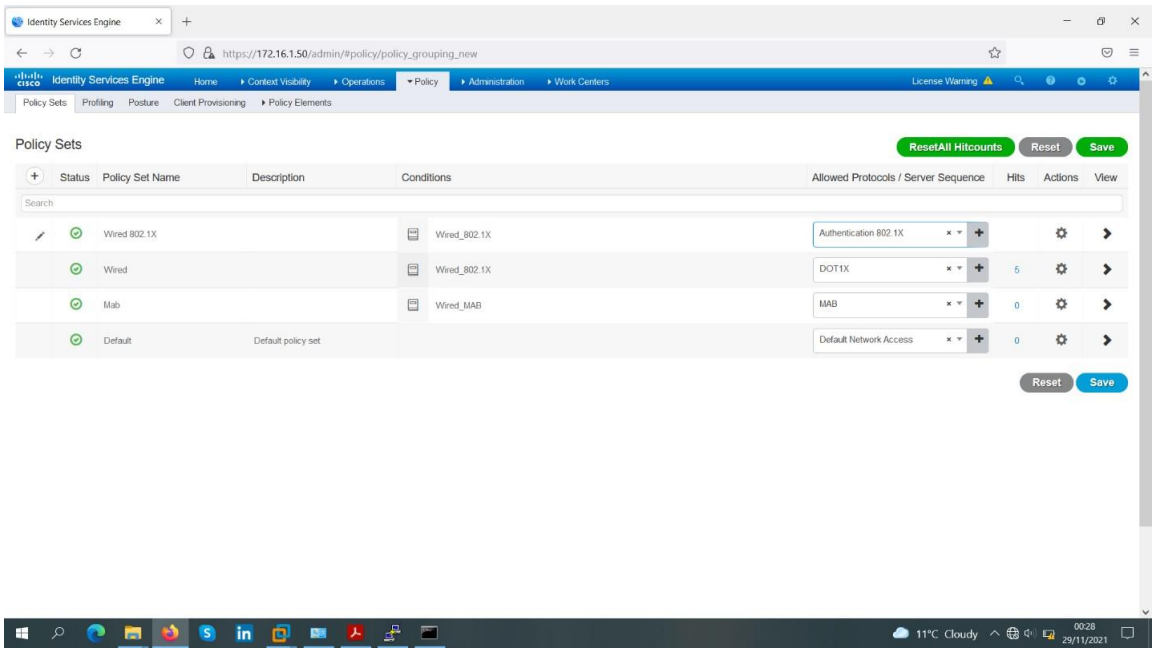


Figure IV-53 Etape 7 de l'ajout de politiques d'authentification.

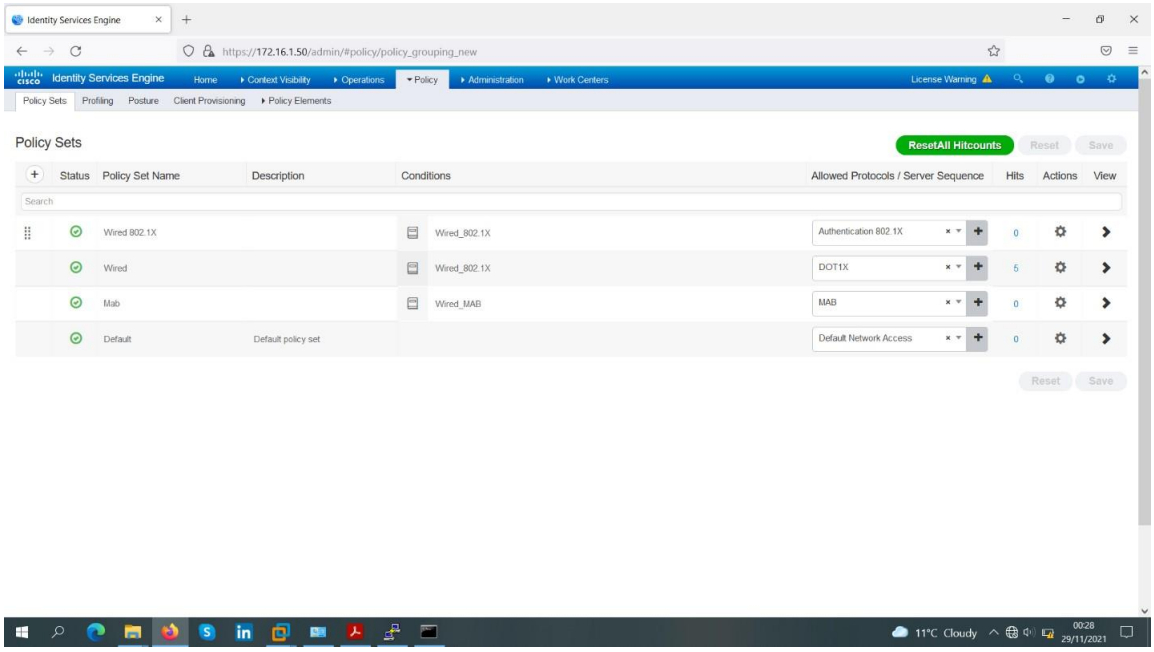


Figure IV-54 Etape 8 de l'ajout de politiques d'authentification.

Annexe B

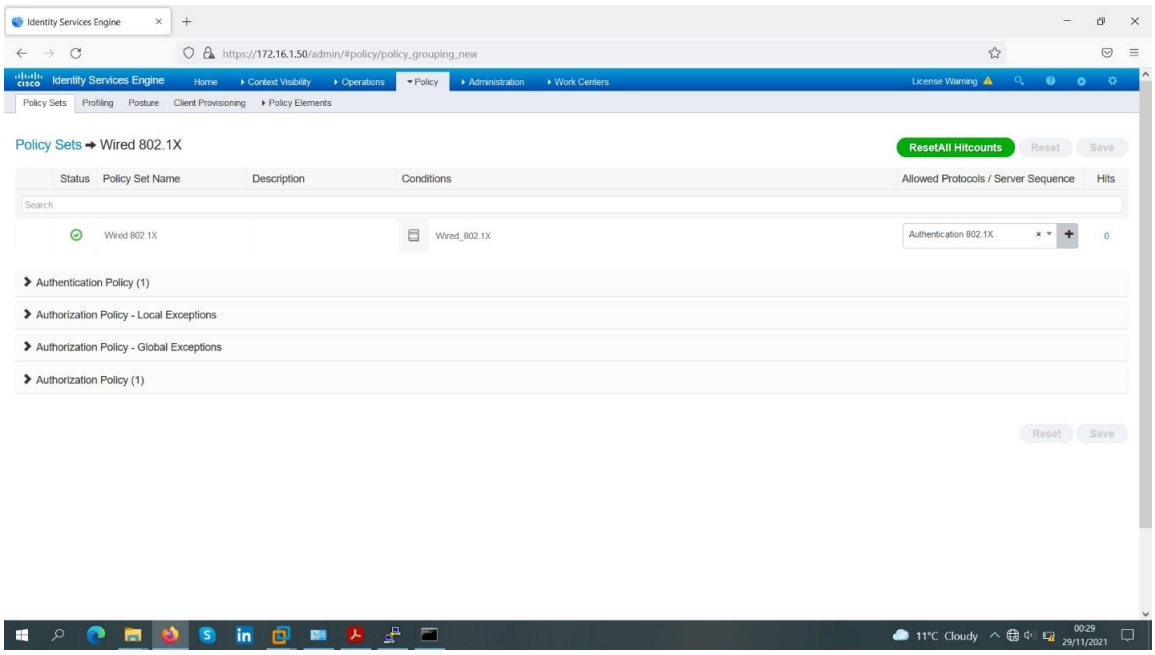


Figure IV-55 Etape 9 de l'ajout de politiques d'authentification.

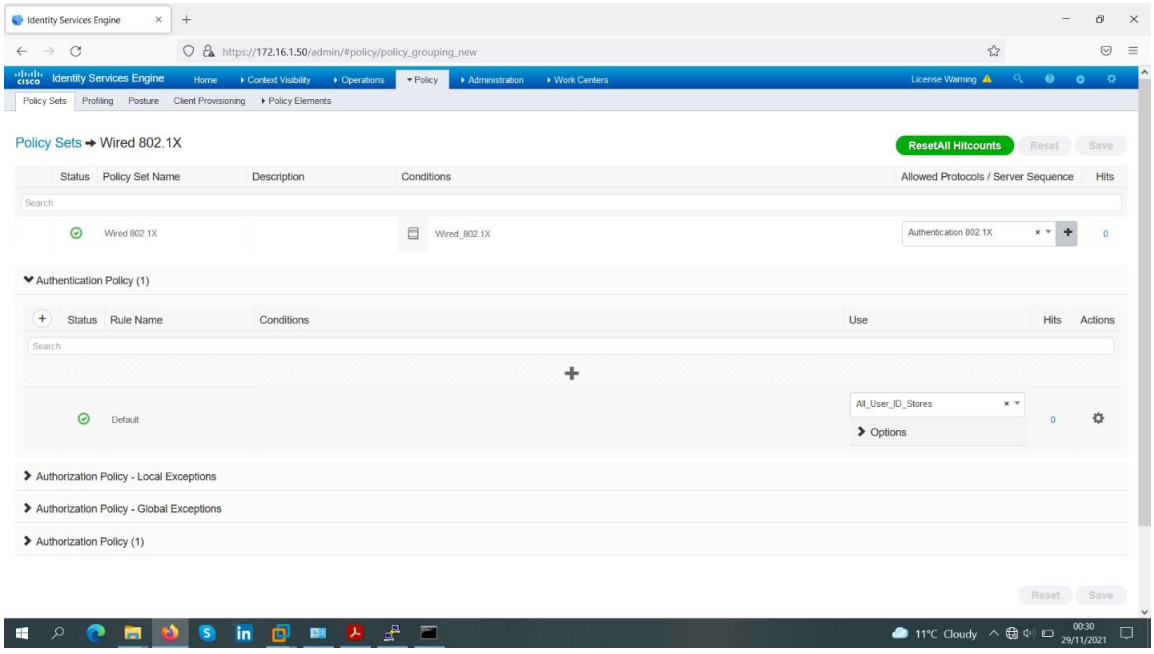


Figure IV-56 Etape 10 de l'ajout de politiques d'authentification.

Annexe B

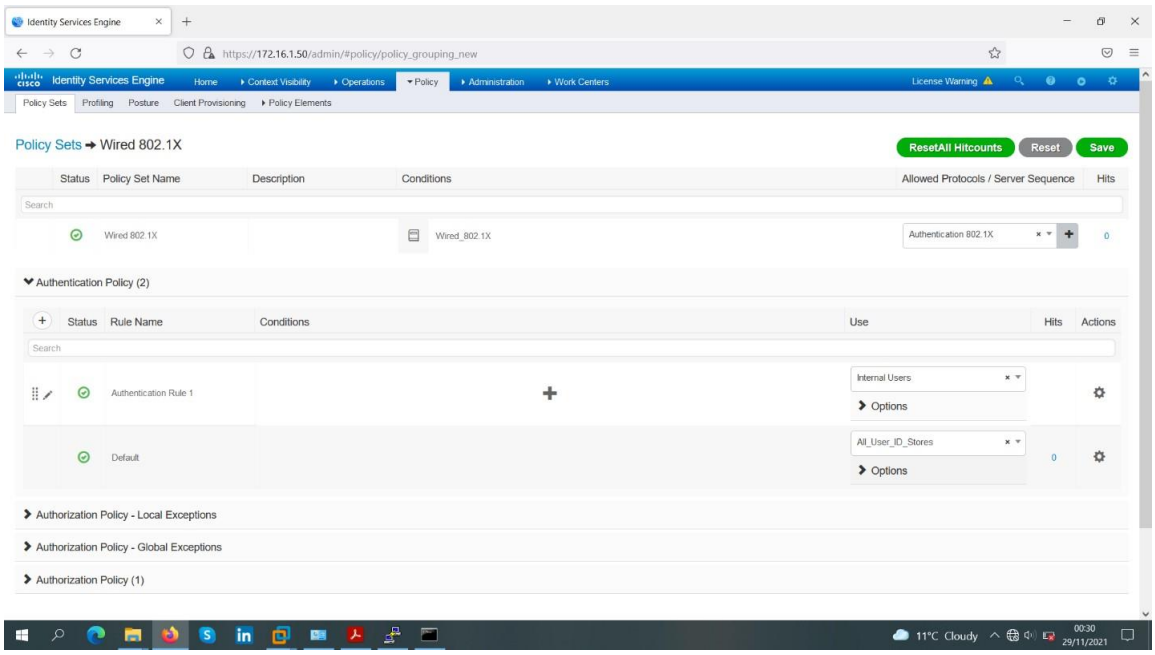


Figure IV-57 Etape 11 de l'ajout de politiques d'authentification.

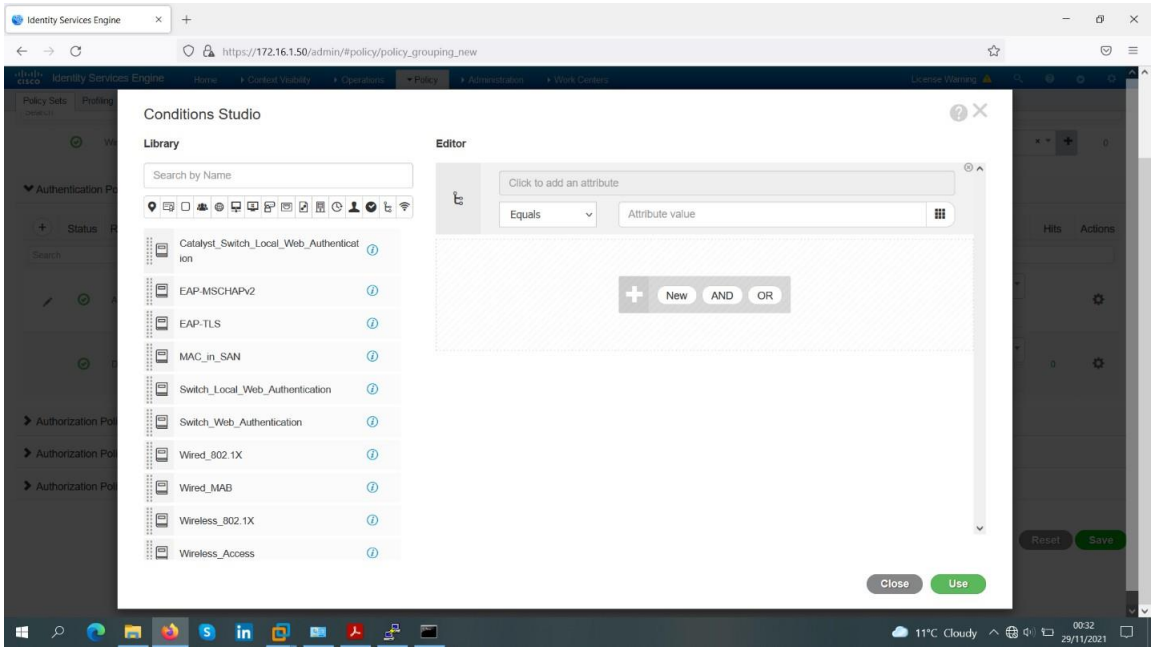


Figure IV-58 Etape 12 de l'ajout de politiques d'authentification.

Annexe B

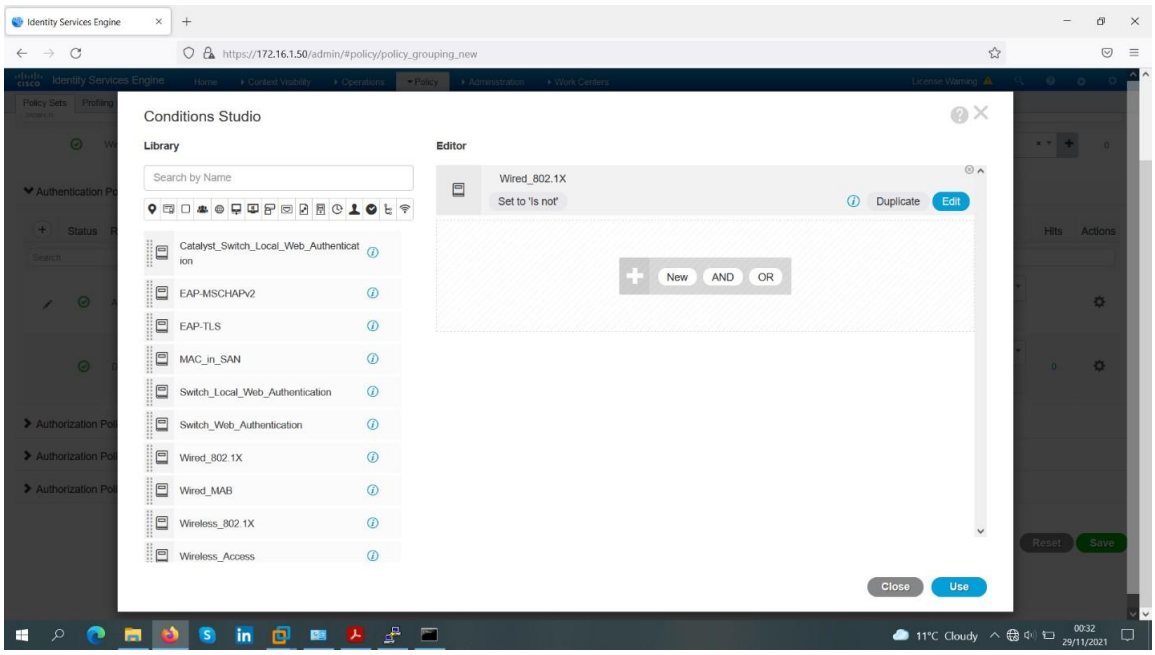


Figure IV-59 Etape 13 de l'ajout de politiques d'authentification.

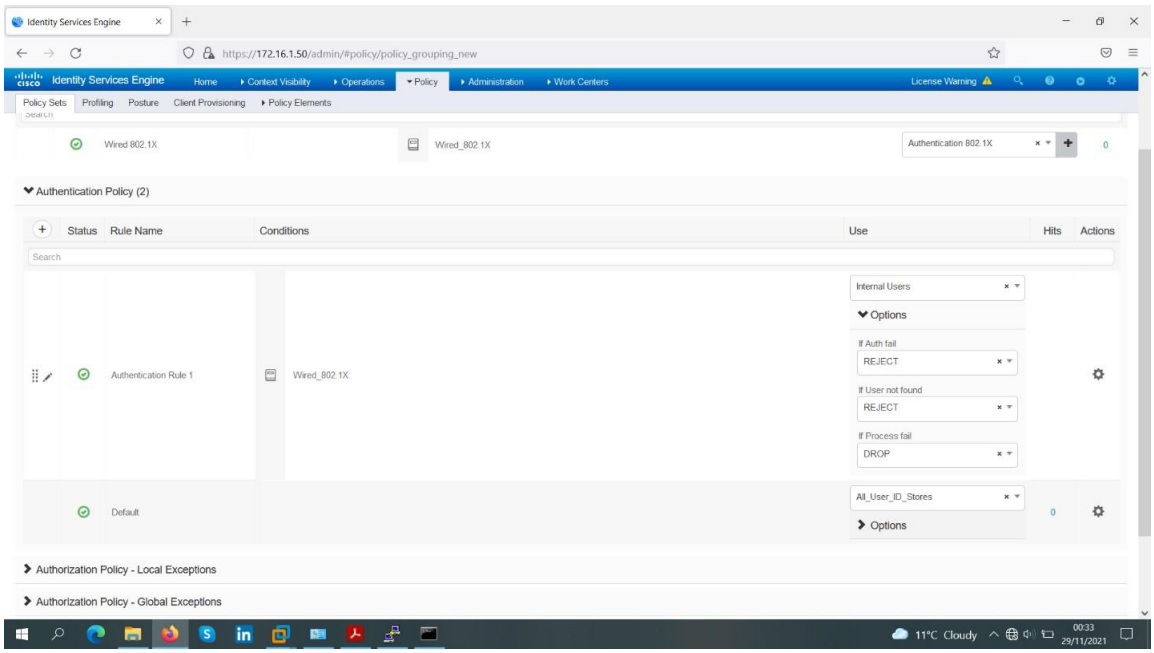


Figure IV-60 Etape 14 de l'ajout de politiques d'authentification.

Annexe B

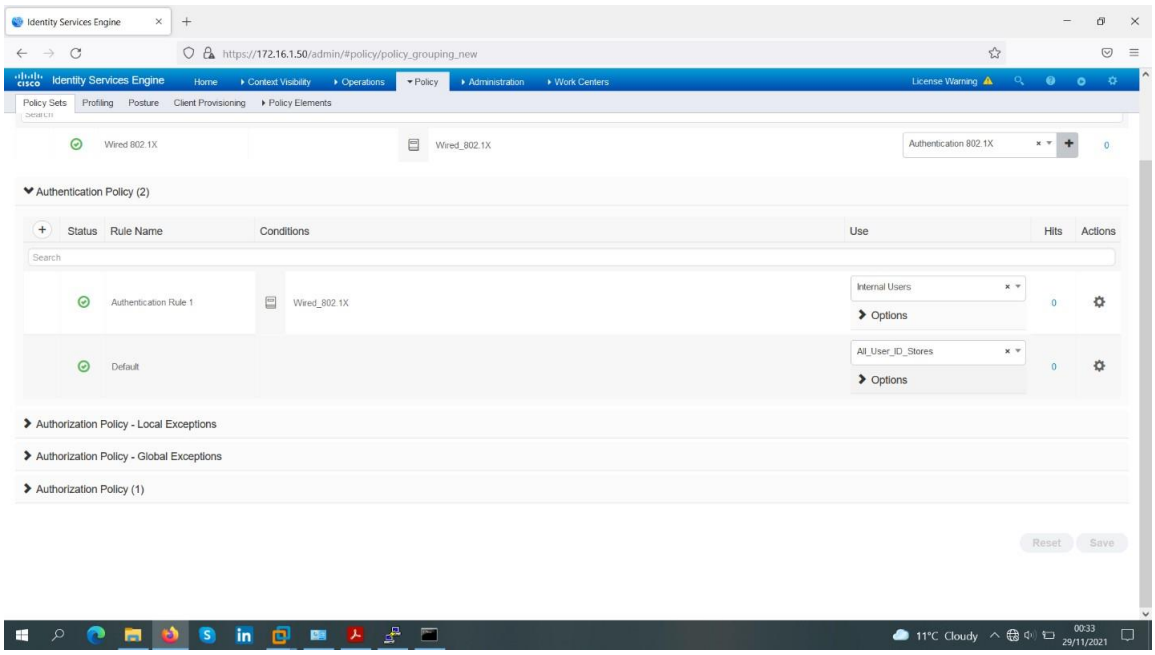


Figure IV-61 Etape 15 de l'ajout de politiques d'authentification.

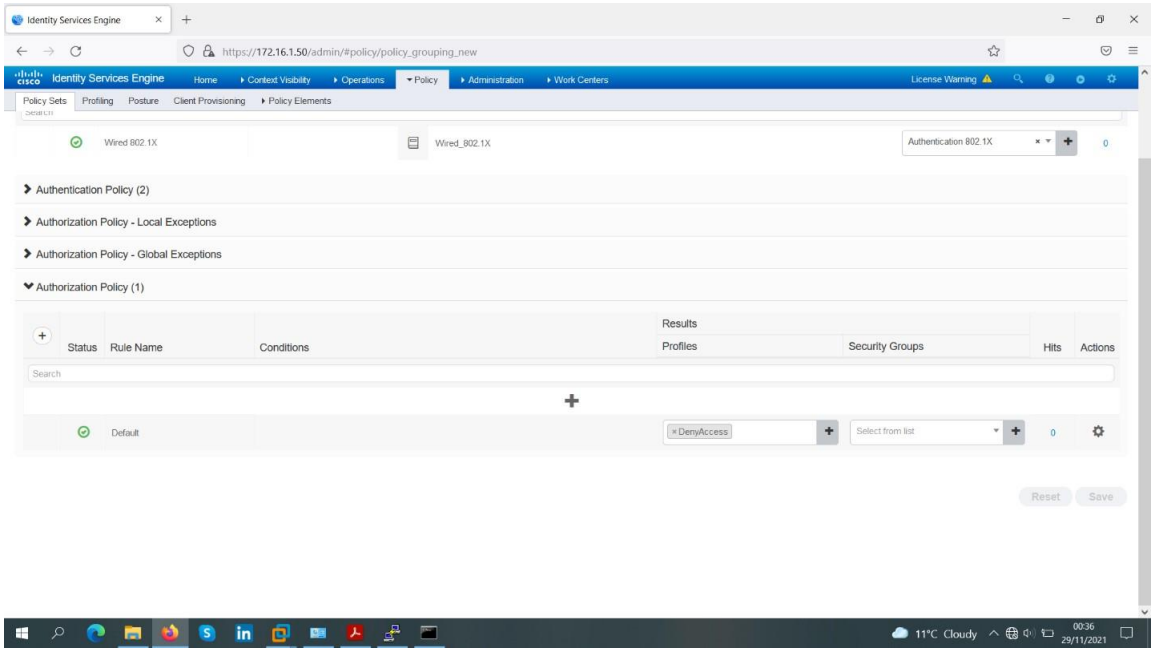


Figure IV-62 Etape 16 de l'ajout de politiques d'authentification.

IV.9.8) **Ajout de politiques d'autorisation (Authorization Policy)802.1X**

Afin d'ajouter des politiques d'autorisation 802.1X, nous avons suivi les étapes suivantes :

Etape 1 : Tout d'abord, nous avons ajouté des profils d'autorisation.

Pour cela nous avons suivi les sous-étapes suivantes :

Etape 1.1 : Nous avons cliqué sur : "Policy" > "Policy Elements" > "Results" > "Authorization" > "Authorization Profiles", l'écran suivant apparaîtra.

Annexe B

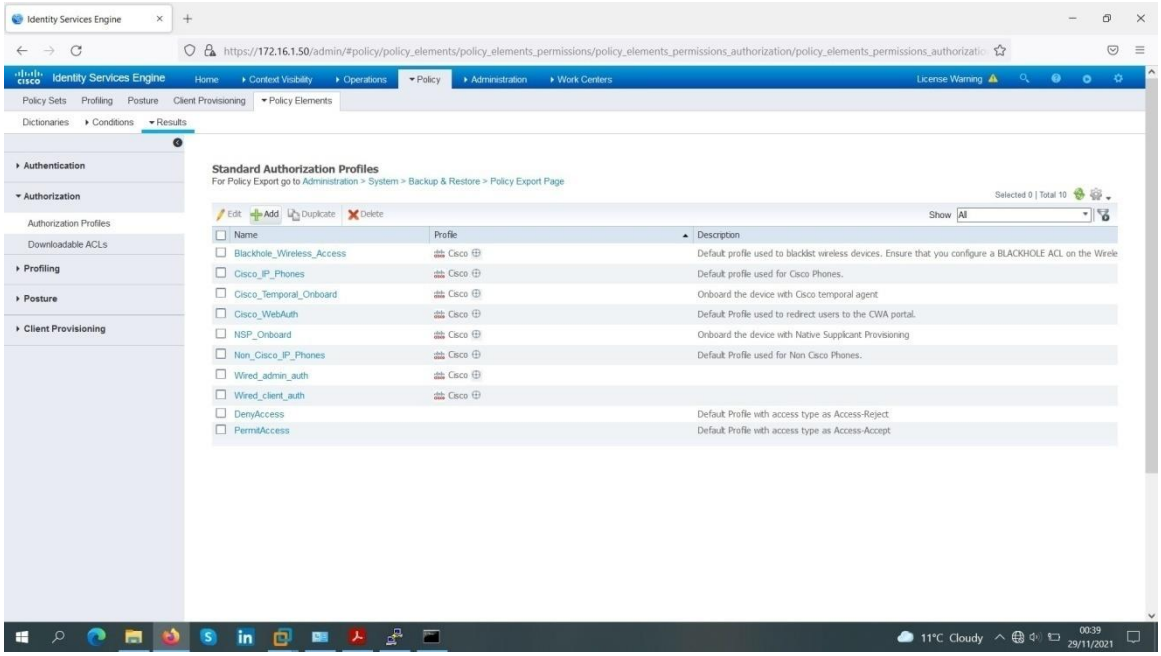


Figure IV-63 Etape 1.1 de l'ajout de politiques d'autorisation 802.1X

Etape 1.2 : Nous avons cliqué sur "ADD".

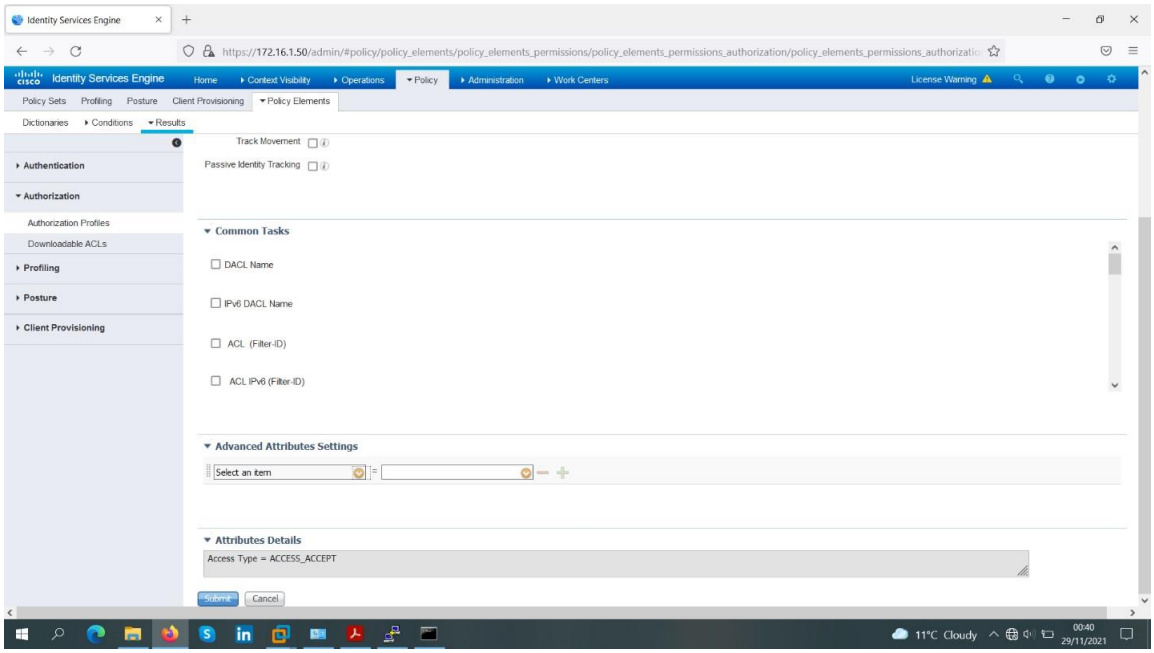


Figure IV-64 Etape 1.2 de l'ajout de politiques d'autorisation 802.1X

Etape 1.3 : Nous avons ajouté un premier profil d'autorisation 802.1Xen remplissant le champ "Name" par "Wired-Student-auth".

Annexe B

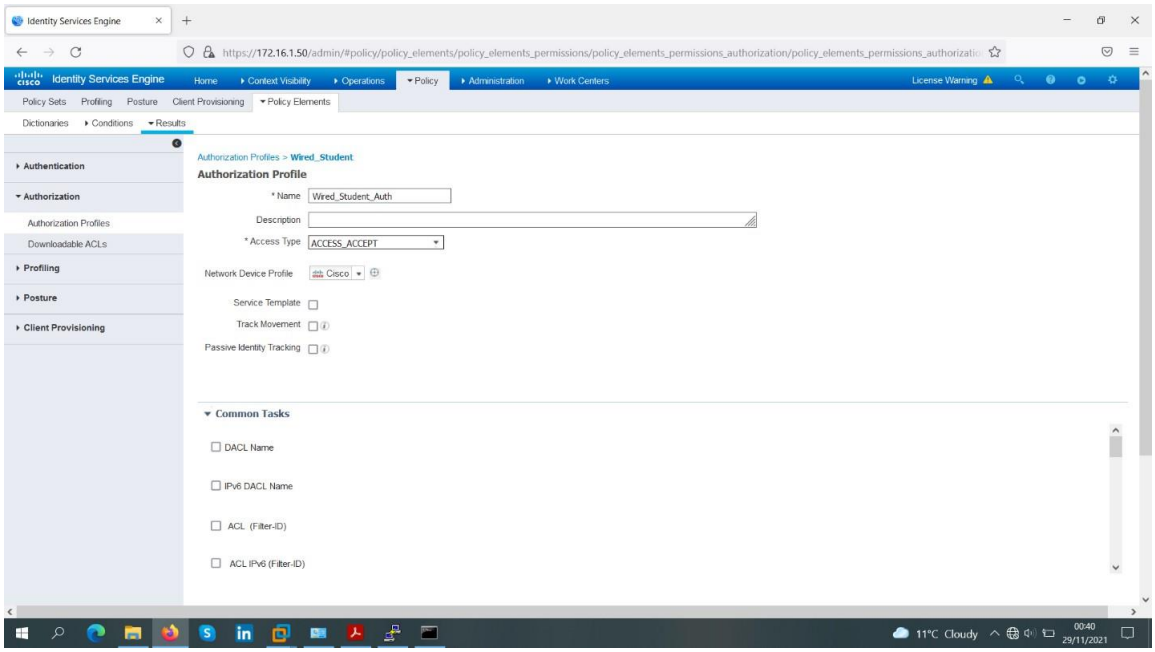


Figure IV-65 Etape 1.3 de l'ajout de politiques d'autorisation 802.1X

Etape 1.4 : Nous avons cliqué sur "Submit" pour appliquer les changements.

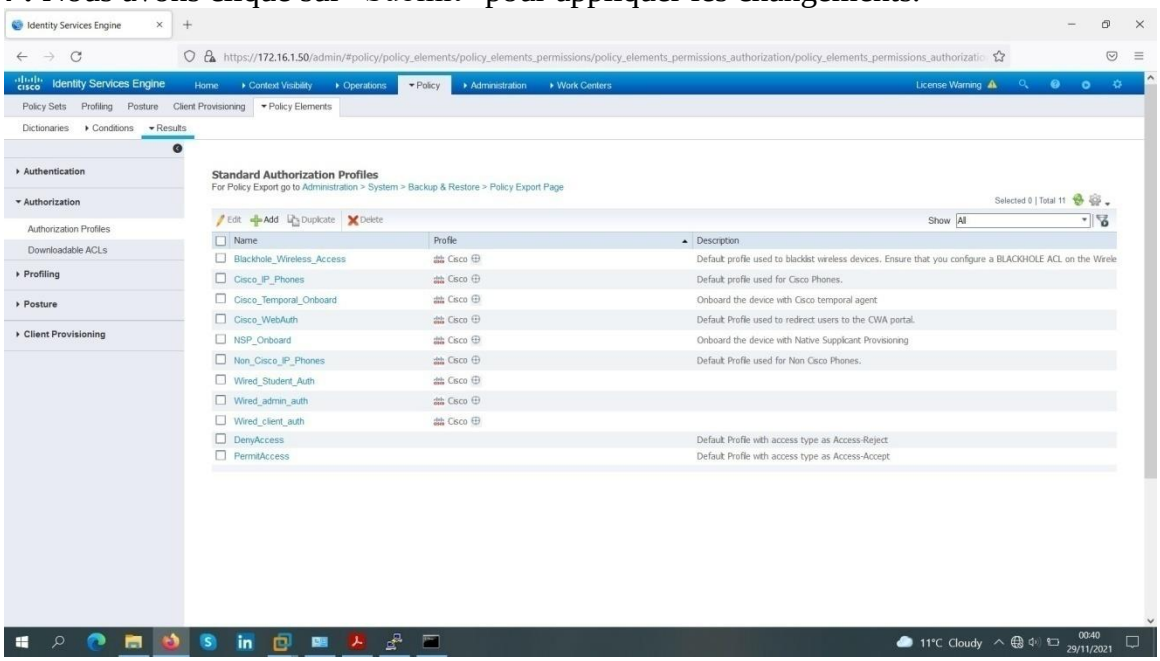


Figure IV-66 Etape 1.4 de l'ajout de politiques d'autorisation 802.1X

Etape 1.5 : Nous avons ajouté un premier profil d'autorisation 802.1Xen remplissant le champ "Name" par "Wired-Teacher-auth".

Annexe B

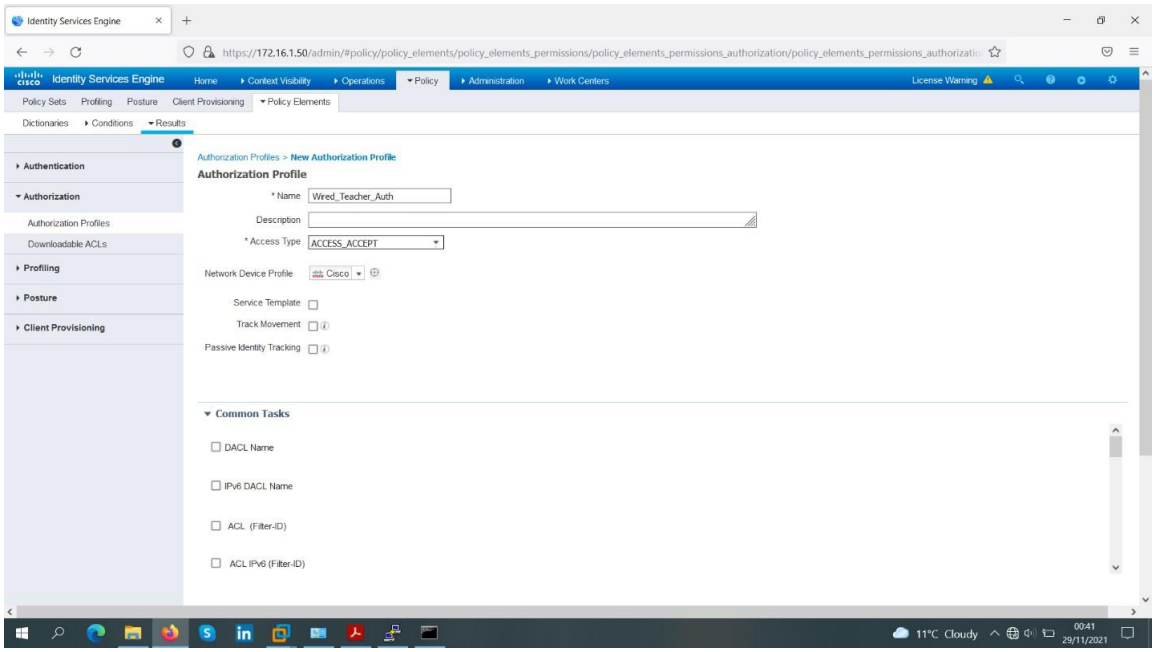


Figure IV-67 Etape 1.5 de l'ajout de politiques d'autorisation 802.1X

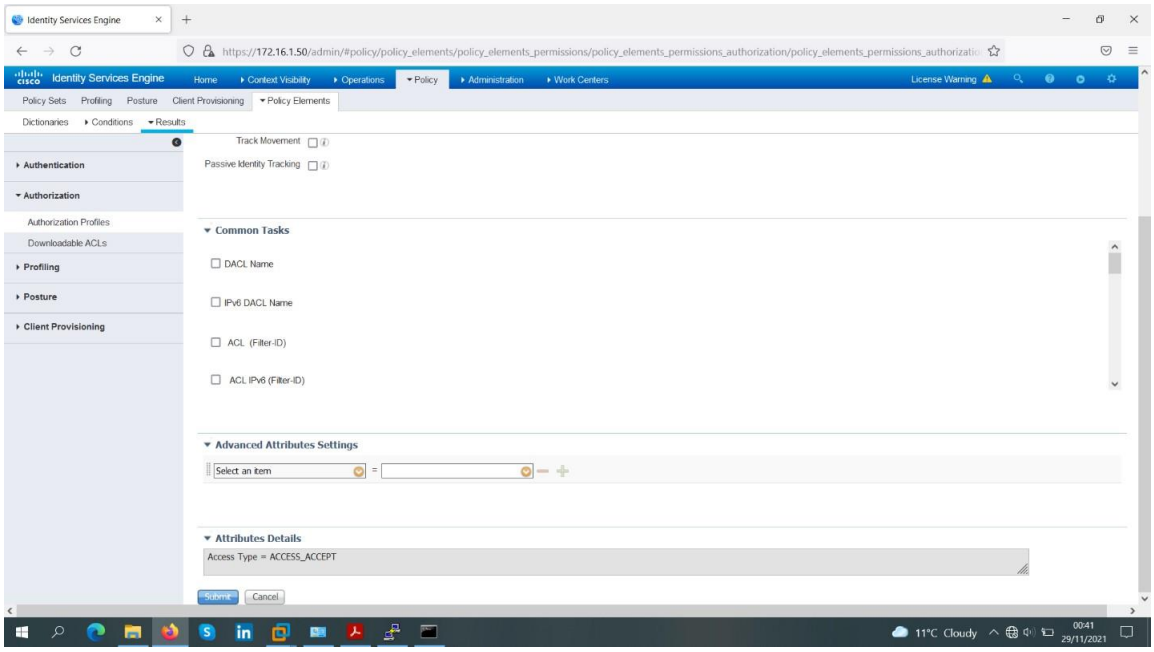


Figure IV-68 Etape 1.5 de l'ajout de politiques d'autorisation 802.1X

Etape 1.6 : Nous avons cliqué sur "Submit" pour appliquer les changements.

Annexe B

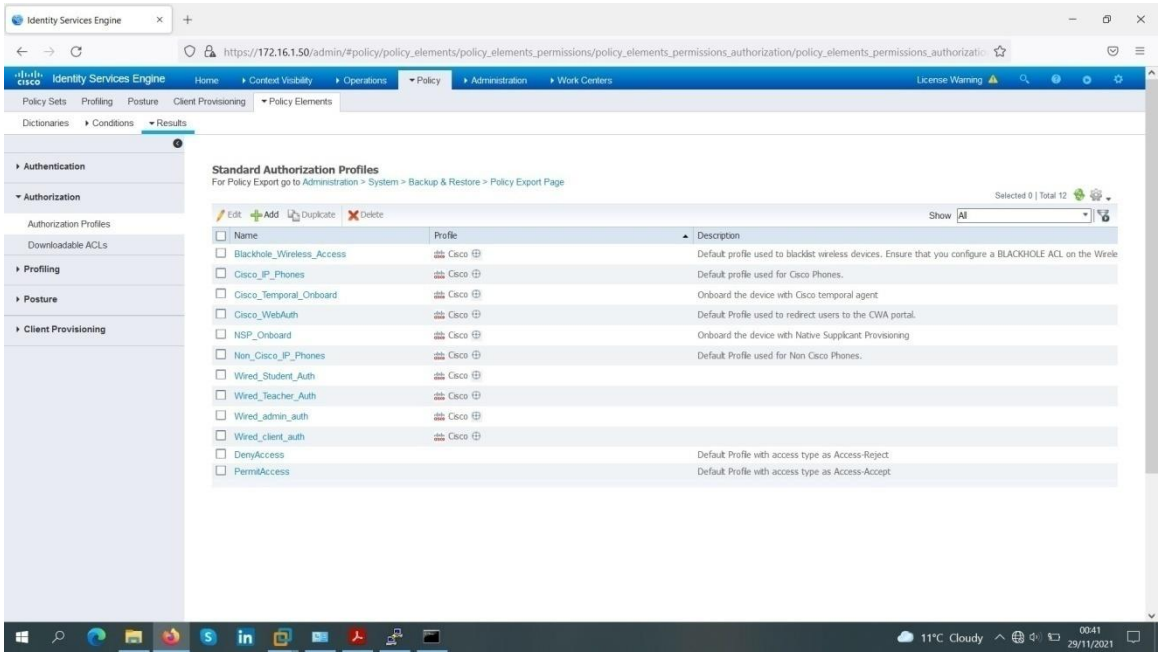


Figure IV-69 vérification de l'ajout de politiques d'autorisation 802.1X

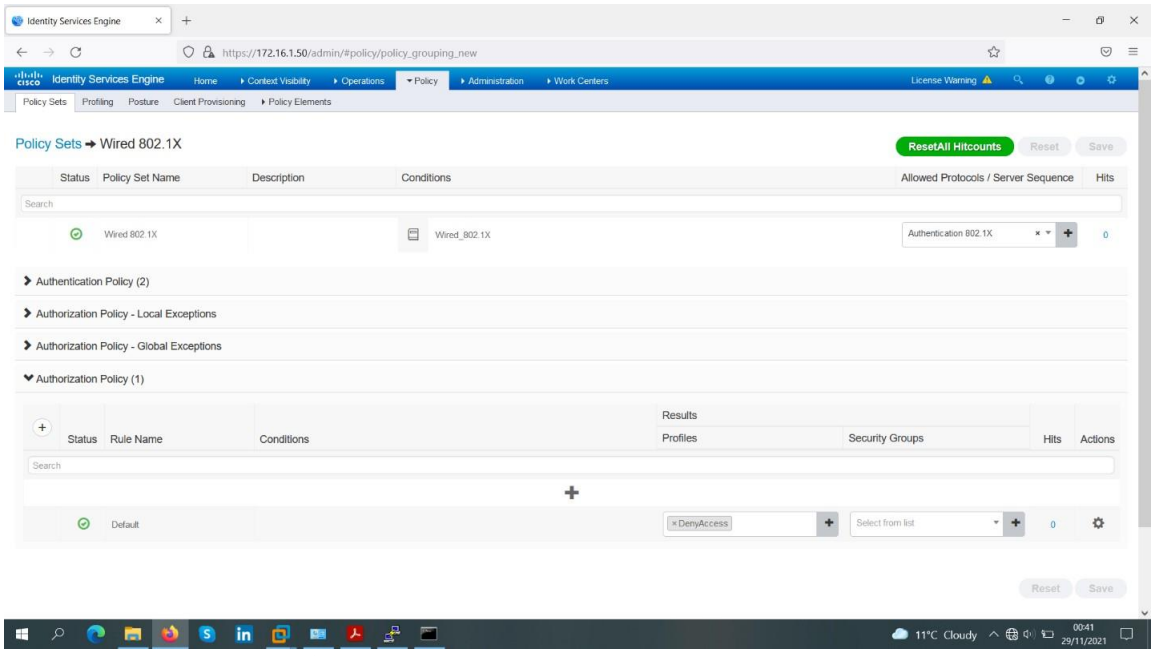


Figure IV-70 Etape 1.7 de l'ajout de politiques d'autorisation 802.1X.

Etape 2 : Nous avons cliqué sur : "Policy" > "Authorization", l'écran suivant apparaîtra.

Annexe B

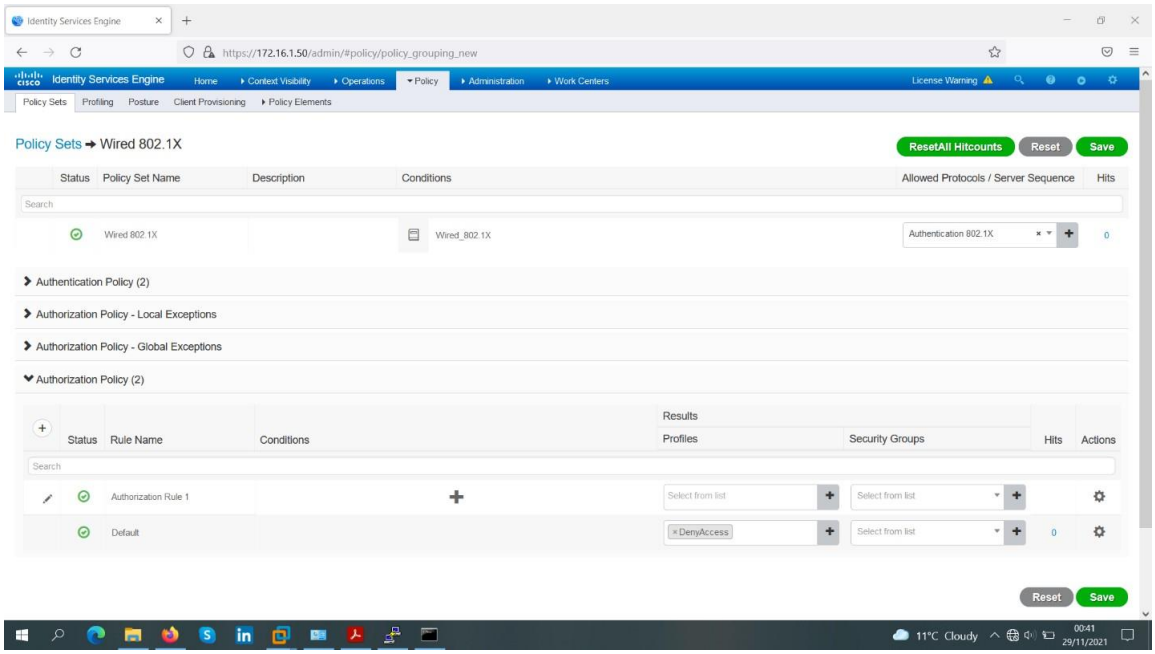


Figure IV-71 Etape 2 de l'ajout de politiques d'autorisation 802.1X "2"

Etape 3 : Nous avons ajouté une première règle en cliquant sur la flèche qui se trouve à côté de l'option "Edit" et nous avons choisi l'option "InsertNew Rule Below".

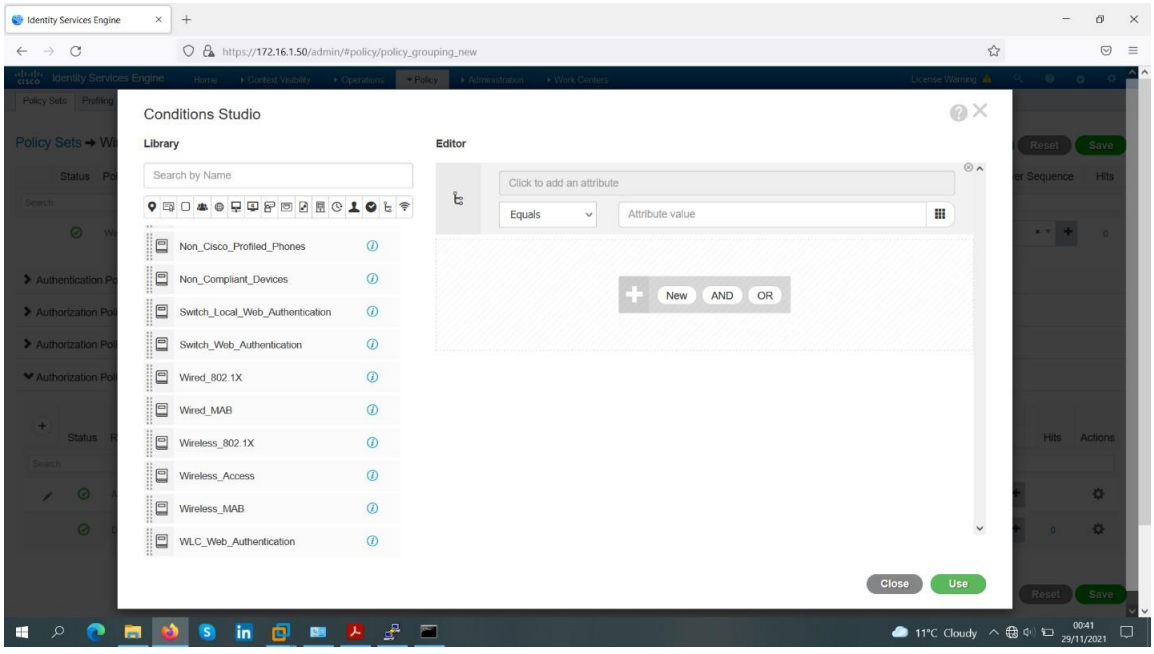


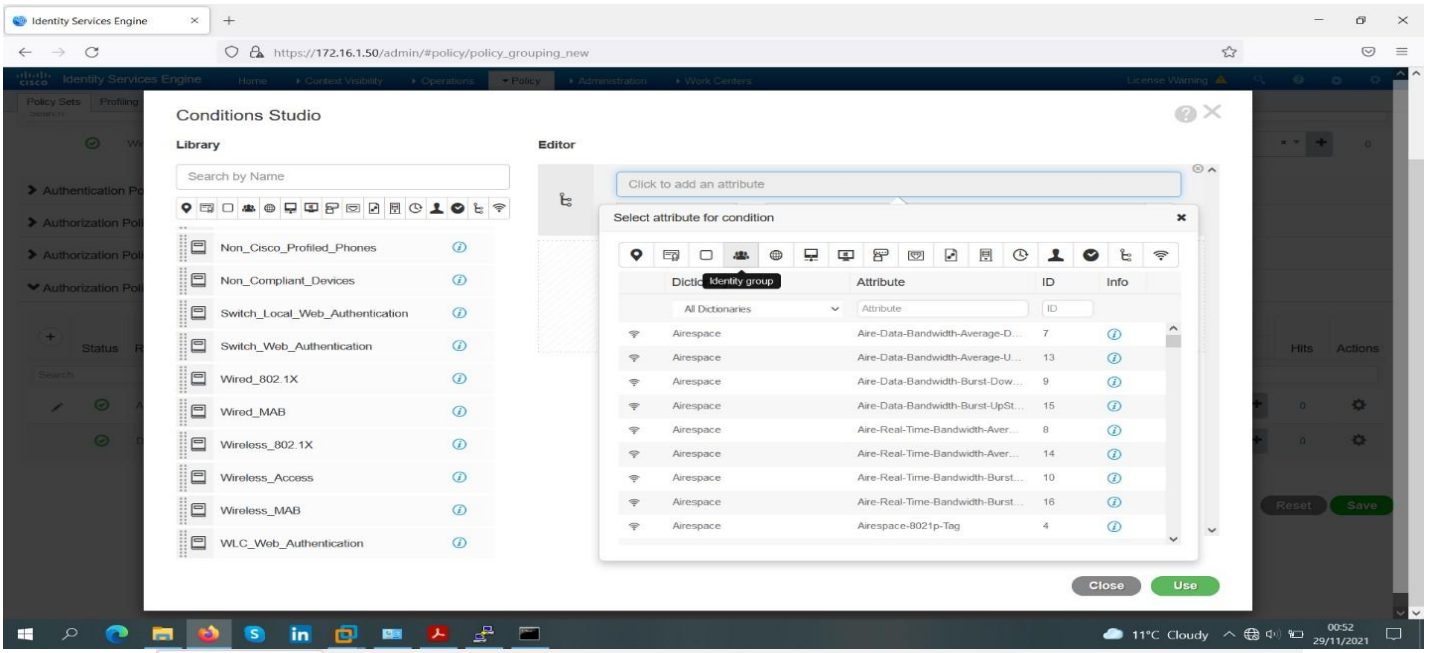
Figure IV-72 Etape 3 de l'ajout de politiques d'autorisation 802.1X "2"

Etape 4 : Nous avons changé le nom de la règle par "Admin-Rule".
Etape 5 : Nous avons choisi le groupe d'identité d'utilisateurs associéà cette règle en cliquant sur "Any" > "Any" > "User Identity Groups" > "Administrateur".

Etape 6 : Nous avons choisi la condition associée à ce groupe en cli- quant sur "Condition(s)" > "Select Existing Condition from Library" > "Select Condition" > "Compound Condition" > "Wired-802.1X".

Etape 7 : Nous avons choisi le profil d'autorisation associé à cette règle en cliquant sur "AuthZ Profiles" > "Select an item" > "Standard"> "Wired-Admin-auth".

Figure IV-73 Etape 3 de l'ajout de politiques d'autorisation 802.1X "2"



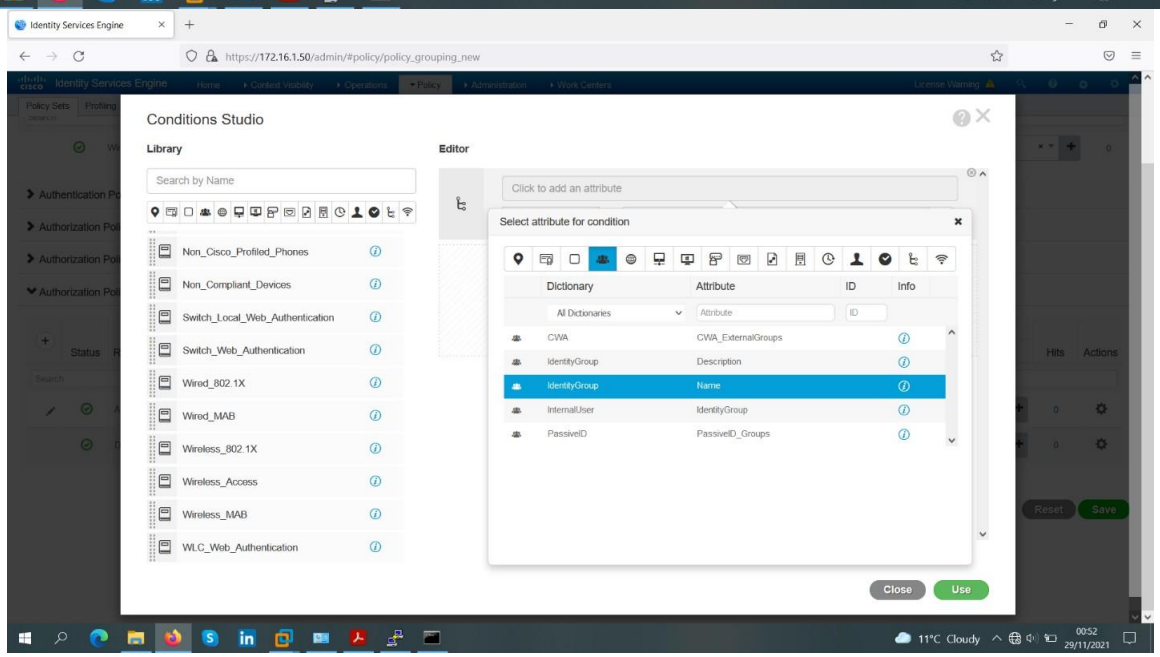


Figure IV-74 Etape 4 de l'ajout de politiques d'autorisation 802.1X "2"

Annexe B

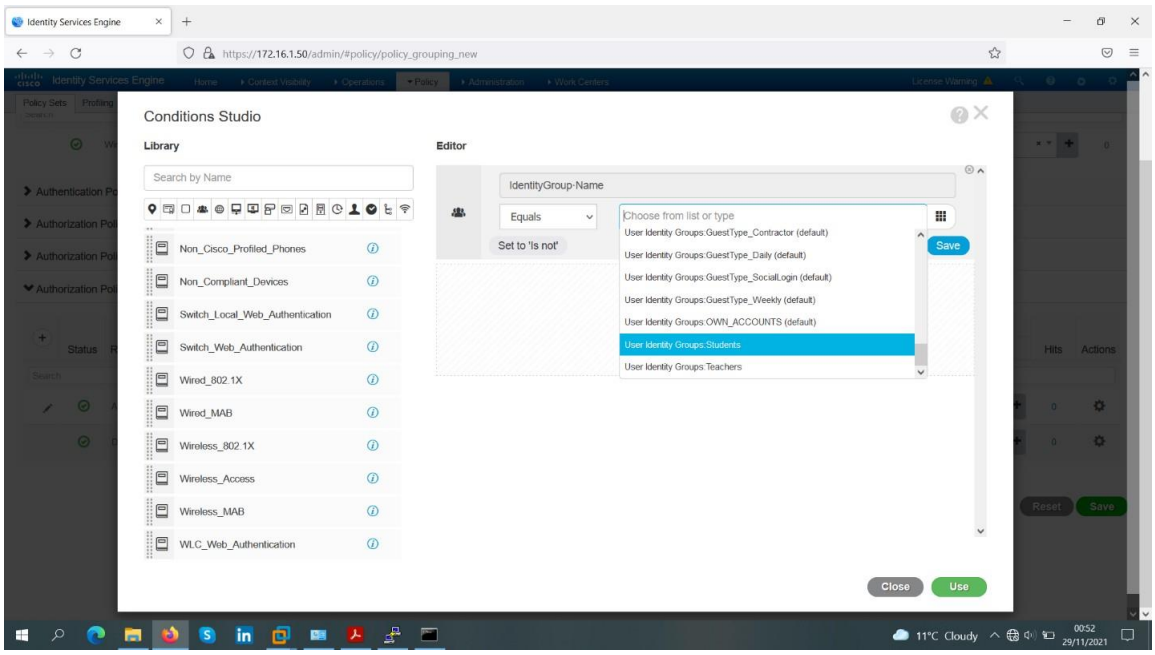


Figure IV-75 Etape 5 de l'ajout de politiques d'autorisation 802.1X "2"

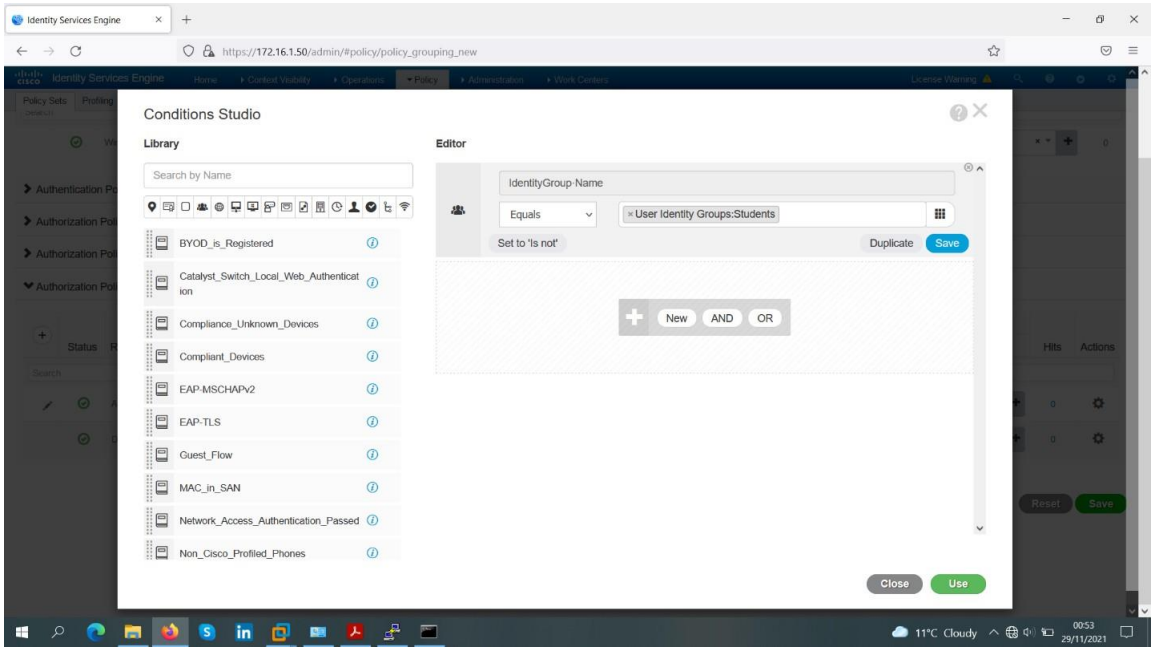
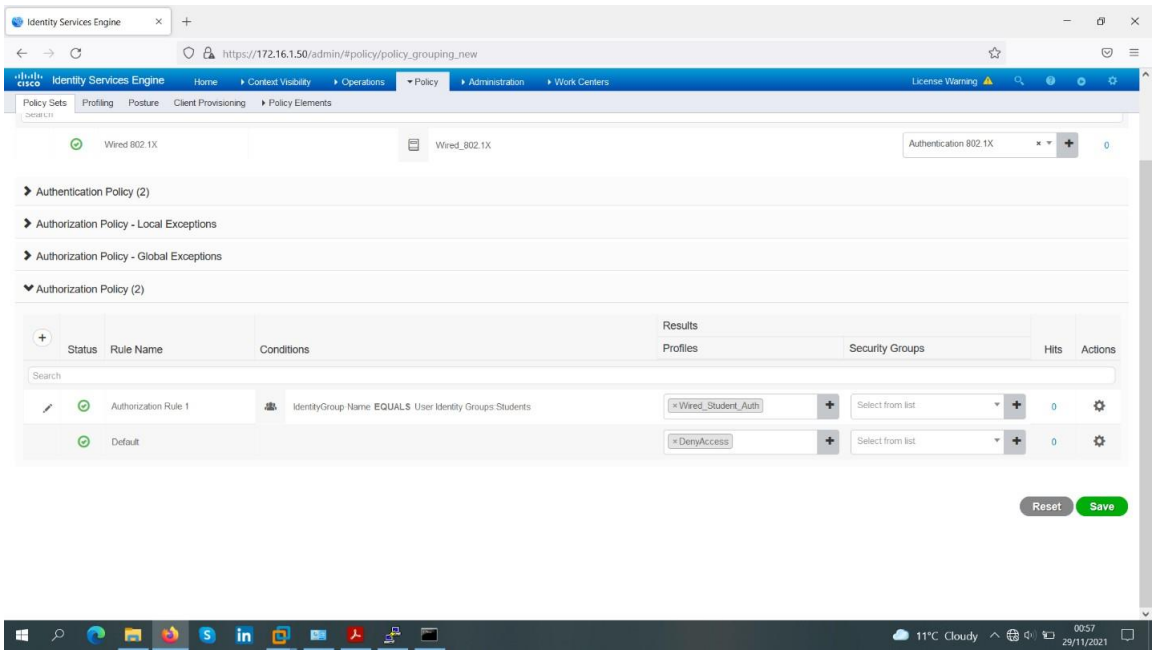


Figure IV-76 Etape 6 de l'ajout de politiques d'autorisation 802.1X "2"

Annexe B



IV-77 Etape 7 de l'ajout de politiques d'autorisation 802.1X "2"

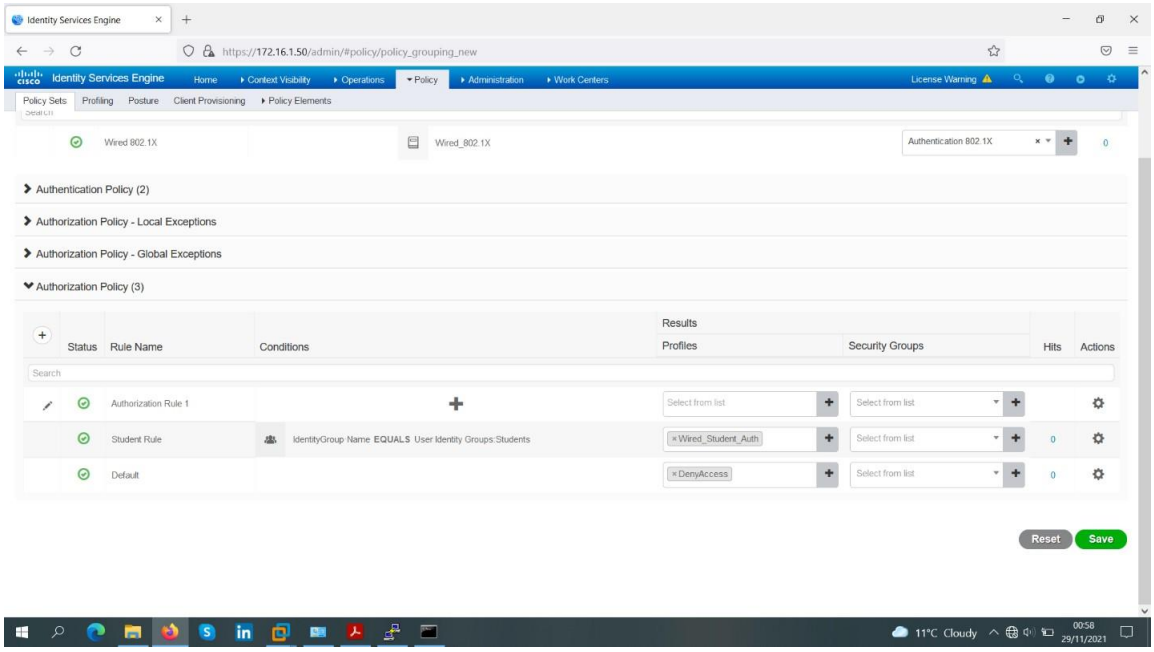


Figure IV-78 vérification de l'ajout de politiques d'autorisation 802.1X "2"

Annexe B

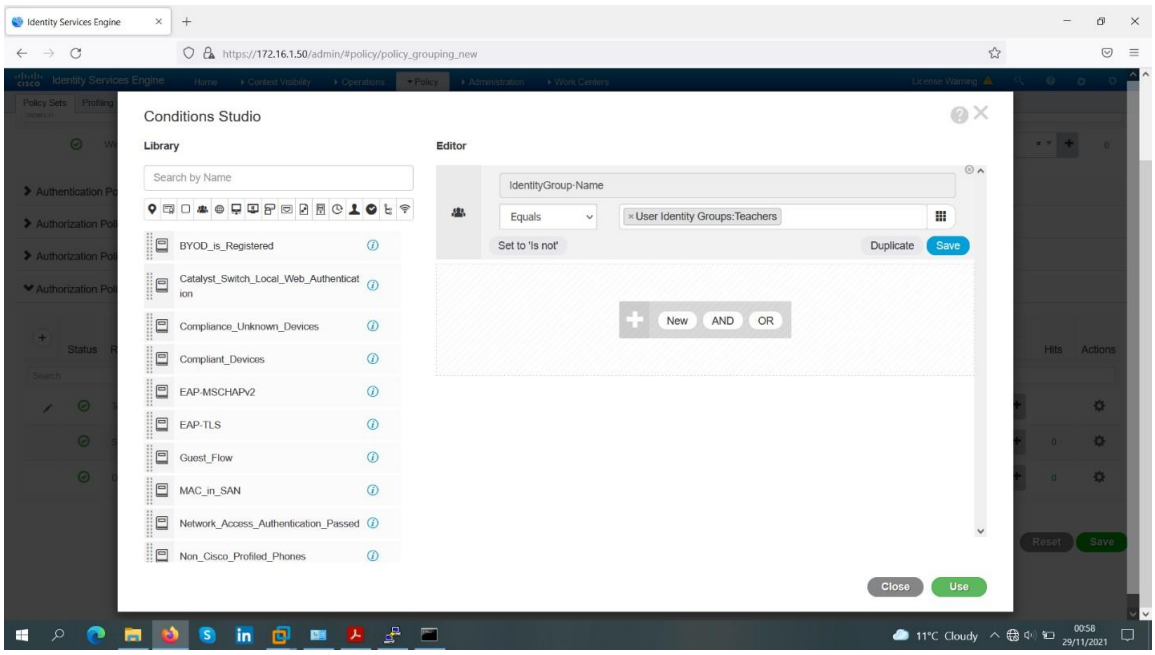


Figure IV-79 Etape 8 de l'ajout de politiques d'autorisation 802.1X "2"

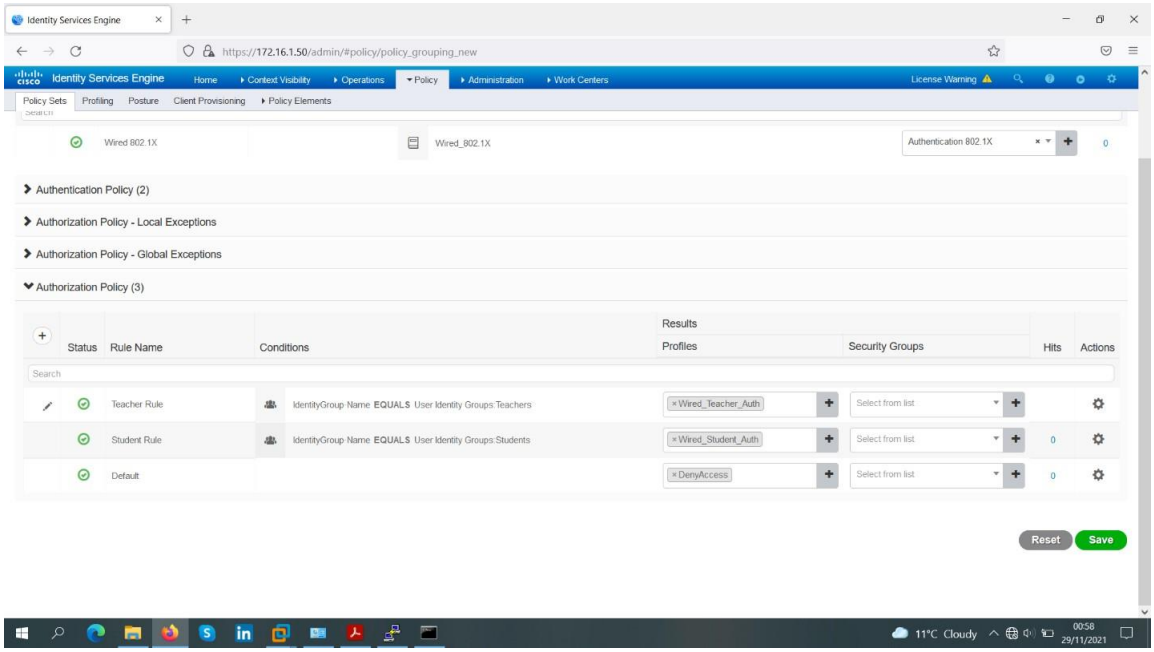


Figure IV-80 Etape 9 de l'ajout de politiques d'autorisation 802.1X "2"

Annexe B

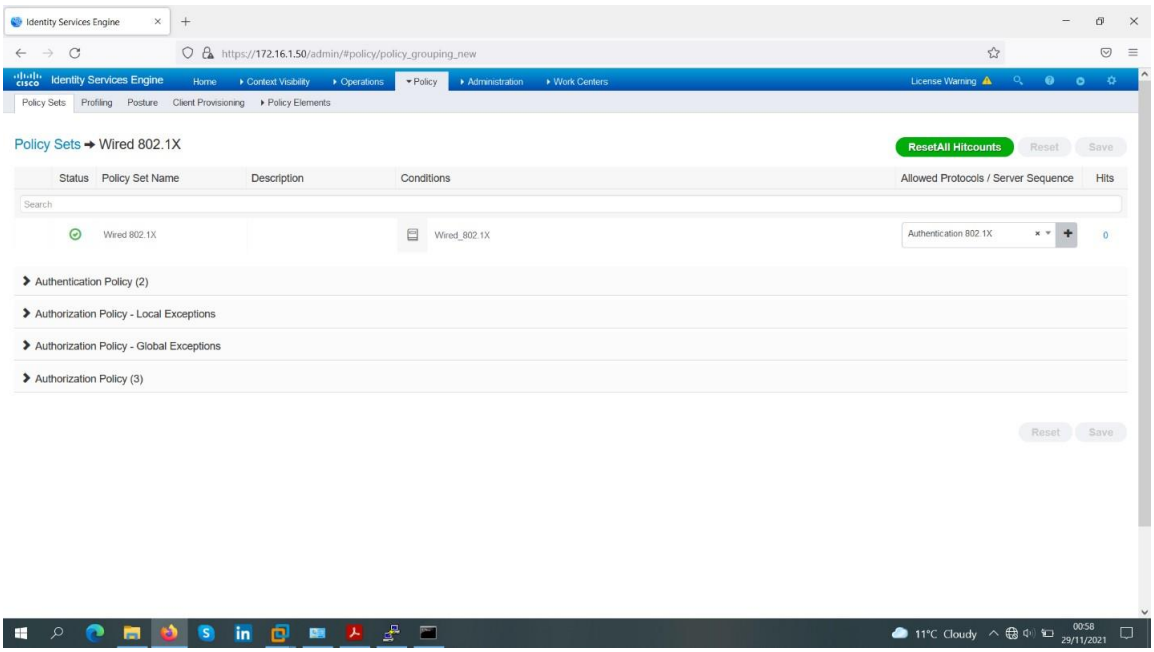


Figure IV-81 Etape 10 de l'ajout de politiques d'autorisation 802.

Nous avons cliqué sur "Submit" pour appliquer les changements.

Quant on termine tout les configurations et implémentations de notre protocole le client « Teacher » il va se connecté avec Wlans, et il va s'affiché une fenêtre pour faire authentification on demande l'identité et le mode passe :

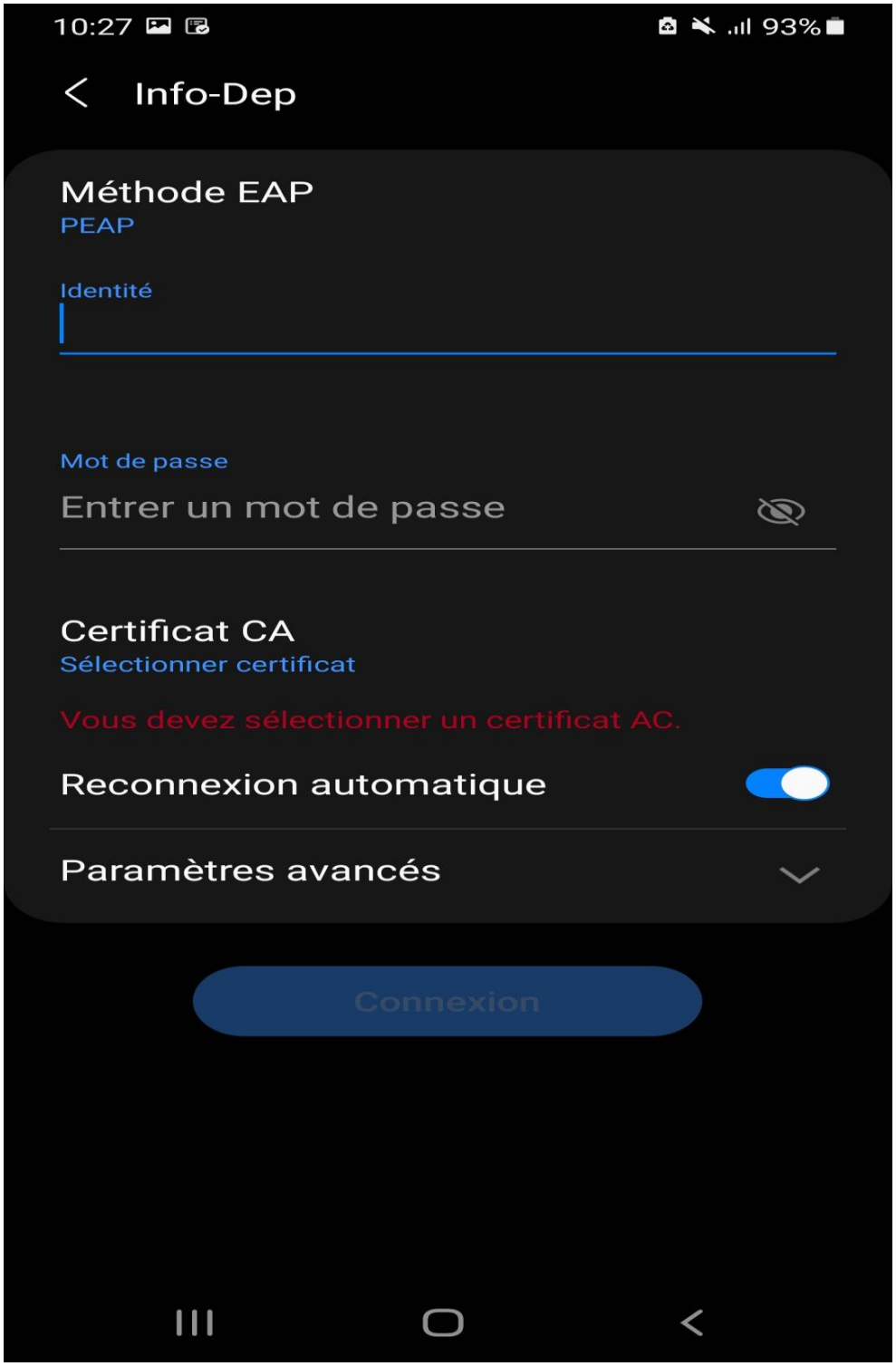
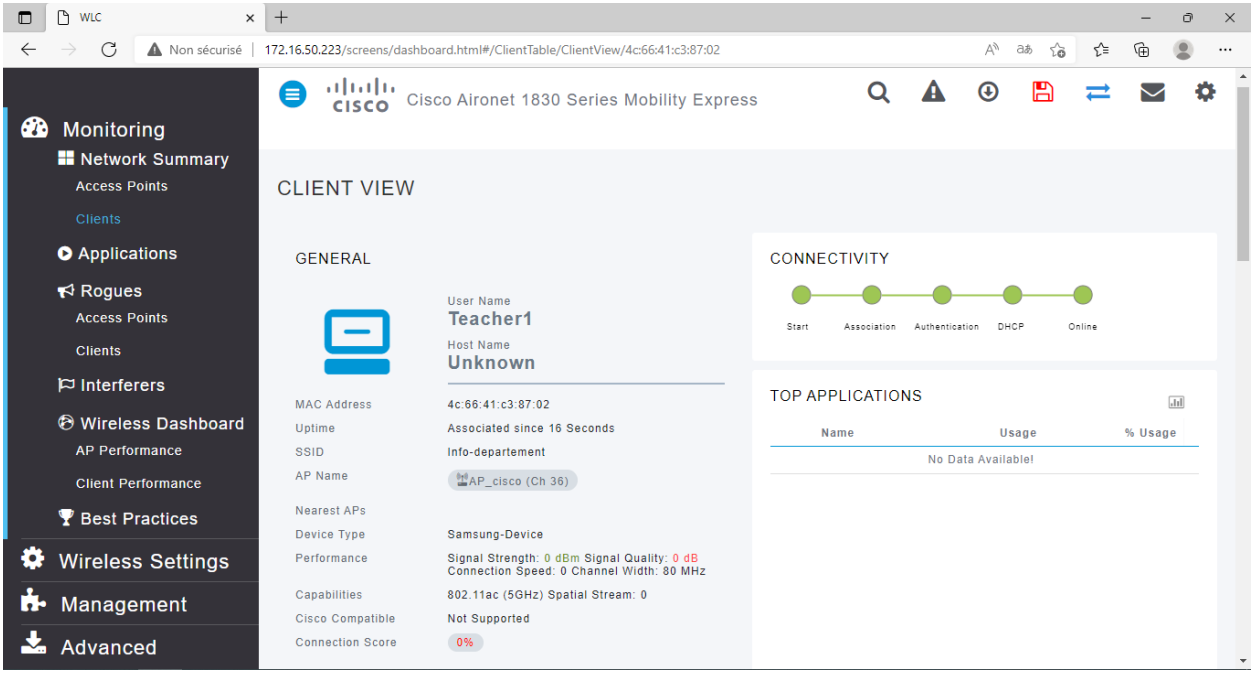


Figure IV-82 fenétre demande l'identité par portable

Le client remplit ses informations et il se connecté avec le réseau si authentification a été bien fait et il est autorisé

Annexe B


WLC
Non sécurisé | 172.16.50.223/screens/dashboard.html#/ClientTable/ClientView/4c:66:41:c3:87:02
Cisco Aironet 1830 Series Mobility Express
Monitoring
Network Summary
Access Points
Clients
Applications
Rogues
Access Points
Clients
Interferers
Wireless Dashboard
AP Performance
Client Performance
Best Practices
Wireless Settings
Management
Advanced
CLIENT VIEW
GENERAL
User Name
Teacher1
Host Name
Unknown
MAC Address 4c:66:41:c3:87:02
Uptime Associated since 16 Seconds
SSID Info-departement
AP Name AP_cisco (Ch 36)
Nearest APs
Device Type Samsung-Device
Performance Signal Strength: 0 dBm Signal Quality: 0 dB
Connection Speed: 0 Channel Width: 80 MHz
Capabilities 802.11ac (5GHz) Spatial Stream: 0
Cisco Compatible Not Supported
Connection Score 0%
CONNECTIVITY
Start
Association
Authentication
DHCP
Online
TOP APPLICATIONS
Name
Usage
% Usage
No Data Available!

Bibliographie

[1] PUJOLLE, Guy. Les réseaux. Editions Eyrolles, 2014.

[2] PILLOU, Jean-François et LEMAINQUE, Fabrice. Tout sur les réseaux et Internet: routeur, switch, téléphonie 3G-4G, CPL, TCP-IP, DNS, DHCP, NAT, VPN, Ethernet, Bluetooth, WiMAX, Wifi etc. Dunod, 2012.

[3] SERVIN, Claude. Réseaux & télécoms: cours avec 129 exercices corrigés. Dunod, 2009.

[4] https://www.commentcamarche.net/contents/1309-reseaux-sans-fil-wireless-networks consulté le 5 avril 2022

[5] DORDOIGNE, José. Réseaux informatiques: Notions fondamentales [4e édition]. 2011.

[6] FRÉDÉRIC, DI GALLO. WI-fi l'essentiel qu'il faut savoir. Extraits de source diverses récoltées en, 2003, p. P5.

[7] https://www.cisco.com/c/en/us/solutions/small-business/resourcecenter/networking/wireless-network.html#~benefits consulté le 15 avril 2022

[9] https://selectra.info/telecom/guides/technologies/wifi-6#tout-comprendre-au-wifi-origines-fonctionnement-et-normes-wifi consulté le 15 avril 2022

[10] https://www.meilleure-innovation.com/wifi-7-tout-savoir/ consulté le 23 avril 2022

[11] https://www.echosdunet.net/dossiers/wifi-6 consulté le 23 avril 2022

[12] https://www.cisco.com/c/fr_ca/solutions/small-business/resource-center/networking/what-is-access-point.html consulté le 1 mai 2022

[13] https://community.fs.com/fr/blog/wireless-lan-controller-explained.html consulté le 1 mai 2022

[14] GAHA, Maher. Sécurité dans les réseaux Wi-Fi: étude détaillée des attaques et proposition d'une architecture Wi-Fi sécurisée. 2007.

[15] https://www.memoireonline.com/11/17/10154/m_Desenclavement-numerique-d-un-site-multidisciplinaire-cas-du-campus-universitaire-du-lac-de-Goma35.html consulté le 18 mai 2022

[16] HOFMANN, Markus et BEAUMONT, Leland R. Content networking: architecture, protocols, and practice. Elsevier, 2005.

[17] PENG, Haishen. WIFI network information securityanalysisresearch. In : 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). IEEE, 2012. p. 2243-2245.…

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

[19] ZIDANI, Ferroudja. Solution d'authentification et de gestion de clés pour le standard 802.11 i des réseaux WiFi. 2018. Thèse de doctorat.

[20] LOHIER, Stephaneet PRÉSENT, Dominique. Réseaux et Transmissions. 2016.
[21] https://www.memoireonline.com/07/09/2324/m_Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite2.html consulté le 20 mai 2022

[22] THINHINANE, Ammariet DJAMILA, Attab. Etude et application des outils de sécurité d'un réseau Wi-Fi. 2015. Thèse de doctorat. Université Mouloud Mammeri.
[23] SERET, Dominique, MEHAOUA, Ahmed, et DORTA, Neilze. réseaux et télécommunications . support de cours, Université René Descartes–Paris, 2006.

[24] NICOPOLITIDIS, Petros, OBAIDAT, Mohammed S., PAPADIMITRIOU, Georgios I., et al. Wireless networks. John Wiley& Sons, 2003.

[25] https://web.maths.unsw.edu.au/~lafaye/CCM/wifi/wifi-wpa2.html

[26] FRAtsit https://br.atsit.in/fr/?p=15747 consulté le 23 mai 2022

[27] J.BISIMWA Ngabo « Exploitation des failles de sécurité et étude des méthodes de protection du réseau wifi de micro finance. Cas de la COOPEC Nyawera » Université Biosadec - Licence 2015.

[28] WIFI Aliance https://www.wi-fi.org/discover-wi-fi/security consulté le 26 mai 2022

[29] BORDÈRES, Serge. Authentification réseau avec Radius: 802.1 x, EAP, FreeRadius. Editions Eyrolles, 2006.

[30] RIDENE, Fètenet RAISSI, Adel. Authentification dans les Réseaux Wifi par le protocole radius. 2011. Thèse de doctorat. Université Virtuelle de Tunis.