République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
Kaissa BERRAHMOUNE
Ghada BOULKROUN

Thème

Les Objets connectés Internet of Everything «IoE »

Mémoire soutenu publiquement le /07/ 2017 devant le jury composé de :

M Prénom NOM
Grade, Lieu d'exercice, Président

M^{me} Leila LAHDIR
Maitre Assistante à l'Université Mouloud Mammeri, Tizi Ouzou. Encadreur

M Prénom NOM
Grade, Lieu d'exercice, Examinateur

M Prénom NOM
Grade, Lieu d'exercice, Examinateur

REMERCIEMENT

On remercie avant tout Dieu le tout puissant qui nous a donné la force et le courage pour réaliser ce modeste travail.

On tient à adresser nos vifs remerciements à l'ensemble des enseignants et l'administration des départements génie électrique qui nous ont accompagnés tout au long de notre cursus à l'Université Mouloud MAMMERI avec beaucoup de patience, de pédagogie et de confiance.

Le succès et l'accomplissement de cette thèse découle d'effort, de confiance et de dévouement offert par notre encadreur Mme LEHDIR qui a bien accepter de superviser notre thèse, de nous avoir aidé par les discussions fructueuses etorientations bénéfiques et indispensables.

Nous tenant également à remercier les membres de jury qui nous font l'honneur de présider et d'examiner notre travail.

Enfin, on remercie tous ceux qui ont participé de loin ou de près à la réalisation de ce travail, ainsi que Mme SAHED, formatrice de l'académie CISCO, qui a mis a notre disposition touts les supports nécessaires à la réalisation de ce travail.

Dédicaces

Je dédie ce travail, à mes très chers parents

A mon frère et mes sœurs

A mon mari

A mon binôme Boulkroun avec qui j'ai partagé ce travail.

Ainsi que tous ceux qui m'ont aidé de près ou de loin.

Kaissa.

Dédicaces

Je dédie ce travail, à mes parents qui m'ont soutenue tout au long de mon cursus.

A mes frères et sœurs, a mes neveux et nièces.

A mes amis

A mon cher binôme Berrahmoune avec qui j'ai partagé ce travail.

Ghada.

SOMMAIRE

Introduction

Introduction

Internet a évolué de telles manières que nous n'aurions jamais pu imaginer. Au tout début, les progrès ont eu lieu lentement. Aujourd'hui, l'innovation et la communication se produisent à un rythme effréné.

Depuis le timide lancement du projet ARPANET (Advanced Research Projects Agency Network) en 1969, dans lequel seulement quelques sites étaient interconnectés, on prévoit aujourd'hui qu'Internet reliera quelque 50 milliards d'objets d'ici 2020. Internet fournit désormais les connexions mondiales qui rendent possibles la navigation sur le Web, les médias sociaux ainsi que l'utilisation des périphériques mobiles intelligents. L'évolution d'Internet a connu quatre phases distinctes. Chacune de ces phases a eu un impact plus profond sur la vie professionnelle et la société que la phase précédente qui est la numérisation des interactions (les entreprises, les réseaux sociaux).

D'une manière générale, lorsque des personnes parlent d'Internet, ils ne se réfèrent pas aux connexions physiques présentes dans le monde réel. En revanche, ils ont tendance à considérer Internet comme un ensemble de connexions dénué de forme. C'est en effet « l'endroit » où les gens se rendent pour rechercher ou partager des informations. Il s'agit par exemple à la fois de la bibliothèque du 21è siècle, d'un magasin de vidéos et d'un album photo personnel.

En très peu de temps, Internet a considérablement modifié notre manière de travailler, de vivre, de nous distraire et d'apprendre. Pourtant, nous ne sommes qu'au début de l'aventure. À l'aide de technologies nouvelles et existantes, nous connectons le monde physique à Internet. C'est en connectant ce qui ne l'est pas encore que nous passons d'Internet à l'Internet of Everything(IoE).

L'IoE repose sur quatre piliers visant à rendre les connexions réseau plus efficaces et plus utiles qu'auparavant, à savoir les personnes, les processus, les données et les objets. Les informations issues de ces connexions conduisent à des décisions et des actions qui créent de nouvelles possibilités, des expériences plus riches et des opportunités économiques sans précédent, et ce, pour les utilisateurs, les entreprises et les pays**.**

Cinquante milliards d'objets fournissent des trillions de gigaoctets de données. Comment ces objets peuvent-ils fonctionner ensemble en vue d'améliorer notre processus de prise de décision et nos interactions afin d'améliorer nos vies privées et professionnelles ?

Introduction

L'activation de ces connexions s'effectue par le biais des réseaux que nous utilisons quotidiennement. Ces réseaux constituent la base d'Internet et, au final, de l'IoE

Qu'est-ce que l'IoE et comment Connecter ce qui ne l'est pas encore ?

Pour comprendre l'IoE et la manière de connecter les objets qui ne le sont pas encore; nous avons réalisé une simulation sur packet tracer qui résume les différentes étapes qui nous ont initié à la compréhension de monde de l'internet des objets . Celle ci présente deux cas a savoir : la maison connectée ainsi l'assistance médicale a temps réel d'un patient diabetique.

Pour mettre en évidence notre travail et définir les déférents points qui relie ces objets entre eux, nous l'avons organisé comme suit :

Apres une introduction générale, des généralités sur les réseaux seront définies dans un premier chapitre.

Le deuxième chapitre introduira les objets connectés considérés comme la troisième évolution de l'internet, baptisé web3.0, le principe de base à leurs compréhensions ainsi que les différents piliers qui les constituent.

La simulation, permettant de mettre en pratique la manière par la quelle les objets sont connectés, est l'objet du troisième chapitre.

Et nous terminerons par une conclusion générale et des perspectives.

Introduction :

La fusion entre la télécommunication et l'informatique a engendré, une technologie moderne qui a su s'imposer en peu de temps pour devenir incontournable dans la gestion de l'entreprise. Il s'agit des réseaux informatiques qui est l'interconnexion de station de travail et de périphérique relier par des matériels ou immatériels, échangeant des informations, selon des regèles biens définis.

Aujourd'hui, l'utilisation de cette technologie pour développer et renforcer notre capacité de communication et devenue de plus en plus développer. La généralisation de l'utilisation d'internet a l'échelle mondiale s'est opérer plus vite que quiconque aurait pu l'imaginer. Le développement de ce dernier verra les novateur se servir d'internet comme un tremplin pour créer de nouveaux produit et services spécialement conçus pour exploiter les capacités des réseaux interconnectés qui forment internet sont appelées a jouer un rôle croissant dans le succès de ce projet.

Les méthodes que nous utilisons pour communiquer évoluent constamment. Alors que nous avons été par le passé limités aux interactions en face à face, les innovations technologiques ont considérablement augmenté la portée de nos communications. Des peintures rupestres à la presse écrite, la radio, la télévision et la vidéo conférence, chaque innovation a amélioré notre capacité à communiquer les uns avec les autres.

I.1. Réseaux :

Les réseaux constituent la base de l'IoE. Les réseaux peuvent être de différentes tailles. Il existe des réseaux élémentaires, constitués de deux ordinateurs, mais également des réseaux extrêmement complexes, capables de connecter des millions de périphériques.

Les réseaux les plus simples permettent de partager des ressources, telles que des imprimantes, des documents, des images et de la musique, entre quelques ordinateurs locaux.

Dans les grandes entreprises et organisations, les réseaux peuvent offrir des produits et des services aux clients par le biais de leur connexion à Internet. Les réseaux peuvent également être utilisés à une échelle encore plus large en vue de permettre la consolidation, le stockage et l'accès aux informations présentes sur des serveurs réseau.

a) Petit réseau :

Les petits réseaux domestiques relient quelques ordinateurs entre eux et a internet.

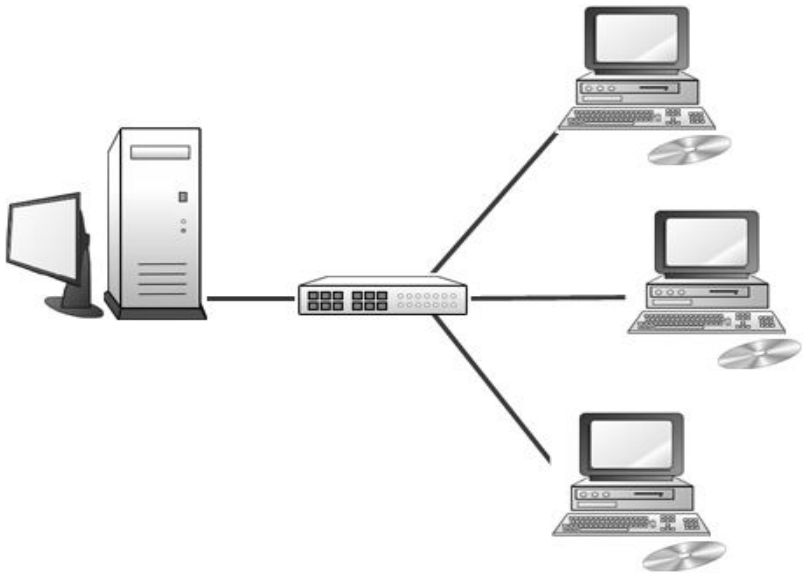

Figure I.1. Petit réseau.

b) Réseau de petit bureau/bureau a domicile :

Dans les réseaux des petits bureaux/bureaux à domicile, un ordinateur peut se connecter au réseau de l'entreprise pour accéder aux ressources.

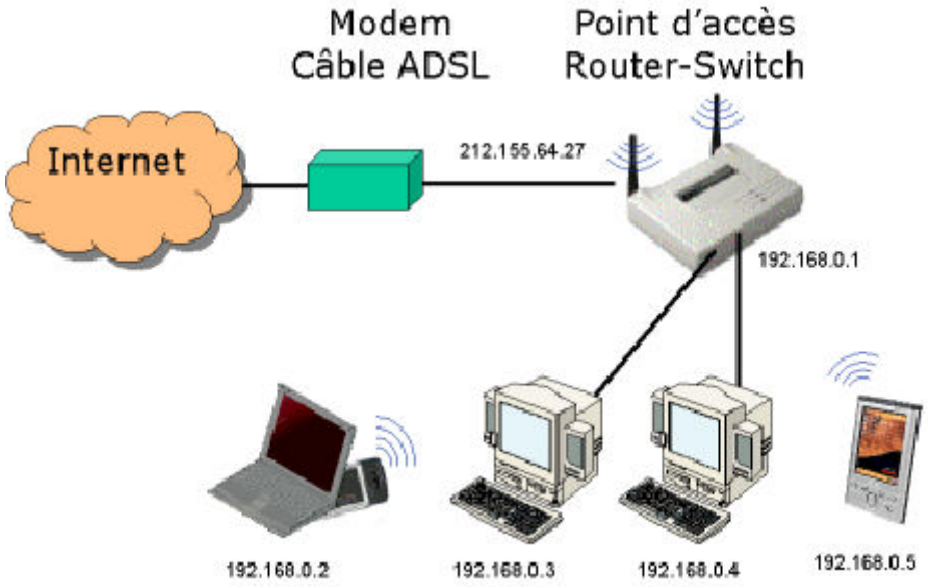

Figure I.2. Réseau petit bureau/bureau a domicile

c) Moyen et grand réseau :

Les moyens et grands réseaux peuvent comporter plusieurs sites avec des milliers d'ordinateurs interconnectés. Ces réseaux peuvent inclure de nouvelles technologies telles que PIN (Places in the Network). Citons par exemple les PAN (Plant Area Network) et les FAN (Field Area Network) qui étendent leur portée et leur puissance au profit des nouvelles applications et des nouveaux appareils.

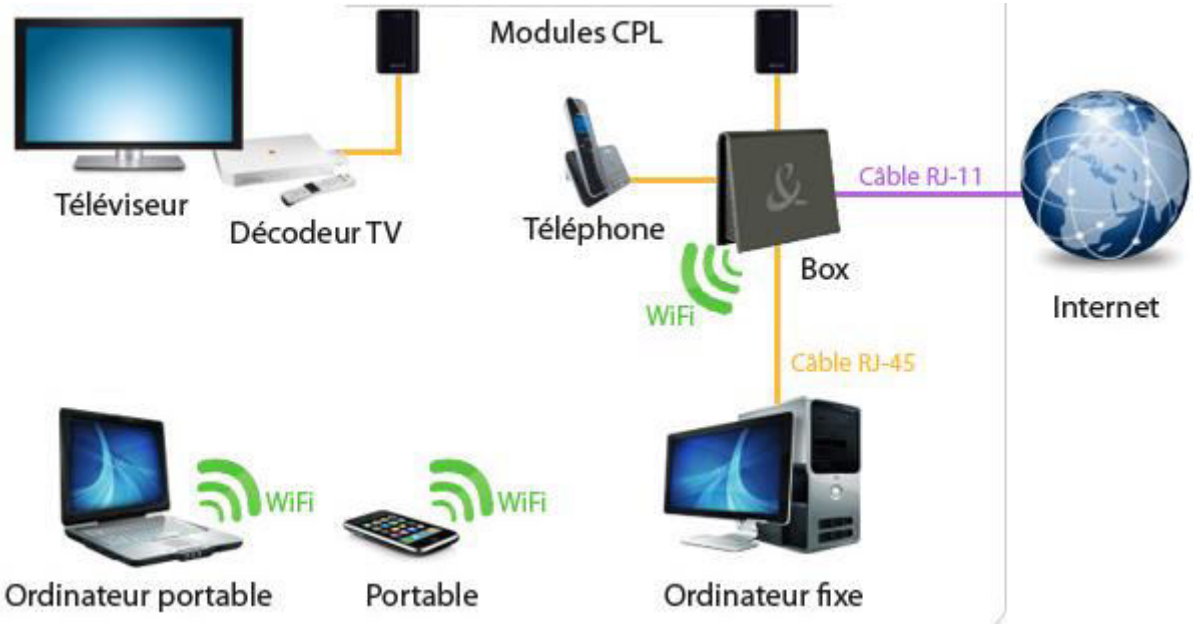

Figure I.3. Moyen et grand réseau.

d) Réseaux mondiaux :

Internet est un réseau qui relie des centaines de millions d'ordinateurs dans le monde.

Figure I.4. Réseaux mondiaux.

I.2 Composants du réseau :

L'infrastructure réseau constitue la plate-forme qui prend en charge le réseau. Elle fournit le canal stable et fiable à travers lequel nos communications peuvent s'établir.

Les périphériques et les supports sont les éléments physiques, ou le matériel, du réseau. Le matériel correspond souvent aux composants visibles de la plate-forme réseau, par exemple un ordinateur portable, un ordinateur de bureau, un commutateur, un routeur, un point d'accès sans fil ou le câblage qui sert à relier ces périphériques. Parfois, certains composants ne sont pas visibles. Dans le cas d'un support sans fil, les messages sont transmis à travers l'air, à l'aide d'une fréquence radio ou d'ondes infrarouges invisibles.

Les composants réseau sont utilisés pour fournir des services et des processus. Les services et les processus sont les programmes de communication, appelés logiciels, qui sont exécutés sur les périphériques réseau. Un service réseau fournit des informations en réponse à une demande.

I.3 Périphériques :

a) Périphériques finaux :

Les périphériques réseau auxquels les personnes sont le plus habituées sont appelés périphériques finaux. Tous les ordinateurs Caméras de surveillance

- Appareils mobiles (smartphones, tablettes, PDA, lecteurs de cartes bancaires et scanners de codes-barres sans fil).

Capteurs, tels que thermomètres, connectés à un réseau et qui participent directement aux communications transmises sur le réseau sont des hôtes. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent.

Voici quelques exemples de périphériques finaux :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers et serveurs. Web)
- Imprimantes réseau.
- Téléphones VoIP.
- Points de terminaison vidéo conférence
- balances et autres périphériques qui seront connectés à l'IoE.

Les périphériques finaux sont la source ou la destination des données transmises sur le réseau. Afin qu'il soit possible de distinguer un périphérique final d'un autre, chaque périphérique final présent sur un réseau est identifié à l'aide d'une adresse. Lorsqu'un périphérique final initie une communication, il utilise l'adresse du périphérique final de destination afin de spécifier à quel emplacement le message doit être envoyé. Nous avons deux type de périphériques finaux qui nous aide a ce connectes a certain nombre d'appareil tel que un serveur et un client qui sont tous les deux périphériques finaux qui se connecte a un réseau précis.

b) Périphériques réseaux intermédiaire :

Les périphériques intermédiaires relient des périphériques finaux. Ils offrent une connectivité et opèrent en arrière-plan pour s'assurer que les données sont transmises sur le réseau. Les périphériques intermédiaires connectent les hôtes individuels au réseau et peuvent connecter plusieurs réseaux individuels afin de former un inter réseau.

Parmi ces périphériques réseau intermédiaires, citons :

- Commutateurs et points d'accès sans fil (accès réseau).
- Routeurs (inter réseaux).
- Pare-feu (sécurité).

Ces périphériques utilisent l'adresse d'hôte de destination, avec les informations concernant les interconnexions réseau, de manière à déterminer le chemin que doivent emprunter les messages à travers le réseau.

Les processus qui s'exécutent sur les périphériques du réseau intermédiaire remplissent les fonctions suivantes :

- Régénérer et retransmettre des signaux de données.
- Gérer des informations indiquant les chemins qui existent à travers le réseau et l'inter réseau.
- Indiquer aux autres périphériques les erreurs et les échecs de communication.
- Diriger des données vers d'autres chemins en cas d'échec de liaison.
- Classer et diriger les messages en fonction des priorités de qualité de service.
- Autoriser ou refuser le flux de données, selon des paramètres de sécurité.

c) Supports réseaux :

La communication sur un réseau s'effectue par l'intermédiaire d'un support, comme un câble ou l'air. Ce support facilite la communication entre la source et la destination.

Les réseaux modernes utilisent principalement trois types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises.

➢ **Définition du fil métallique**

- **Fils métalliques :** Le codage du signal qui doit se produire afin de transmettre le message diffère selon le type de support. Sur des fils métalliques, les données sont codées en impulsions électriques qui correspondent à des modèles spécifiques.
- **Fibres de verre (câbles en fibre optique)** : Les transmissions par fibre optique s'effectuent via des impulsions de lumière, dans des plages de lumière infrarouges ou visibles.
- **Transmission sans fil :** Dans les transmissions sans fil, des modèles d'ondes électromagnétiques illustrent les différentes valeurs de bit.

Les différents types de supports réseau possèdent divers avantages et fonctionnalités. Tous les supports réseau ne possèdent pas les mêmes caractéristiques et ils ne conviennent pas non plus à toutes les applications. Les critères de choix d'un support réseau sont :

- La distance sur laquelle les supports peuvent transporter correctement un signal.
- L'environnement dans lequel les supports doivent être installés.
- La quantité de données et le débit de la transmission.
- Le coût des supports et de l'installation.

I.4 Types de réseaux :

I.4.1 Classement des réseaux par portée :

a) Réseaux LAN :

Infrastructure réseau permettant d'accéder aux utilisateurs et périphériques finaux dans une zone limitée, comme une maison, une école, un immeuble de bureaux ou un campus. Un réseau local fournit une bande passante très élevée aux périphériques finaux et intermédiaires internes.

b) Réseaux MAN :

Interconnexion des réseaux locaux, reliant des ordinateurs situes dans le même espace géographique (inferieur à 100 km).

Exemple : réseau de point de vente dans une ville.

c) Réseau WAN :

Infrastructure réseau permettant de relier entre eux des réseaux locaux sur des zones géographiquement étendues, comme plusieurs villes, provinces, pays ou continents. Les réseaux **WAN** sont généralement détenus par une organisation autonome, comme une entreprise ou une administration publique. Les réseaux WAN fournissent généralement des vitesses de liaison entre réseaux locaux plus faibles que celles en vigueur à l'intérieur d'un réseau local.

d) Les réseaux convergés :

Les réseaux d'aujourd'hui sont en perpétuel évolution, au préalable nous avions deux sortes de réseaux :

Les réseaux de données qui se reposent sur les systèmes informatique connectes et autres technologies pour la transmission de signal.

Les réseaux téléphoniques, radio et télévision qui eux aussi ont leurs technologie de communication a transmission de signal.

Chaque service a son réseau dédié, ses propres règles, et ces normes destiner a sa communication mais l'avancement de la technologie à pu rassembler tout ca de réunir tous sur une seul plat forme qui sont les réseaux convergés qui permet la transmission de la voix , vidéo, image , texte et autre périphériques sur un même canal de transmission.

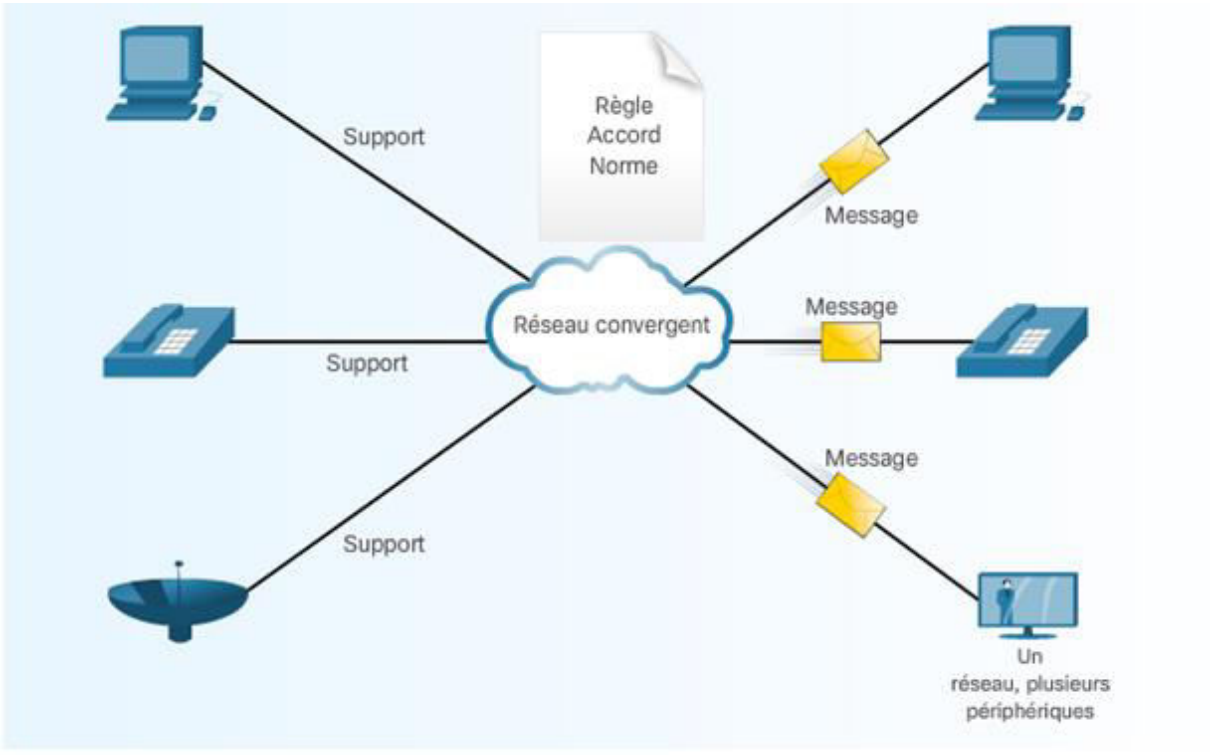

Figure I.5. Réseau convergé

I.5 Architecture réseaux :

L'architecture de réseau est l'organisation d'équipements de transmission, de logiciels, de protocoles de communication et d'une d'infrastructure filaire ou radioélectrique permettant la transmission des données entre les différents composants.

I.5.1 Modèle poste à poste :

Dans une architecture poste à poste, contrairement à une architecture de réseau informatique de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du *réseau* est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau informatique.

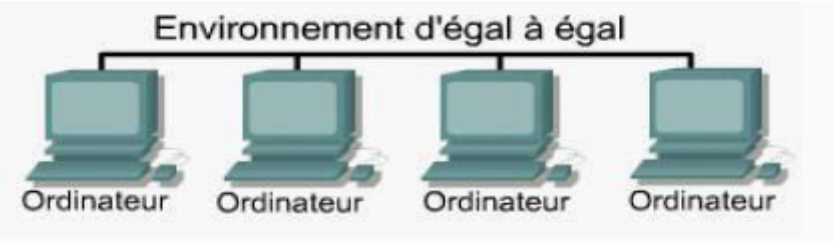

Figure I.6 : Modèle poste à poste.

- **Modèle clients serveur :**

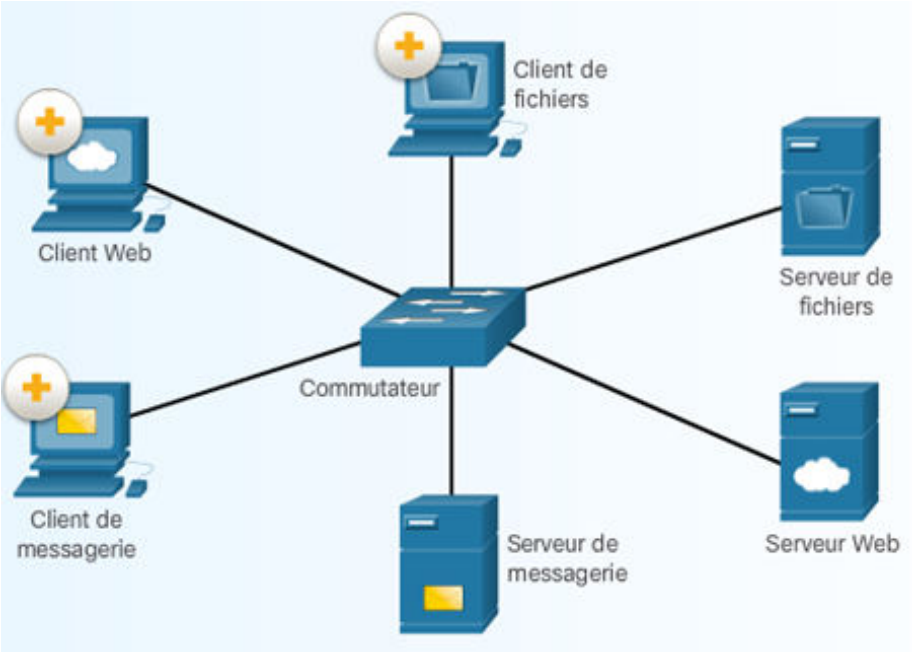

Figure I.7. Modèle client serveur

La compréhension de la connectivité réseau est une étape importante dans la compréhension du mode de déplacement des données sur le réseau.

Depuis la création d'Internet, la méthode principale utilisée par les entreprises pour le traitement des données a été le modèle client-serveur. On peut implémenter des serveurs de fichiers. Les utilisateurs finaux appartenant à une organisation peuvent stocker un nombre quelconque de fichiers et de documents sur le serveur de fichiers, tout en permettant aux périphériques finaux de conserver de la mémoire et de la puissance de traitement pour les applications locales. Le stockage des fichiers sur un serveur de fichiers central permet aux autres utilisateurs de l'organisation d'accéder facilement à ces fichiers, d'où une collaboration plus efficace et un meilleur partage des informations. La présence de services centralisés (comme les serveurs de fichiers) permet une sécurité centralisée ainsi que des procédures de sauvegarde destinées à assurer la protection de ces ressources.

Avec le développement d'internet le modèle client-serveur n'est pas tres efficaces car, de plus en plus d'individus se connectant à partir de distances toujours plus éloignées, l'utilisation d'un serveur centralisé peut ne pas être optimale. En effet, il se peut que les personnes situées loin du serveur connaissent des délais plus importants et rencontrent plus de difficultés à accéder aux informations. Ces changements en matière d'exigences des organisations et des individus a conduit au développement du **Cloud Computing.**

I.6. Equipements d'interconnexion réseaux informatique :

Pour répondre à l'accroissement d'une entreprise, nous devons étendre son réseau. Chaque topologie ou architecture réseau possèdent ses propres limites, il est toutefois possible d'installer des composants pour augmenter la taille du réseau, pour cela nous avons fait appel a des équipements d'interconnexion réseaux tel que :

a) Répéteurs :

Le répéteur est le dispositif qui permet de régénérer et d'amplifier le signal qui arrive en fin de course (fin de segment) cela permet d'étendre le réseau

Figure I.8. Répéteur.

b) Concentrateurs (hub) :

Le concentrateur, ou le hub, est un équipement dit de couche 1 du modèle OSI c'est-à-dire qu'il travaille au niveau électrique de l'envoie du signal. C'est un boitier qui possède des prises de RJ45 femelles sur lesquelles on peut brancher des câbles a paire torsadées avec des prises RJ45 males.

Le hub reçoit donc un signal électrique sur un de ses ports (une de prises RJ45 femelles) et réémet le signal électrique reçu sur les autres ports pour que les machines connectes reçoivent le signal. Ainsi, elles peuvent dialoguer entre elles par l'intermédiaire du hub.

Ce boitier qui centralise la connexion des machines simule une topologie dite **en bus,** ou toutes les machines connectées au media qui transmet l'information reçoivent le signal transmis.

L'un des inconvenants de cet équipement est donc que le media qui permet le dialogue est partage entre toutes les machines. Elles utilisent toutes ce même media, et lorsque deux signaux envoyés en même temps par deux machines se superposent, ils en résultent une collision au niveau du signal électrique qui devient alors incompréhensible .Plus il y a de machine et plus la probabilité d'obtenir des collisions est importante. Ainsi le nombre de machine que l'ont peut connecter a un ou plusieurs hubs est limite. Le hub crée donc ce que l'on appelle un domaine de collusion .Les réseaux développant de plus en plus, il est devenu important de trouver une nouvelle technologie permettant de s'affranchir de ce problème .Ainsi sont arrives les ponts.

Figure I.9. Concentrateur.

c) Commutateurs (Switch) :

- Le commutateur, ou Switch, est donc aussi un équipement de couche 2. Il est ainsi capable d'interpréter les informations de couche 2 contenue dans la trame réseau. Et en plus il a **x ports**, ce qui fait qu'il sépare x domaines de collusions. Ainsi, on peut connecter des machines entre elles par l'intermédiaire d'un Switch.
- Un Switch a donc un domaine de collusion par port, et on dit qu'il crée un domaine de broadcast, qui sont les messages destines à toutes les machines du réseau, sont envoyés sur tout les ports du Switch.
- Ces différents équipements de connexion qui permettent de connecter plusieurs machines entre elles. Par contre, ils ne permettent pas à deux machines sur des réseaux différents de dialoguer, cela ne peut se faire qu'à travers un routeur.

Figure I.10. Commutateurs.

d) Routeurs :

Un routeur est un périphérique qui achemine le trafic à partir du réseau local vers les périphériques situés sur les réseaux distants. La présence d'un routeur est nécessaire, car les périphériques finaux ne conservent pas les informations relatives à la localisation des destinations distantes vers lesquelles ils envoient leurs paquets. Un routeur est un périphérique intelligent qui collecte des informations sur l'emplacement des différents réseaux. Le routeur utilise ces informations pour déterminer le meilleur chemin permettant d'atteindre ces destinations, ce qui est connu sous le nom de processus de routage.

Il existe de nombreux types de routeur d'infrastructure qui nécessite :

- Des systèmes d'exploitation.
- Des processeurs.
- Des interfaces d'entrée/sortie (E/S).
- De la mémoire.

Ce boitier qui centralise la connexion des machines simule une topologie dite **en bus,** ou toutes les machines connectées transmettent l'information qui reçoit le signal transmis.

L'un des inconvenants du concentrateur, c'est qu'il permet le dialogue est partage entre toutes les machines. Elles utilisent toutes ce même media, et lorsque deux signaux envoyés en même temps par deux machines se superposent, ils en résultent une collision au niveau du signal électrique qui devient alors incompréhensible .Plus il y a de machine et plus la probabilité d'obtenir des collisions est importante. Ainsi le nombre de machine que l'ont peut connecter a un ou plusieurs hubs est limite. Le hub crée donc ce que l'on appelle un domaine de collusion .Les réseaux se développent de plus en plus, il est devenu important de trouver une nouvelle technologie permettant de s'affranchir de ce problème .Ainsi sont arrives les ponts.

Figure I.11. Routeur.

e) Ponts (bridge) :

Le pont, ou le bridge, est un équipement de couche 2. Cela veut dire qu'il est capable d'interpréter les informations de couche 2 contenues dans la trame réseau, comme par exemple Ethernet. Notamment, il peut lire les adresses MAC source et destination et savoir quelle machine dialoguer avec l'autre, et dans ce cas, n'envoyer les informations qu'a la bonne machine de destination. Ainsi, on réduit très fortement le risque de collusion. Par contre, le pont n'a que deux ports. Il peut donc séparer un domaine de collusion en deux, pour

limiter le nombre de collusion. Il permet aussi dans certain cas de passer d'un protocoles de couche deux à une autre, d'Ethernet a Toking Ring. Ainsi, on peut utiliser un pont pour connectées deux domaines de collusion, par exemple **deux hubs.** On augmente ainsi le nombre de machines que l'on peut ajouter dans le réseau.

Figure I.12. Pont.

I.7 Modèle OSI :

Le **modèle OSI** (de l'anglais ***O**pen **S**ystems **I**nterconnection*) c'est un modèle de communications entre ordinateurs proposé par l'ISO qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

a) Les différentes couches du modèle OSI :

Le modèle OSI se compose de couches supérieures et de couches inferieures.

Les couches supérieurs : application, présentation, session, ces couches du modèle OSI sont souvent appelées couches des applications.les couches sont chargées sur une interface utilisateur du formatage de données et de l'accès aux applications.

b) Couche application :

Elle fournit des services utilisables sur le réseau par les applications installées.

Les principaux services sont :

- Transfert de fichiers(FTP)
- Messagerie ou courrier électronique
- Lecteur de pages Internet (http)
- Accès à distance(Telnet)

c) Couche présentation :

Elle permet de transcrire les données dans un format compréhensible par les deux systèmes (formatage des données)

- Elle assure la mise en forme de l'information pour qu'elle soit accessible à l'utilisateur
- Elle effectue les fonctions de codage, compression, cryptage, et décryptage.

d) Couche session :

C'est la première couche orientée traitement :

- Elle permet l'ouverture et la fermeture d'une session de travail entre deux systèmes distants et assure la synchronisation du dialogue.
- Elle définit le mode de transmission (half duplex, full duplex)
- Elle définit la liaison entre deux programmes d'application et gère le dialogue.

Les couches inferieures : Physique, liaison ; réseau, transport : ces couches ont pour rôle de définir la manière dont les données sont transmis sur un support physique via les équipements réseau jusqu'à la station terminale de destination.

e) Couche physique :

Elle se charge de l'adaptation du signal au support de transmission, ce qui définit les caractéristiques électriques, logique et physiques de la station sur le réseau (câbles, connecteurs, cartes réseau,…)

- Elle gère le type de transmission (synchrone ou asynchrone)
- S'il y a lieu, elle met en œuvre les mécanismes de modulation et démodulation du signal
- L'unité d'échange est le bit

f) Couche liaison :

- Elle définit les règles d'émission et de réception des données à travers la connexion physique de deux systèmes
- Elle doit transmettre les données sans erreurs et détermine la méthode d'accès au support
- Elle met en œuvre la détection et la correction des erreurs

- Elle gère les réémission s'il y a lieu
- Elle établir et contrôle la liaison au niveau logique
- L'unité d'échange est la trame

g) Couche réseau :

- Elle gère l'acheminement des données en assurant le routage (choix du trajet) des paquets de données
- Si un nœud est surcharge ou hors service, les données seront alors routées vers un autre nœud
- L'unité d'échange est le paquet
- La couche réseau assure également la traduction des adresses logique en adresses physiques

h) Couche transport :

- Elle fournit un service de transport de bout en bout transparent pour l'utilisateur (même à travers plusieurs réseaux)
- Elle assure également les services qui n'ont pas été pris en compte par les couches inferieures (gestion des erreurs, routage…)
- Elle permet de multiplexer plusieurs flux sur le même support
- En tant qu'émetteur, elle segmente les messages en paquet numérotés
- En tant que récepteur, elle reconstitue les messages en plaçant les paquets dans l'ordre

I.8 Le modèle de référence TCP/IP :

I.8.1 Définition :

TCP/IP est un protocole d'internet qui a un ensemble de règles, de procédures qui détermine le processus de réalisation d'une action.

TCP/IP est un protocole de communication : il décrit comment les messages sont transportés et adressés dans un réseau.

I.8.2 Les différentes couches du modèle TCP/IP :

a) La couche réseau :

La couche réseau est la première couche de la pile TCP/IP, en effet, elle recouvre les couches physiques et liaison de données du modèle OSI

b) La couche internet :

Réalise l'interconnexion des réseaux hétérogènes distants

- permettre l'injection de paquets dans n'importe quel réseau et acheminement de ces paquets indépendamment les uns des autres jusqu'à destination
- Gère le routage des paquets au travers des réseaux empruntés Protocole IP (Internet Protocol)

c) La couche transport :

La couche transport assure l'acheminement des données sur le réseau local. Elle gère deux protocoles de livraison des informations.

TCP :

- assure le contrôle des données et orienté la connexion (vérifier les envois des données par des signaux d'accusés de réception)

UDP :

- Plus simple que TCP mais non fiable (remise non garantie)
- Fonctionne sans connexion
- Plus rapide que TCP
- Il utilisé quand on néglige volontairement le contrôle de flux et le séquencement des paquets.

d) La couche application :

La couche application englobe les applications standard du réseau :

- SMTP :(Simple Mail Transport Protocole), gestion des mails.
- TELNET : protocole permettant de se connecter sur une machine distante serveur en tant qu'utilisateur.
- FTP (File Transport Protocole) protocole permettant d'échanger des fichiers via le réseau.

I.9 Comparaison entre modèle OSI et le modèle TCP/IP :

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication a couche et utilisent l'encapsulations des données. On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches de modèle OSI dans des couches plus générales
- TCP/IP est plus qu'un modèle de conceptions théorique, c'est sur lui que repose le réseau internet actuel.

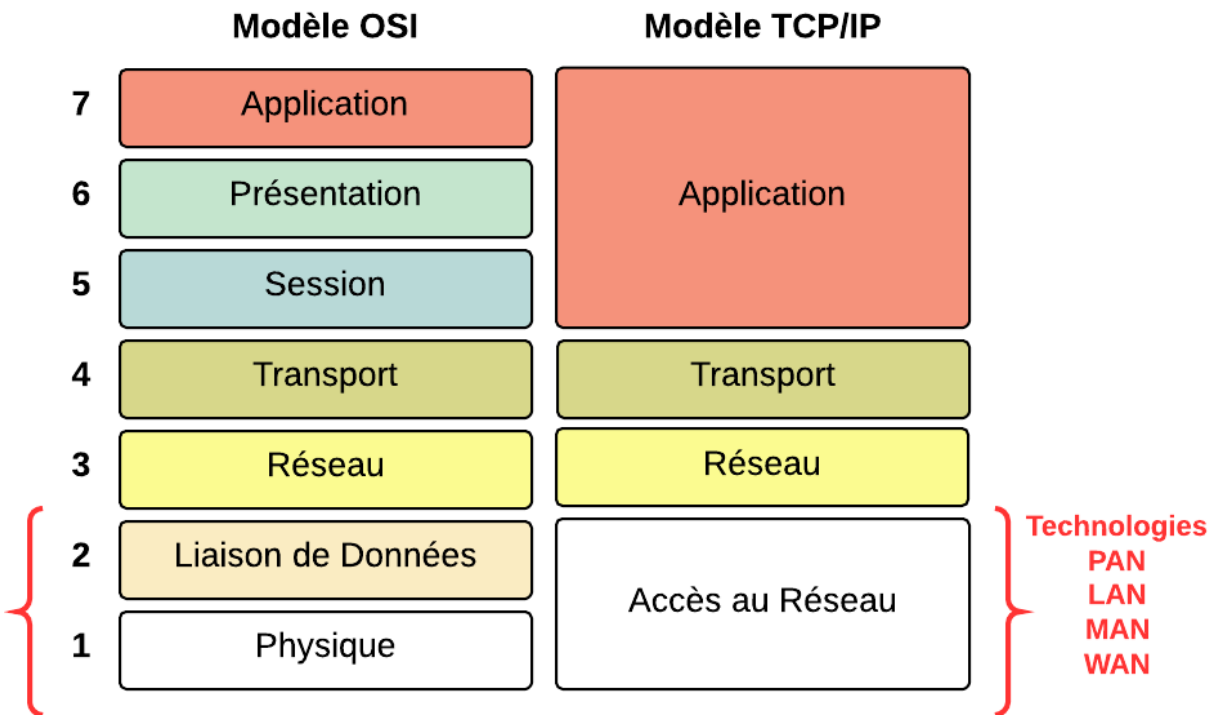

Figure I.13. Comparaison entre OSI et TCP/IP.

I.10 Adressage IP :

Dans les réseaux de données, les périphériques sont identifiés par des adresses IP numériques pour l'envoi et la réception de données sur les réseaux. La plupart des gens ne retiennent pas cette adresse numérique. Pour cette raison, des noms de domaine ont été créés pour convertir les adresses numériques en noms simples et explicites.

Le protocole DNS (Domain Name System) a été créé afin de permettre la résolution de nom pour ces réseaux. Le protocole DNS utilise un ensemble distribué de serveurs pour convertir les noms associés à ces adresses en numéros.

I.10.1 Structure d'une adresse IP :

- **Identificateur de réseau (Net Id) :**

La première partie de l'adresse IP correspond a l'indicateur de réseau, qui identifie le segment de réseau sur lequel se trouve l'ordinateur.

Cet identificateur doit être le même pour tout les ordinateurs qui se trouvent sur un même segment.

- **Identificateur d'hôte (host Id) :**

La deuxième partie de l'adresse IP correspond a l'indicateur d'hôte, qui identifie un ordinateur, un routeur ou tout autre périphérique sur un segment. L'identificateur de chaque hôte doit être unique dans l'identificateur de réseau.

I.10.2 L'adresse logique (IP) :

L'adresse IP d'un nœud est une adresse logique définie indépendamment de toutes topologies d'ordinateur ou de réseau .sont format reste identique quelque soit le support utilisé.

Pour être en mesure d'échanger des paquets entre ordinateurs TCP/IP nécessite l'utilisation de trois valeurs :

- Une adresse IP : qui identifie de manière unique chaque hôte sur le réseau
- Un masque de sous réseau : qui permet de distinguer le type de réseau ou de segmenter celui-ci en plusieurs sous réseau.
- Une passerelle par défaut : qui est l'adresse où sont envoyés les paquets distingué aux autres réseaux ou sous réseau.

10.2 Classes d'adresses :

Il existe 5 classes d'adresses IP :

- **Classe A :**

Dans cette classe l'adresse réseau est définie sur 7 bits et l'adresse hôte sur24 bits.

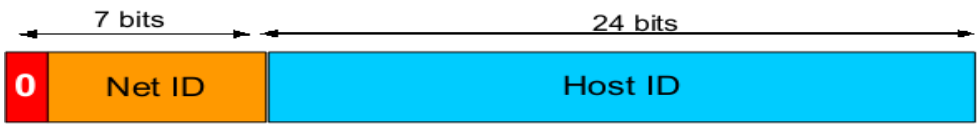

Figure I.14 Classe A.

- **Classe B :**

Dans cette classe, l'adresse réseau est sur 14 bits et l'adresse hôte sur 16 bits.

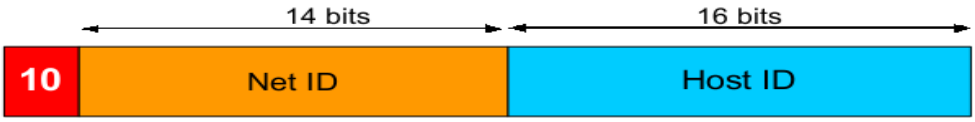

Figure I.15 Classe B.

- **Classe C :**

Dans cette classe l'adresse du réseau est codifiée sur 21 bits et l'adresse hôte sur 8 bits

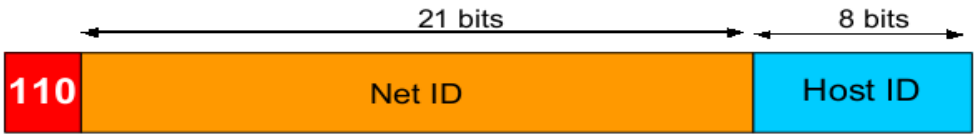

Figure I.16 Classe C.

- **Classe D :**

Dans cette classe l'adresse du réseau est codifiée sur 28 bits et sert à diffuser des trames vers des groupes de stations.

Figure I.17 Classe D.

10.2.5 Classe E :

Cette classe est réservée à un usage futur.

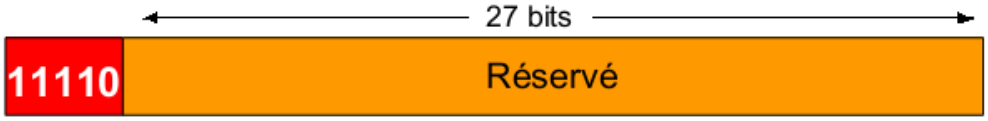

Figure I.18 : Classe E

I.11 Les types d'adresse :

a) Adresse statique :

Quand une configuration IP est réalisée sur chaque machine du réseau en spécifiant de façon fixe son adresse ; on parle de configuration statique.

b) Adresse dynamique :

Si l'affectation des adresses est laissé à un serveur sur le réseau ; on parle d'affectation dynamique.

Le serveur chargé d'attribuer les adresses IP fait appel au protocole DHCP

I.12 Le protocole DHCP (Dynamic Host Configuration Protocol) :

Ce protocole permet une configuration dynamique des adresses IP et des informations associées, ceux-ci signifie que chaque hôte de réseau est capable de solliciter de lui-même une configuration IP auprès d'un serveur spécialisé appelé serveur DHCP. L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'hôte peut utilisé une configuration IP attribuée avant de devoir solliciter le renouvellement de bail auprès de serveur DHCP

Le DHCP :

- Facilite la gestion du réseau
- Empêche les conflits d'adresse
- Contrôle l'affectation des adresses IP de manière centralisé

I.13 Adresses réservées :

- **Adresse de diffusion :**

C'est une adresse dont tous les bits d'identificateur d'hôte sont positionnes a 1.

- **Adresse du réseau :**

C'est une adresse dont tous les bits d'identificateur d'hôte sont positionnes a 0.

- **Adresse de bouclage (Loopback) :**

Permettent aux utilisateurs d'effectuer des tests sur le fonctionnement de leurs carte réseaux, elle redirige le trafic vers l'émetteur.

I.14 Gestion des adresses :

Sur Internet, chaque adresse IP doit être unique. L'IANA (Internet Assigned Numbers Authority) est responsable du contrôle de la distribution des adresses IP de manière à éviter les erreurs. Cette association alloue des blocs d'adresses IP à l'un des cinq organismes d'enregistrement Internet locaux situés dans les différentes parties du monde. Les FAI obtiennent ensuite des blocs d'adresses IP de la part de l'organisme d'enregistrement Internet correspondant à leur région géographique.

Le FAI détermine où transférer le trafic. Les paquets sont transmis d'un routeur à l'autre, parfois par l'intermédiaire des réseaux de plusieurs FAI, jusqu'à atteindre leur destination finale. Les routeurs de chacun des FAI utilisent l'adresse de destination des paquets IP pour déterminer le meilleur itinéraire sur Internet. La commutation de paquets est un processus transparent pour l'utilisateur, celui-ci ne voyant en effet que ce qui a été envoyé et reçu.

I.15 les différents types de topologies :

Une topologie de réseau est une carte identifiant les différents éléments d'un réseau informatique. Un réseau peut être caractérisé par deux types de topologies, à savoir une topologie physique et une topologie logique.

a) Topologie physique

La topologie physique montre la disposition et l'emplacement de l'ensemble des périphériques présents dans le réseau. Elle décrit les interconnexions réelles entre les périphériques, réalisées à l'aide de fils et de câbles, comme illustré à la **Figure I.19**.

Cette topologie physique varie lors de l'intégration de périphériques mobiles, ces périphériques ont besoin d'une connectivite permanente pour permettre une liaison de données vers les contrôleurs.

Certains éléments doivent être pris en considération lors de la détermination d'une topologie physique :

- L'emplacement des ordinateurs des utilisateurs
- La position des équipements réseau, tels que les commutateurs, les routeurs et les points d'accès sans fil
- La position des contrôleurs et des serveurs
- La position des capteurs et des actionneurs
- Le potentiel de croissance future du réseau

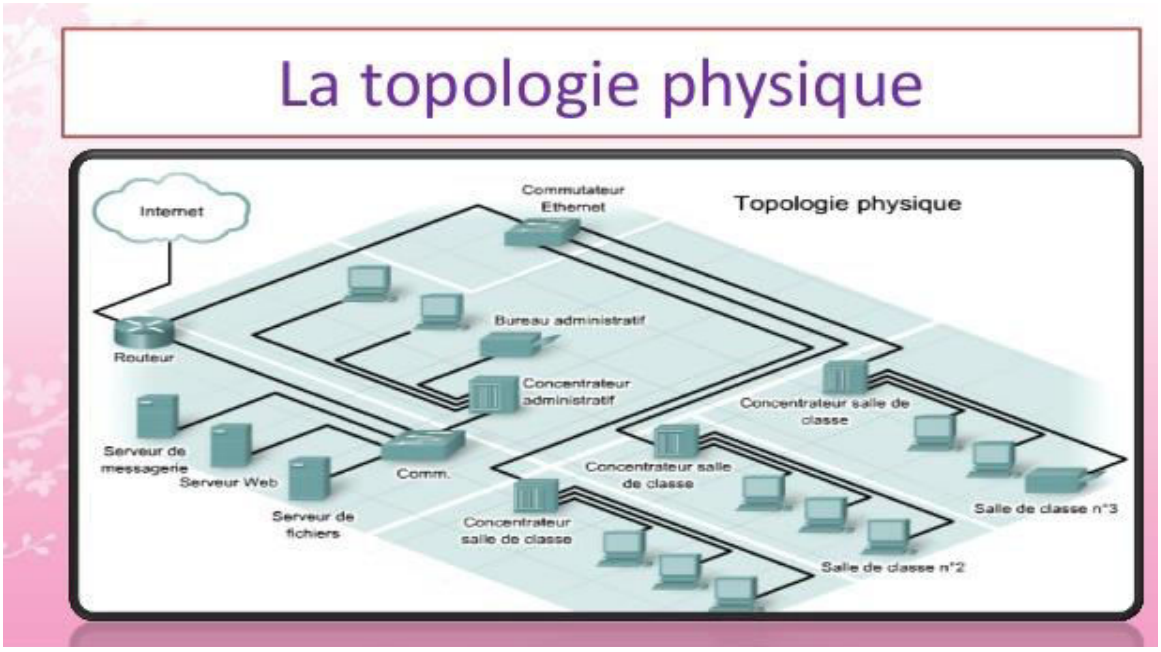

Figure I.19 : La topologie physique

b) Topologie logique :

Les topologies logiques se basent sur le mode de fonctionnement des protocoles de communication et concernent un point de vue différent de celui des topologies physiques. La topologie logique indique comment les données sont transmises sur le réseau. Elle décrit comment les périphériques échangent des données avec les utilisateurs du réseau.

1) La topologie en bus :

Une topologie en bus désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie.

2) La topologie en anneau :

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

3) **La topologie en étoile :**

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, qui le régénère, et qui le transmet qu'à son destinataire. C'est en réalité un réseau de "n" liaisons point par point, car il établit un circuit entre une paire d'utilisateurs.

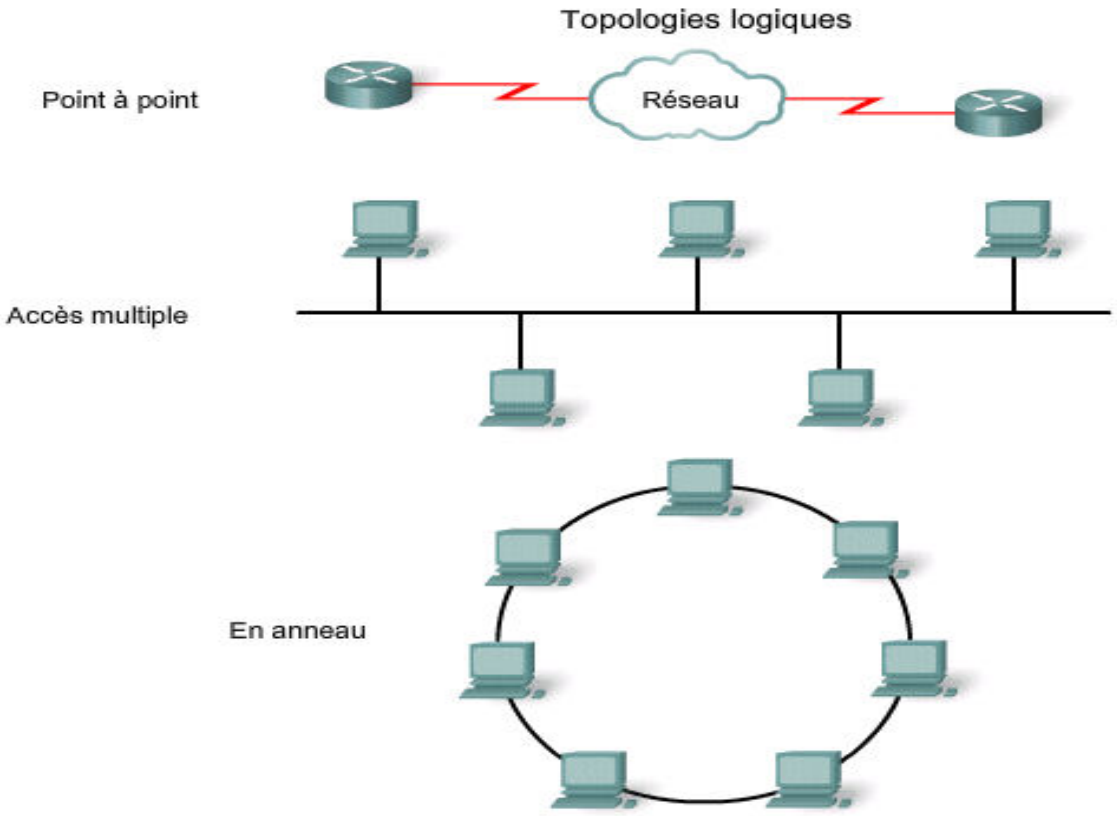

Figure I.19 : Topologie logique.

Conclusion :

Dans notre travaille on est arrivées au terme que les réseaux d'aujourd'hui sont de plus en plus développer par leur différents équipements de connexion et d'interconnexion, nous citons a titre d'exemple les répéteurs, concentrateurs, ponts, Switch, et les routeurs qui est de plus en plus utiliser a notre époque.

Par ailleurs nous avons eu à faire aux protocoles et architectures réseaux tel que le modèle OSI, le modèle TCP/IP et l'adressage IP qui a pris une grosse partie dans notre travaille ce qui nous prépare dans les étapes à suivre ou nous allons parler des différentes adresses IP et leurs gestions des phases d'internet et les différentes technologies utilisées pour pouvoir connecter ce qui ne l'est pas encore.

Introduction :

L'évolution d'Internet a connu quatre phases distinctes. Chacune de ces phases a eu un impact plus profond sur la vie professionnelle et la société que la phase précédente.qui est la numérisation des interactions(les entreprises, les réseaux sociaux).

Au fil des ans, les sociétés technologique on en effet recherché de nouveaux modes de communication et de collaboration. L'avantage de l'IoE découle de l'impact combiné de ces connexions et de la valeur que cette connectivité qui a augmenté crée au fur et à mesure que « tout » est mis en ligne.

Figure 1 : les quatre phases d'internet.

.II.1 Les acteurs principaux de l'internet des objets :

L'IoE repose sur quatre piliers visant à rendre les connexions réseau plus efficaces et plus utiles qu'avant, à savoir les personnes, les processus, les données et les objets.

a) Les personnes :

Aujourd'hui, la plupart d'entre nous tissent des liens sociaux par le biais des périphériques connectés au web. Au fur et à mesure que l'IoE évoluera, de nouvelles façons de communiquer verront le jour.

Pour établir une interaction machine a personne ou machine à machine l'intervention de l'être humain est obligatoire vue que sans l'intervention de ce dernier cette interaction ne peut pas avoir lieu.

b) Les processus :

Les processus interviennent entre tous les autres piliers de l'IoE. C'est l'ensemble des éléments qui relie les personnes les objets et les données et leur permet de ce connecter entre eux. Ces connexions apportent la bonne information, aux bonnes personnes, au bon moment et de la manière la plus pertinente.

c) Les données :

Les données sont les informations générées par les personnes et les objets. Ces données, combinées aux analyses, fournissent des informations exploitables sur les personnes et les machines. Cela aboutit à de meilleures décisions et à de meilleurs résultats.

c.1) Gestion des données :

Les ordinateurs ne disposent généralement pas de la sensibilité contextuelle et de l'intuition des êtres humains. Par conséquent, il est important de tenir compte des deux états de données suivants : structurées et non structurées.

- **Données structurées :**

Les données structurées sont des données qui sont entrées et mises à jour dans des champs fixes au sein d'un fichier ou d'un enregistrement. Elles sont facilement entrées, classées, interrogées et analysées par un ordinateur.

- **Données non structurées :**

Les données non structurées ne possèdent pas l'organisation que l'on retrouve dans les données structurées. Ce sont des données brutes, Il n'est par conséquent pas possible d'identifier leur valeur, et ne présentent pas de moyen défini permettant de les saisir, de les regrouper et de les analyser.

Au fil des années, l'espace de stockage disponible a augmenté de manière exponentielle. À l'heure actuelle, on parle de téraoctets.

Il existe trois types principaux de modes de stockage des données :

- **Données locales** :

Concerne des données accessibles directement à partir de périphériques locaux. Les disques durs, les lecteurs flash USB et les CD/DVD sont des exemples de stockage local de données.

- **Données centralisées** :

Données stockées et partagées à partir d'un serveur centralisé unique. Ces informations sont accessibles à distance à l'aide de plusieurs périphériques sur le réseau ou sur Internet. L'utilisation d'un serveur de données centralisées peut générer des dysfonctionnements, pouvant donner lieu à l'apparition de défaillance.

- **Données distribuées** :

Données gérées par un système de gestion de bases de données centralisé. Les données distribuées sont répliquées et stockées dans divers emplacements. Cela permet un partage à la fois aisé et efficace des données. Elles sont accessibles par le biais de l'utilisation d'applications locales et globales. Avec un système distribué, il n'y a pas de défaillance. Si un site n'est plus alimenté, les utilisateurs peuvent toujours accéder aux données à partir des autres sites.

c.2) Données en mouvement :

D'une manière générale, les données sont considérées comme des informations collectées avec le temps.

Toutefois, avec la croissance accélérée du volume des données, la majeure partie de la valeur de ces données est perdue pratiquement dès la création de celles-ci. Les périphériques, les capteurs et la vidéo sont à l'origine de cette croissance permanente du volume de nouvelles données. Elles présentent une valeur ajoutée maximale, étant donné qu'elles interagissent en temps réel, elles portent le nom de « données en mouvement ».

Cet afflux de nouvelles opportunités de données offre de nouveaux moyens d'améliorer notre monde. Il existe un potentiel incroyable pour des solutions intelligentes capables de collecter, de gérer et d'évaluer des données à la vitesse des communications

humaines. Par conséquent, l'Internet of Everything concernera de plus en plus des « données en mouvement ».

- **Fournisseurs d'accès Internet (FAI) :**

Dans les environnements de stockage de données centralisées et distribuées, les données doivent être transportées sur le réseau ou sur Internet.

Les périphériques qui transfèrent des données sur Internet doivent utiliser un fournisseur d'accès Internet (FAI). Il permet à des particuliers et à des entreprises d'accéder à Internet, et il peut également être relié à d'autres FAI..

Internet se compose de liaisons de données haut débit qui relient ensemble de nombreux FAI. Ces interconnexions font partie d'un immense réseau haute capacité, appelé le « réseau fédérateur Internet ».

d) Les objets :

Les objets sont des dispositifs matériels connectés à Internet et entre eux. Ils détectent et recueillent plus de données, deviennent sensibles au contexte et fournissent des informations plus concrètes pour aider les personnes et les machines.

Actuellement, le pilier Objets, se compose principalement de divers types d'ordinateurs et de périphériques informatiques traditionnels, Toutefois, l'IoE intégrera à l'avenir tous les types d'objets, y compris les objets et les périphériques qui ne sont généralement pas connectés.

Les objets connectés sont dotés d'une technologie intégrée qui leur permet d'interagir avec des serveurs internes et leur environnement externe. Ils sont compatibles avec le réseau et sont capables de communiquer par l'intermédiaire d'une plate-forme réseau sécurisée, fiable et disponible.

L'IoE se base sur les connexions entre les personnes, les processus, les données et les objets. Ce sont les quatre piliers de l'IoE. Toutefois, l'IoE n'a pas pour but de développer ces quatre dimensions de manière isolée. En effet, chacune amplifie les capacités des trois autres. C'est à l'intersection de l'ensemble de ces éléments que se situe la véritable puissance de l'IoE.

II.2) Interactions dans l'IoE :

Les interactions entre les divers éléments présents dans les quatre piliers créent une quantité de nouvelles informations. Les piliers interagissent d'une manière qui établit trois principaux types de connexions au sein de l'environnement IoE : personnes communiquant avec des personnes (P2P), machines communiquant avec des personnes (M2P) et machines communiquant avec des machines (M2M).

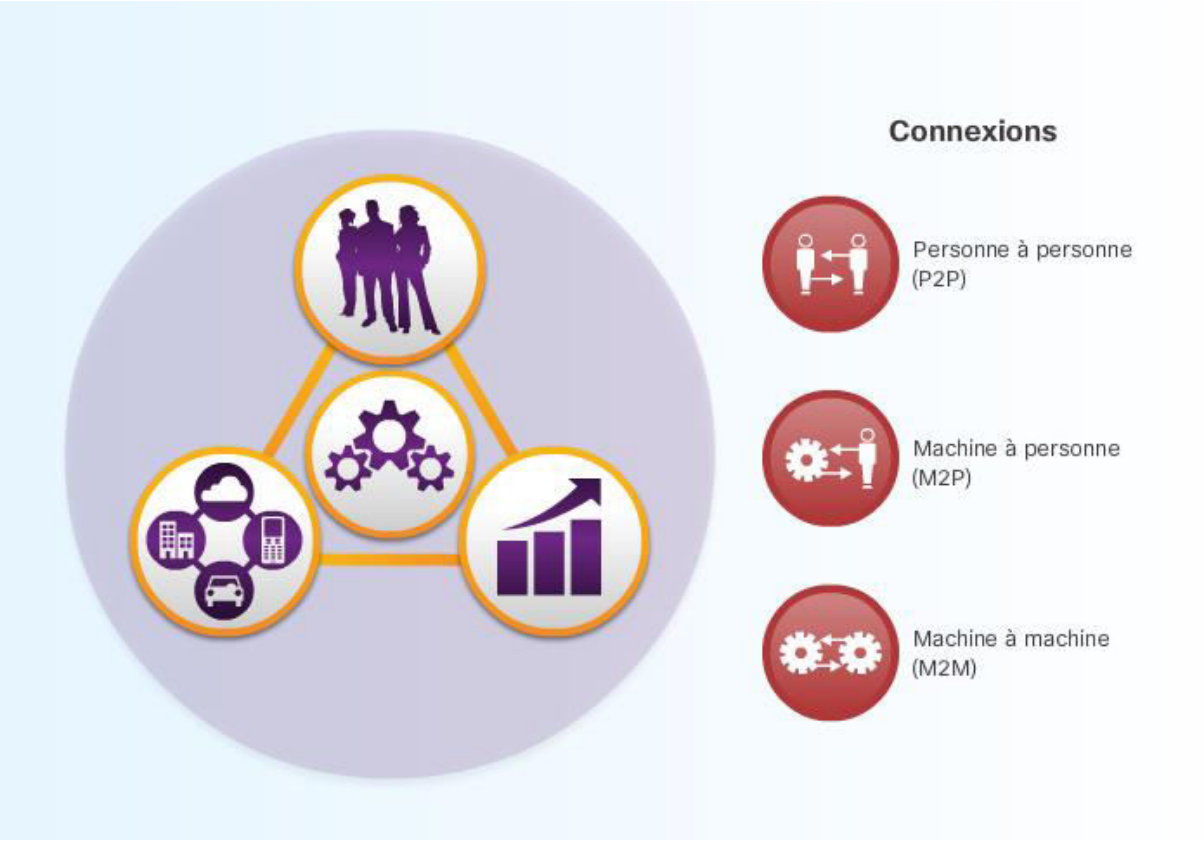

Figure 2 : interaction dans l'IoE.

a) Connexions M2M :

Les connexions de machine à machine (M2M) se produisent lorsque des données sont transférées d'une machine (ou « objet ») à une autre sur un réseau. Les machines incluent des capteurs, des robots, des ordinateurs et des périphériques mobiles.

b) Connexions M2P :

Les connexions de machine à personne (M2P) se produisent lorsque des informations sont transférées entre une machine et une personne. Lorsqu'une personne accède à des

informations situées dans une base de données ou qu'elle effectue une analyse complexe, il s'agit d'une connexion M2P.

c) Connexions P2P :

Des connexions de personne à personne (P2P) se produisent lorsque des informations sont transférées d'une personne à une autre. De plus en plus, les connexions P2P ont lieu par l'intermédiaire de la vidéo, des périphériques mobiles et des réseaux sociaux. Les connexions P2P sont souvent appelées « collaboration ».

II.3 Les éléments de l'IoE:

a) Capteurs :

Les capteurs constituent un moyen de collecter des données à partir d'appareils autres que des ordinateurs. Ils convertissent les aspects physiques de notre environnement en signaux électriques susceptibles d'être traités par des ordinateurs. Des capteurs en tous genres joueront un rôle important dans la connexion à l'IoE des appareils qui étaient traditionnellement non connectés. Le capteur le plus populaire utilise l'identification par radiofréquence (RFID). La technologie RFID utilise des champs électromagnétiques de radiofréquence pour échanger des informations entre de petites étiquettes codées (étiquettes RFID) et un lecteur RFID.

Les modèles représentés dans la figure II.3 possèdent une plage de transmission de quelques mètres.

Grâce à leur flexibilité et à leur faible consommation d'énergie, les étiquettes RFID constituent un moyen idéal pour connecter un périphérique autre qu'un ordinateur à une solution IoE en fournissant des informations au lecteur RFID.

Figure II.3 : un capteur RFID.

Les capteurs sont généralement livrés avec des instructions spécifiques préprogrammées ; toutefois, certains capteurs peuvent être configurés de manière à modifier leur degré de sensibilité ou leur fréquence de rétroaction. Le paramètre de sensibilité du capteur est une mesure de la variation du résultat de celui-ci lorsque la quantité mesurée varie.

a.1) Capteurs compatibles IP :

Certains capteurs et actionneurs prennent en charge TCP/IP, ce qui permet de se passer de contrôleur.

Les capteurs et les actionneurs peuvent être connectés directement au Cloud, par l'intermédiaire d'une passerelle, ou elle exécute la fonction de routage nécessaire pour permettre aux périphériques compatibles IP de se connecter à Internet. Les données générées par ces périphériques peuvent être transportées vers un serveur régional ou mondial en vue d'être analysées et traitées ultérieurement.

b) Actionneurs :

Un actionneur est un autre périphérique implémenté au sein de l'IoE. C'est un simple moteur qui peut être utilisé pour déplacer ou commander un mécanisme ou un système, sur la base d'un ensemble spécifique d'instructions, il aussi capables d'effectuer une fonction physique, quel que soit le mode selon lequel l'actionneur provoque le mouvement à réaliser, sa fonction de base est de recevoir un signal, puis d'exécuter une action prédéfinie en fonction de ce signal. Les actionneurs ne sont généralement pas capables de traiter des données. En revanche, le résultat de l'action exécutée par l'actionneur se base sur le signal reçu. L'action effectuée par l'actionneur est généralement provoquée par un signal issu du contrôleur

L'IoE utilise trois types d'actionneurs :

Actionneurs hydrauliques :

Ils utilisent la pression d'un fluide pour provoquer un mouvement mécanique.

Actionneurs pneumatiques :

Ils utilisent de l'air comprimé à haute pression pour exécuter une opération mécanique.

Actionneurs électriques :

Ils sont alimentés par un moteur qui convertit l'énergie électrique en énergie mécanique.

c) Contrôleur :

Les capteurs peuvent être programmés pour prendre des mesures, convertir les données obtenues en signaux, puis envoyer ces données à un périphérique principal appelé contrôleur. Le rôle du contrôleur est de collecter les données en provenance des capteurs et de fournir une connexion Internet. Les contrôleurs peuvent parfois prendre des décisions immédiates ou envoyer les données à un ordinateur plus puissant à des fins d'analyse. Cet ordinateur peut se trouver dans le même réseau local que le contrôleur ou n'être accessible que par l'intermédiaire d'une connexion Internet.

Pour atteindre Internet, puis les ordinateurs plus puissants situés dans le data center, le contrôleur commence par envoyer les données à un routeur local. Ce routeur joue le rôle d'interface entre le réseau local et Internet, et peut transmettre des données entre les deux.

c.1) Contrôleurs compatibles IP :

Le contrôleur transfère les informations sur un réseau IP, les individus étant autorisés à accéder au contrôleur à distance. En plus de transférer des informations de base dans une configuration M2M, certains contrôleurs sont également capables de réaliser des opérations plus complexes.ils peuvent ainsi rassembler les informations issues de plusieurs capteurs ou effectuer une analyse de base des données reçues.

d) Définition du fog

Les capteurs collectent les informations relatives aux aspects physiques. Ces informations sont transmises au contrôleur. Le contrôleur transmet une image plus complète de ces informations à un serveur réseau ou sur Internet à un service basé sur le Cloud. Les informations collectées par les nœuds des capteurs et par le contrôleur peuvent ensuite être analysées, tandis que des périphériques mobiles et distants peuvent y accéder.

Le contrôleur collecte les informations en provenance des capteurs en utilisant le protocole ZigBee 802.15. Le contrôleur rassemble les informations reçues, puis transfère les données à la passerelle au moyen de la suite de protocoles TCP/IP.

d.1) Contrôleurs dans le Fog :

Les capteurs collectent des données et les transfèrent aux contrôleurs. Le contrôleur peut transmettre toute information collectée à partir des capteurs vers les autres périphériques situés dans le fog

Le traitement des données dans le Fog se produit dans des environnements réseau moins traditionnels. De nouveaux emplacements de mise en réseau sont créés au fur et à mesure que des objets issus de diverses industries se connectent au réseau. Les réseaux locaux contiennent des équipements renforcés, disposés dans des environnements rudes ou exposés aux intempéries.

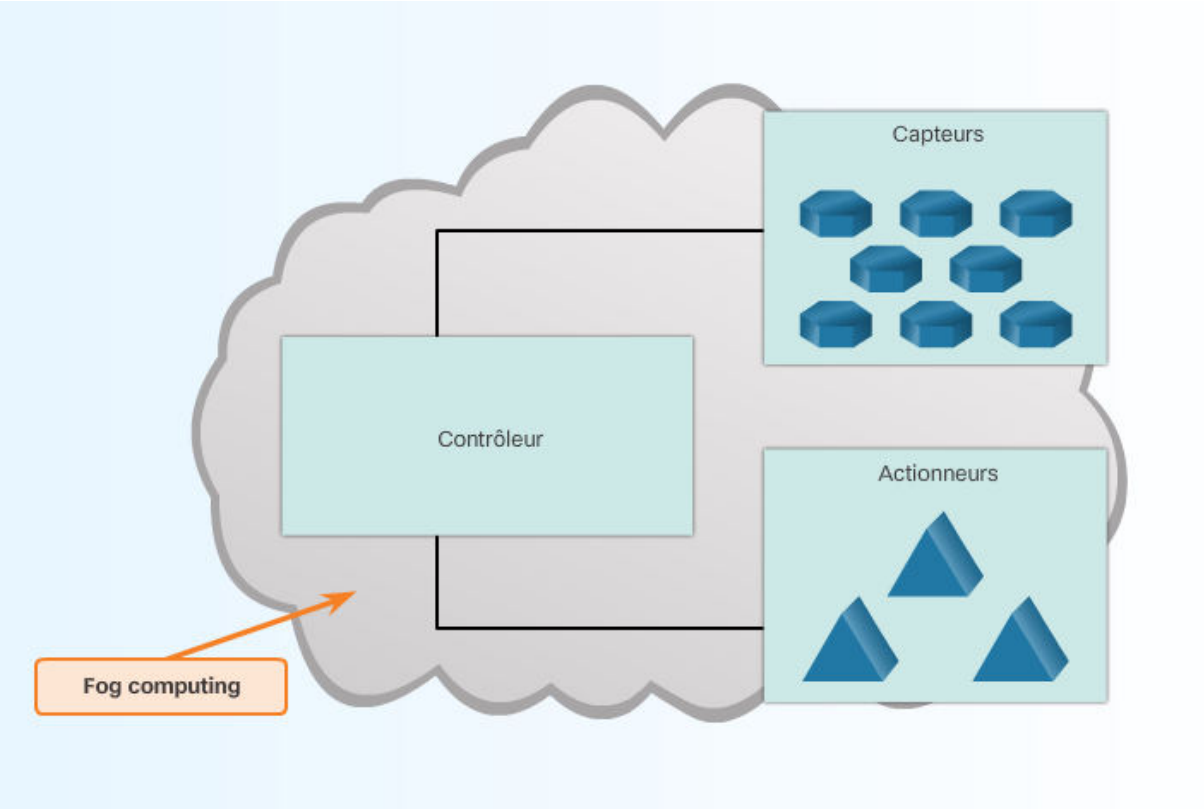

Figure 6: Fog computing

e) Data Centers:

Les data centers constituent un élément critique du Cloud computing. Un data center est une installation qui fournit les services nécessaires à l'hébergement des plus grands environnements informatiques qui existent à l'heure actuelle. Sa fonction principale est de permettre la continuité des activités en assurant la disponibilité des services informatiques.

Plusieurs facteurs doivent être pris en compte lors du déploiement d'un data center en vue de fournir le niveau de service nécessaire :

- **Emplacement :** les data centers doivent être situés dans des endroits présentant un faible risque de catastrophes naturelles et suffisamment éloignés des zones à trafic intense de personnes (aéroports, centres commerciaux, etc.) ainsi que des zones revêtant une importance stratégique pour les gouvernements et les services publics (raffineries, barrages, centrales nucléaires, etc.).

- **Sécurité :** un data center doit présenter des contrôles stricts en matière d'accès physique et de personnel sur site.

- **Électricité :** un accès suffisant doit être prévu en matière d'alimentation électrique, avec une alimentation de secours composée de systèmes d'alimentation sans coupure, de groupes de batteries et de générateurs électriques.

- **Environnement :** il faut prévoir un environnement physique étroitement contrôlé capable de maintenir une température et une humidité appropriées. Des systèmes sophistiqués d'extinction d'incendie doivent également être présents.

- **Réseau :** l'infrastructure réseau doit être évolutive et fiable, avec une connectivité redondante.

Il existe à l'heure actuelle plus de 3.000 data centers dans le monde, offrant des services d'hébergement généraux (IaaS) aux particuliers et aux organisations. Il existe toutefois encore bien plus de data centers détenus et exploités par des entreprises privées, et ce, pour leur usage personnel.

f) Cloud computing :

Le Cloud computing est un autre moyen de gérer et de stocker des données, ainsi que d'y accéder.

Il implique un grand nombre d'ordinateurs reliés entre eux par l'intermédiaire d'un réseau. Les fournisseurs de Cloud computing utilisent énormément la technologie de la vertualisation pour assurer leurs services.

L'utilisation du cloud computing peut aussi permettre à des entreprises de se passer d'équipement informatique sur site, de maintenance et de gestion. L'utilisation de la virtualisation dans les environnements de data center permet une évolutivité rapide du cloudcomputing, avec un minimum de gestion et d'efforts.

D’après, le NIST (National Institute of Standards and Technology) il y a quatre types de modèles de déploiement de cloud : (Privé, Public, Communautaire, Hybride)

- **Cloud privé** est créé exclusivement pour une organisation unique. Son infrastructure peut être physiquement située sur le site ou en dehors de celui-ci, et elle peut appartenir à un fournisseur distinct. Un cloud privé n'offre de services qu'aux membres de cette seule organisation.

- **Cloud public** est destiné à être utilisé par le grand public. Son infrastructure est physiquement située sur le site du fournisseur, mais elle peut être détenue par une ou plusieurs organisations, comme des entreprises, des institutions universitaires ou des gouvernements.

- **Cloud communautaire** est créé pour une utilisation exclusive par une communauté spécifique. La communauté se compose de plusieurs organisations partageant les mêmes préoccupations. L'infrastructure peut être physiquement située sur le site ou en dehors de celui-ci, et elle peut appartenir à un fournisseur distinct ou à une ou plusieurs des organisations de la communauté. Les différences entre clouds publics et clouds communautaires se réfèrent aux besoins fonctionnels qui ont été personnalisés pour la communauté.

- **Cloud hybride** est la combinaison au minimum de deux infrastructures de cloud distinctes (cloud privé, communautaire ou public), représentant des entités uniques. Ces entités sont reliées par le biais d'une technologie permettant la portabilité des données, des applications et à une organisation de conserver un point de vue unique en matière de solution de cloud, tout en profitant des avantages offerts par différents fournisseurs de cloud.

g) Comparaison entre le Cloud computing et le fog computing :

Les solutions de Cloud computing créeront des augmentations substantielles des besoins en bande passante, au fur et à mesure que les données et les services seront déplacés et traités dans le Cloud, favorisant ainsi la flexibilité et l'agilité organisationnelles.

Toutefois, certaines solutions de données et de services doivent de préférence être plus près de la source. Le modèle informatique sélectionné doit offrir les niveaux de résilience, d'évolutivité, de vitesse et de mobilité nécessaires à une utilisation efficace des données.

Afin d'obtenir une valeur ajoutée maximale, les concepteurs de systèmes doivent tenir compte de la distribution des données ainsi que de la présence de différents modèles informatiques. Par conséquent, il se peut que certains services et applications doivent être déplacés depuis le Cloud vers le Fog. Cela peut aider à gérer l'augmentation des besoins en bande passante.

II.4) Bande passante requise :

Avec l'augmentation du nombre d'objets connectés à Internet, la demande de bande passante ne fera que s'accroître en raison des communications M2M dans les applications industrielles, administratives et domestiques.

Il se peut que cinquante capteurs ne consomment pas une grande partie de la bande passante Wi-Fi de votre domicile, tout simplement parce que chaque périphérique transmet de manière intermittente une petite quantité de données. Toutefois, 50 capteurs peuvent être une évaluation très raisonnable du nombre d'objets qui seront connectés dans chaque domicile au cours de la prochaine décennie.

Dans les modèles de services du cloudcomputing, l'activation d'un accès réseau à la demande vers des ressources et des services informatiques partagés sur le réseau augmente les exigences relatives à la bande passante du réseau. À son tour, cette augmentation des exigences de bande passante exige des améliorations de l'infrastructure.

II.5. Définition du big data

Le big data ou méga données désignent l'ensemble des données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles. Cela recoupe les données d'entreprise aussi bien que des données issues de capteurs, des contenus publiés sur le web, des transactions de commerce électronique, des échanges sur les réseaux sociaux, des données transmises par les objets connectés (étiquettes électroniques, compteurs intelligents, smartphones...), des données géo localisées, etc.

a) Gestion du Big Data :

Parmi les facteurs contribuant à cette augmentation de la quantité d'informations, on peut citer le nombre de périphériques connectés à Internet ainsi que le nombre de connexions entre ces périphériques. Mais nous n'en sommes qu'au début. Chaque jour, de nouveaux périphériques sont connectés à Internet, créant ainsi une abondance de nouveaux contenus.

Avec cette quantité d'informations, les organisations doivent apprendre à gérer les données et également à gérer le « Big Data ».

Il y a trois caractéristiques principales du Big Data dont il faut tenir compte, à savoir le volume, la variété et la vitesse.

Le volume concerne la quantité de données transportées et stockées. La variété décrit le type de données dont il s'agit. La vitesse décrit le débit auquel les données se déplacent. Les données ne peuvent pas se déplacer sans la présence d'une infrastructure. La rapidité de l'infrastructure (entrée/sortie, bande passante et latence) ainsi que la possibilité d'activer rapidement des ressources optimales (réseau, processeur, mémoire et stockage) influencent directement la vitesse des données.

b) Analyse du Big Data :

Les applications du Big Data reçoivent des informations à partir d'un large éventail de sources de données, y compris des PC, des smartphones, des tablettes, des machines, des capteurs, des médias sociaux et des applications multimédias. La plus grande partie de cette croissance des données est due à l'utilisation de périphériques mobiles. La mobilité permet d'utiliser n'importe quel périphérique et n'importe quel contenu, à n'importe quel moment et n'importe où.

Par conséquent, le coût et la complexité de ces modèles ont augmenté, incitant à des changements dans la manière dont le Big Data est stocké, analysé et accédé. Les organisations doivent ainsi adapter leurs modèles de données actuels en fonction du Big Data. Elles utilisent par conséquent de plus en plus la virtualisation et le cloudcomputing pour prendre en charge leurs besoins en matière de Big Data.

c) Défis du Big Data :

Avec l'augmentation du nombre d'objets connectés à Internet, la croissance exponentielle des données se poursuit. Toutefois, le fait de disposer d'une plus grande quantité de données n'est pas forcément un avantage si ces données ne sont pas accessibles et si elles ne peuvent pas être analysées et utilisées de manière pratique. Pour que ces données constituent une ressource réelle, elles doivent pouvoir être utilisées efficacement. De plus, l'utilisation de données obsolètes et imprécises représente une perte de temps, de ressources et d'argent.

La gestion de cette quantité croissante de données est à l'origine de nombreux défis, par exemple :

- Capacité en bande passante sur les liaisons existantes connectées aux data centers.

- Confidentialité des données des utilisateurs.

- Gestion des données pour les communications en temps réel.

- Sélection et analyse des données appropriées.

Les éclairages apportés par le Big Data permettront de favoriser l'engagement des clients, d'améliorer les opérations et d'identifier de nouvelles sources de valeur ajoutée. Cependant, les exigences croissantes du Big Data requièrent de nouvelles technologies et de nouveaux processus pour les data centers et l'analyse des données.

II.6) Virtualisation :

Historiquement, chaque ordinateur disposait de son propre système d'exploitation, de ses propres applications et de ses propres composants matériels dédiés. À l'heure actuelle, à l'aide de la simulation logicielle, plusieurs ordinateurs virtuels peuvent s'exécuter sur un même ordinateur physique. Cela signifie que chaque ordinateur virtuel possède son propre système d'exploitation, ses propres applications et ses propres composants matériels dédiés. En informatique, cette technologie porte le nom de virtualisation.

II.7) Connexion de périphériques :

Pour que l'IoE fonctionne, tous les périphériques faisant partie de la solution IoE recherchée doivent être interconnectés de manière à pouvoir communiquer entre eux. Il y a deux manières de connecter des périphériques, à savoir en utilisant une connexion filaire ou sans fil.

Dans la plupart des cas, l'interconnexion de périphériques à l'aide de câbles est une opération trop coûteuse ou difficile à réaliser en pratique. Pour cette raison, la plupart des périphériques doivent envoyer et recevoir des données en utilisant une technologie sans fil.

Il existe de nombreux types de communication sans fil. Les types les plus courants de communication sans fil sont le Wi-Fi, la technologie cellulaire, le Bluetooth et la communication en champ proche (NFC ou Near Field Communication). Certains périphériques, comme les smartphones et les tablettes, utilisent une combinaison de différentes méthodes de communication sans fil pour se connecter à d'autres périphériques.

a) Rôle des périphériques d'infrastructure IoE :

Les périphériques d'infrastructure sont principalement responsables du déplacement des données entre les périphériques des contrôleurs et autres périphériques finaux.

Les périphériques d'infrastructure fournissent un certain nombre de services

-Connectivité filaire et connectivité sans fil.

-Qualité de la file d'attente des services (les données voix avant les données vidéo).

-Disponibilité élevée.

-Transfert sécurisé.

Les périphériques d'infrastructure connectent les périphériques finaux individuels au réseau et ils peuvent connecter plusieurs réseaux individuels pour former un inter réseau. La gestion des données lors de leur passage à travers le réseau est l'un des rôles principaux des périphériques d'infrastructure ou intermédiaires.ils utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau.

b) Périphériques finaux dans l'IoT :

Les périphériques finaux se connectent à Internet et envoient des données sur le réseau. Les téléphones cellulaires, les ordinateurs portables, les PC, les imprimantes et les téléphones IP sont des exemples de périphériques finaux utilisant le protocole Internet (IP). Il existe aujourd'hui de nouveaux types de protocoles de communication sans fil de faible portée pour les objets dont les besoins en énergie sont extrêmement faibles, afin de leur permettre d'envoyer des informations sur le réseau. Dans certains cas, ces protocoles ne sont pas compatibles IP et doivent transférer des informations à un périphérique compatible IP connecté, comme un contrôleur ou une passerelle. Par exemple, un périphérique qui n'utilise pas TCP/IP peut malgré tout communiquer avec un autre périphérique qui utilise TCP/IP, et ce, à l'aide d'une norme telle que la norme IEEE 802.15 (IEEE étant l'acronyme de Institute of Electrical and Electronics Engineers).

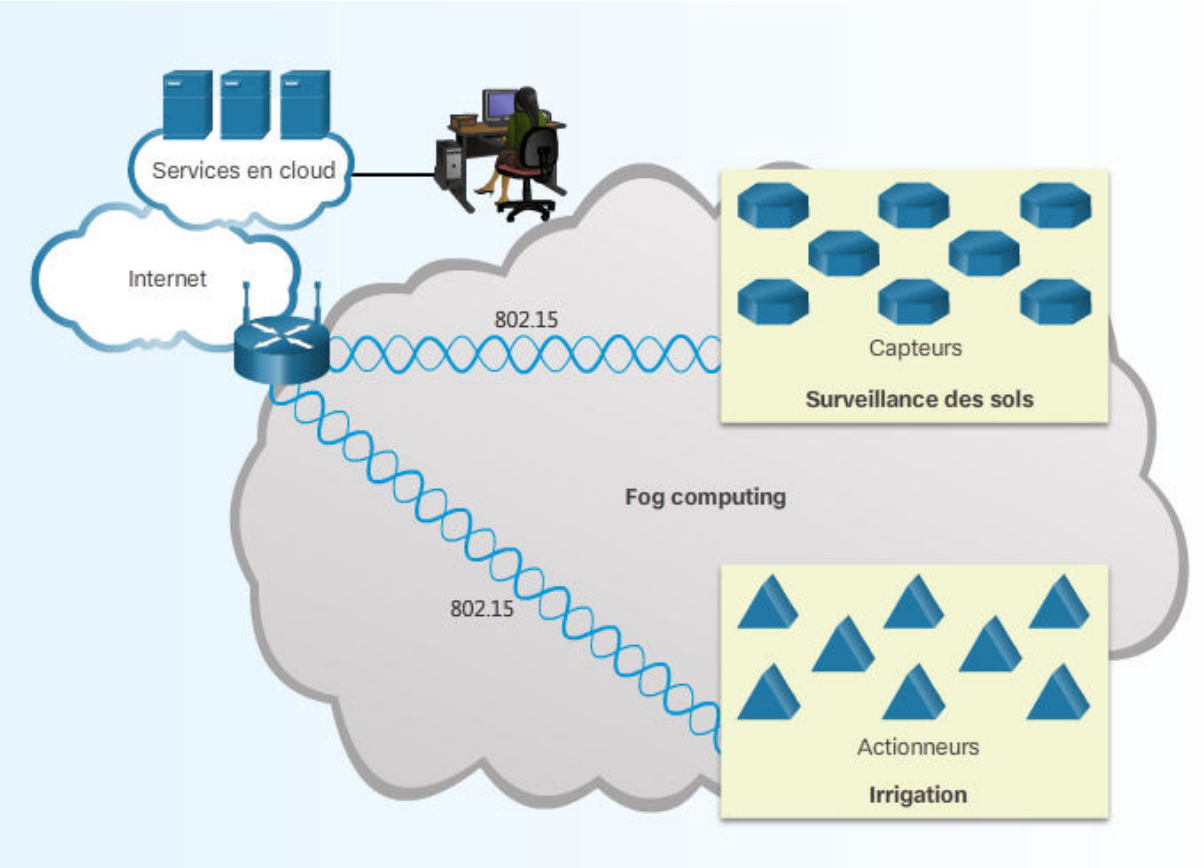

Figure 7 : Accès réseau pour les objets actuellement non connectés.

II.8) La différence entre le IT et OT :

L'IoE s'attache à connecter ce qui ne l'est pas encore, à savoir principalement les « objets » de l'IoE. Connecter ce qui ne l'est pas encore nécessite une certaine convergence entre la technologie opérationnelle (OT) d'une organisation et les systèmes informatiques (IT) dont cette organisation dispose.

L'OT est définie en tant qu'infrastructure industrielle de contrôle et d'automatisation d'une organisation. Elle inclut le matériel (tels que les capteurs et les périphériques finaux) ainsi que les logiciels utilisés pour contrôler et surveiller les équipements et les processus de fabrication. La majeure partie de la communication au sein de l'OT s'effectue entre des machines.

Les systèmes informatiques (IT) se réfèrent à l'infrastructure réseau, aux télécommunications ainsi qu'aux applications logicielles utilisées pour traiter les informations et permettre l'échange de celles-ci entre les êtres humains.

II.9) Convergence entre l'IT et l'OT :

Grâce à la convergence des systèmes IT et OT au sein d'une solution IoE, les organisations peuvent créer de meilleurs produits, diminuer les coûts et les risques, et améliorer leurs performances, leur flexibilité et leur efficacité. Grâce aux solutions IoE, les organisations peuvent mettre en œuvre une approche à la fois simple, intelligente et sécurisée, qui leur permet de :

- **Simplifier l'infrastructure (approche simple)** : la convergence harmonieuse des infrastructures IT et OT permet de diminuer les coûts d'exploitation et d'accroître l'efficacité des processus.
- **Créer de l'intelligence et de l'agilité (approche intelligente)** : l'utilisation d'analyses axées sur les applications permet à ces dernières de s'exécuter avec des performances maximales et d'obtenir des informations à partir de l'infrastructure en vue de nouveaux services.
- **Fournir de la sécurité de bout en bout (approche sécurisée)** : l'infrastructure convergée est capable de se défendre contre les attaques et de répondre aux menaces de manière à la fois intelligente et dynamique.

Pour implémenter des solutions IoE, les organisations doivent examiner et prendre en compte trois types de connexions distincts, à savoir M2M, M2P et P2P.

II.10) Approche architecturale de l'IoE :

L'approche architecturale de Cisco en ce qui concerne l'IoE est organisée en trois couches fonctionnelles. La couche application dépend de la couche de la plate-forme, qui dépend à son tour de la couche de l'infrastructure.

Cette approche architecturale reflète les modèles de services du modèle de Cloud computing, qui tire parti du logiciel en tant que service, de la plate-forme en tant que service et de l'infrastructure en tant que service.

a) Couche application :

Cette couche assure des réponses automatisées, dynamiques, axées sur les applications aux fluctuations du trafic et de l'utilisation. Elle intègre les fonctionnalités intelligentes nécessaires

pour améliorer l'expérience utilisateur. Elle permet d'intégrer les applications IT traditionnelles et d'utiliser des applications de collaboration et des applications spécialisées.

b) Couche plate-forme :

Cela fait référence aux solutions Cisco qui assurent l'orchestration, la gestion et l'adaptation des règles en fonction de l'évolution des besoins afin d'accélérer la fourniture des services. Cette couche permet aux applications et aux utilisateurs de recevoir les ressources dont ils ont besoin, au moment où ils en ont besoin, sans nécessiter de changements de configuration ni de tâches informatiques manuelles ou compliquées. Elle apporte la flexibilité dont a besoin l'entreprise en mettant en place de nouveaux services et de nouvelles applications analytiques capables de relever les défis du bigdata.

c) Couche infrastructure :

Cette couche intègre la puissance, la sécurité, les réseaux principaux, les architectures d'accès et le stockage avec les ressources matérielles et virtuelles. Elle comprend la bonne combinaison de matériels et de logiciels partout dans l'entreprise, le cloud et les réseaux des fournisseurs de services. Elle fait converger toutes les connexions, OT et IT, dans une structure IP et sait gérer le Cloud computing et la connectivité mobile.

II.11) Stratégie de sécurité :

Plus la solution IoE est grande et intégrée, plus le réseau est décentralisé. Cela permet la présence d'un plus grand nombre de points d'accès dans le réseau, d'où un plus grand nombre de vulnérabilités. Un nombre important d'appareils communiquant par le biais de l'IoE transmettront des données à partir d'emplacements non sécurisés, mais ces communications doivent toutefois être sûres. Cependant, la sécurisation d'une solution IoE peut être difficile à mettre en œuvre en raison du nombre élevé de capteurs, d'objets intelligents et d'appareils connectés au réseau. Les dommages potentiels liés à l'accès au réseau d'une organisation par des appareils non sécurisés constituent un véritable défi pour les professionnels de la sécurité.

a) Sécurité adaptable et en temps réel :

Il faudra gérer la sécurité au fur et à mesure de la croissance en déployant une sécurité adaptable et en temps réel. Les entreprises doivent suivre le rythme de leur évolution et adapter les niveaux de sécurité pour minimiser les risques.

b) Connexions sécurisées et dynamique :

S'assurez que le niveau de sécurité adéquat est en place pour toutes les connexions et en permanence. Les mesures de sécurité avancées et les protocoles permettent d'assurer le respect des règles et de la confidentialité. Tous les éléments importants, tels que la propriété intellectuelle, les données, les employés et les bâtiments sont protégés.

c) Protection des clients et confiance dans la marque :

Réduire l'impact et le coût des failles de sécurité avec une stratégie de sécurité transparente. Les failles de sécurité nuisent à la confiance des clients et à l'intégrité de la marque. La stratégie de sécurité doit détecter, confirmer et atténuer les menaces, et y remédier, dans toute l'entreprise.

d) Approche globale :

À l'heure actuelle, la sécurité des réseaux est en grande partie due à des efforts d'anticipation des menaces. Tout comme les médecins tentent de prévenir de nouvelles maladies en traitant les problèmes existants, les professionnels de la sécurité réseau essaient d'empêcher de futures attaques en minimisant les effets des attaques réussies.

La sécurité doit être persuasive au sein de l'IoE. L'approche de sécurité doit être :

- Cohérente, automatisée et s'étendre jusqu'aux frontières sécurisées des organisations.
- Dynamique, afin de mieux identifier les menaces de sécurité par le biais d'analyses prédictives en temps réel.
- Intelligente, offrant de la visibilité sur l'ensemble des connexions et des éléments de l'infrastructure.
- Évolutive, afin de répondre aux besoins d'une organisation en pleine croissance.
- Agile et capable de réagir en temps réel.

- Solution totale de bout en bout.

Une solution de sécurité globale permet d'éviter les implémentations de sécurité incohérentes pouvant être une source de complexité, être difficiles à gérer et nécessiter du personnel et des connaissances techniques supplémentaires pour pouvoir être prise en charge.

e) Architecture de sécurité :

La sécurisation des réseaux IoE ne peut pas se limiter à celle des périphériques individuels. En revanche, il s'agit de mettre en œuvre une solution de sécurité de bout en bout.

Une solution de sécurité offrant de la protection avec une gestion centralisée des stratégies et une mise en œuvre distribuée doit être intégrée au réseau. Une surveillance continue de l'activité du réseau est nécessaire pour collecter et corréler des données dans l'environnement connecté, exploiter les informations et entreprendre les actions requises.

Les architectures de sécurité de Cisco utilisent les couches infrastructure, plate-forme et application afin de fournir un ensemble complet d'outils et de systèmes. Ces outils et systèmes fonctionnent de manière conjointe en vue de produire une intelligence de sécurité exploitable, pratiquement en temps réel, tout en permettant au réseau de s'adapter aux menaces de sécurité avec peu ou pas d'intervention humaine nécessaire.

e.1) Contrôle d'accès :

Le contrôle d'accès assure l'accès en fonction des politiques pour tous les utilisateurs ou appareils cherchant à se connecter au réseau distribué. Les utilisateurs sont authentifiés et autorisés. Les périphériques finaux sont également analysés afin de déterminer s'ils sont conformes à la politique de sécurité. Les équipements qui ne sont pas authentifiés, par exemple les imprimantes, les caméras vidéo, les capteurs et les contrôleurs, sont automatiquement identifiés.

Les politiques sensibles au contexte utilisent un langage métier descriptif simplifié pour définir les politiques de sécurité en fonction du contexte d'une situation dans son ensemble : qui envoie quoi, quand, où et comment. Ces politiques sont harmonisées au mieux avec les politiques de l'entreprise et sont plus simples à administrer dans toute l'entreprise. Elles permettent de mettre en place une sécurité plus efficace et de la faire respecter plus aisément.

e.2) Inspection selon le contexte et l'application :

L'inspection selon le contexte et l'application de la sécurité utilisent l'intelligence réseau et les informations globales pour prendre des décisions sécuritaires à l'échelle du réseau. Des options de déploiement flexibles, telles que les services de sécurité intégrés, des applications autonomes ou des services de sécurité dans le cloud assurent la protection plus près de l'utilisateur.

e.3) L'intelligence réseau et les informations globales :

Les données globales sont corrélées pour permettre au réseau de reconnaître les environnements réputés pour leurs activités malveillantes. Cela fournit des informations détaillées sur l'activité réseau et les menaces pour assurer une protection rapide et précise, ainsi que la mise en application des politiques**.**

e.4) Dispositifs de sécurité :

Parmi les périphériques de l'architecture de sécurité pouvant être utilisés pour contrôler l'accès, examiner le contenu et appliquer des stratégies, on peut citer les éléments suivants :

1. Pare-feu :

Un pare-feu crée une barrière entre deux réseaux. Le pare-feu analyse le trafic réseau afin de déterminer si ce trafic peut être autorisé à transiter entre les deux réseaux, en fonction d'un ensemble de règles préprogrammées.

2. Systèmes de prévention des intrusions (IPS) :

Un IPS surveille les activités se produisant sur un réseau et détermine si elles sont malveillantes ou non. Un IPS tente d'empêcher les attaques en éliminant le trafic en provenance du périphérique malveillant ou en réinitialisant la connexion.

3. Sécurité axée sur les applications :

Lorsque des organisations migrent vers des environnements axés sur les applications, les solutions de sécurité traditionnelles ne sont plus adéquates. Les solutions de sécurité de Cisco ACI protègent les environnements en intégrant totalement des technologies de sécurité personnalisées pour les besoins d'une application spécifique. Les solutions de sécurité de

Cisco ACI peuvent être gérées comme un pool de ressources attaché aux applications et aux transactions par l'intermédiaire d'un contrôleur central. Cette solution peut évoluer automatiquement en fonction de la demande, fournissant ainsi une sécurité harmonieuse basée sur la stratégie.

Cette solution permet une approche holistique et basée sur la stratégie de la sécurité, permettant de diminuer les coûts et la complexité. Elle intègre des technologies de sécurité physiques et virtuelles, directement dans les infrastructures de Cloud et de data center.

4. Sécurité sans fil :

La difficulté de préserver la sécurité d'un réseau filaire est amplifiée avec un réseau sans fil. Un réseau sans fil n'est ouvert à toute personne qui se trouve à portée d'un point d'accès et qui dispose des identifiants appropriés pour s'y associer.

La sécurité sans fil est souvent implémentée au niveau du point d'accès, c'est-à-dire à l'endroit où la connexion sans fil pénètre à l'intérieur du réseau. Une sécurité sans fil de base inclut les éléments suivants :

- Configuration de protocoles d'authentification utilisant des mots de passe forts
- Configuration de la sécurité administrative
- Activation du chiffrement
- Modification de l'ensemble des paramètres par défaut
- Mise à jour du micro logiciel

Toutefois, même avec ces paramètres de configuration, un pirate informatique peut accéder au réseau d'une organisation ou d'une personne, à condition de disposer d'un périphérique sans fil et de connaître les techniques de piratage. De plus, de nombreux nouveaux périphériques sans fil qui se connectent à l'IoE ne prennent pas en charge la fonctionnalité de sécurité sans fil. Pour cette raison, le trafic en provenance des périphériques sans fil et mobiles intelligents, ainsi que le trafic issu des détecteurs et des objets embarqués, doivent traverser les dispositifs de sécurité et les applications sensibles au contexte sur le réseau.

5. Redondance et haute disponibilité :

Avec un aussi grand nombre de connexions au réseau, il est important de s'assurer que ce dernier est disponible et fiable.

La redondance nécessite l'installation d'éléments d'infrastructure réseau, de liaisons de télécommunication et d'autres composants d'alimentation supplémentaires visant à assurer la sauvegarde des ressources principales en cas de défaillance. La redondance permet également le partage de la charge des ressources, fournissant ainsi un système à haute disponibilité qui garantit qu'un niveau préalablement défini de performances opérationnelles sera atteint au cours d'une période contractuelle de mesure.

En plus de disposer d'équipements et de connexions redondants, il est également nécessaire de sauvegarder les données. Les sauvegardes sécurisées permettent d'archiver les données sous un format chiffré, évitant ainsi tout accès non autorisé aux archives stockées.

6. Le maillon faible de L'IOE :

Certaines personnes sont malveillantes, tandis que d'autres commettent des erreurs ou utilisent des pratiques non sécurisées, mettant ainsi l'équipement et les données en danger. Afin de protéger les ressources, des règles et des réglementations doivent être mises en place en vue de définir la manière dont les utilisateurs doivent agir, quelles actions sont adaptées ou erronées, ce que les personnes sont autorisées à faire, et comment elles peuvent accéder aux systèmes et aux données.

a) Politique d'accès a distance :

Définit qui peut se connecter, de quelle manière, quand et quels appareils peuvent être utilisés pour se connecter à distance à un système. Cette politique détermine également à quelles ressources peut accéder un utilisateur distant.

b) Politique de confidentialités des informations :

Définit les méthodes utilisées pour protéger les informations selon le niveau de sensibilité. En général, plus les informations sont sensibles, plus le niveau de protection est élevé.

c) Politique de sécurité informatique :

Définit la manière dont les utilisateurs peuvent utiliser les ordinateurs. Cette politique peut stipuler qui peut utiliser certains ordinateurs et les programmes à utiliser pour protéger un ordinateur, ou indiquer si un type de support de stockage particulier est autorisé.

d) Politique de sécurité physique :

Définit comment les équipements matériels sont sécurisés. Certains peuvent nécessiter un verrouillage pendant la nuit ou l'installation permanente dans une zone fermée à clé. D'autres peuvent être spécifiquement conçus pour ne pas quitter le bâtiment.

e) Politique d'accès par mots de passe :

Définit le mot de passe, et son degré de complexité, à utiliser pour accéder à certaines ressources. Souvent, cette politique vérifie la fréquence à laquelle un mot de passe doit être modifié.

II.12) Données personnelles et IoE :

Les organisations ont la possibilité de collecter toutes sortes de données personnelles ; toutefois, il existe un équilibre juridique et éthique entre l'accès et la confidentialité. Les blocs de données peuvent être améliorés grâce à la présence de métadonnées incluant des informations sur l'emplacement de création de ces données, l'identité de la personne qui les a créées ainsi que la destination de celles-ci. De cette manière, les données deviennent un bien de propriété pouvant être échangé. Cette modification permettra aux informations personnelles d'être auditées afin de permettre l'application de stratégies et de réglementations en cas de problèmes.

La définition de ce que l'on entend par données personnelles évolue cependant. Ainsi, ce qui peut être considéré comme étant des données personnelles pour une personne ne le sera pas forcément pour une autre. Il se peut par exemple qu'une personne atteinte d'un cancer et une autre en bonne santé aient des idées très différentes quant à la nature des informations médicales qu'elles souhaitent maintenir privées.

II.13) Modélisation d'une solution d'IoE :

a) La modélisation :

La modélisation de la solution potentielle permet de visualiser les modifications apportées aux processus de l'organisation. Le modèle peut être partagé par l'ensemble des parties intéressées afin de s'assurer de la compréhension du mode de fonctionnement et d'interaction des nouvelles solutions.

Un modèle peut être une représentation d'un système. Les modèles aident les individus et les organisations à mieux comprendre les processus qui sont implémentés et à identifier les problèmes. Les modèles permettent de réaliser des scénarios de simulation qui révèlent les avantages et les obstacles à l'implémentation d'une nouvelle solution. Lorsqu'une organisation entame la réingénierie d'un processus, elle a avantage à utiliser un modèle avant d'exécuter un plan quelconque.

Même si la modélisation n'est pas toujours une tâche aisée, les avantages d'une modélisation correcte compensent les coûts d'une modélisation simpliste ou trop rapide pour la plupart des organisations.

b) Outils d'analyse :

D'énormes quantités de données sont créées au sein de l'IoE. Pour appliquer ces données aux processus, il est nécessaire d'utiliser des logiciels d'analyse. Les logiciels d'analyse vont de simples tableurs utilisés pour calculer des statistiques relatives à une plage de données à des suites logicielles professionnelles complexes. Ce type de logiciel peut avoir été créé et commercialisé par une grande entreprise, développé de manière indépendante et distribué sous la forme d'un programme open source, ou conçu par l'entreprise elle-même pour ses propres besoins.

Par le passé, les analyses étaient principalement une méthode de prévision de la demande, basée sur le nombre d'unités vendues au cours d'une période donnée. Les analyses effectuées au sein de l'IoE se sont développées et concernent maintenant de nombreux nouveaux aspects de la vie professionnelle. Certains des types d'analyses suivants sont utilisés pour aider à définir le mode de fonctionnement d'une entreprise :

- Analyse descriptive : utilise des données historiques pour créer des rapports conçus pour faciliter la compréhension des phénomènes.

- Analyse prédictive : utilise l'exploration de données (data mining) ainsi que les techniques de modélisation pour tenter de déterminer ce qui va se produire à l'avenir.
- Analyse prescriptive : utilise la simulation, les règles commerciales et l'apprentissage des machines pour recommander l'exécution d'une action et indiquer quel pourrait être le résultat de celle-ci.

II.14) Le prototypage :

a) Définition du prototypage :

Le prototypage est l'étape suivante dans le processus de modélisation. En ce qui concerne le prototypage d'idées pour l'IoE, il est utile de posséder des connaissances en conception, en électricité, en physique et en mécanique (travaux manuels pour l'assemblage des objets), en programmation ainsi que sur le mode de fonctionnement des protocoles TCP/IP. Toutefois, vous n'avez pas besoin d'être un expert dans ces domaines. En fait, le prototypage vous aide à améliorer ces compétences.

L'IoE étant toujours en cours de développement, il y a encore des tâches inconnues à découvrir. L'IoE impliquant à la fois les individus, les processus, les données et les objets, il n'y a pas de limite aux inventions que l'IoE peut aider à créer puis à mettre en œuvre. Toute fois il est :

- Totalement fonctionnel, mais pas à l'abri d'une défaillance
- Véritable version opérationnelle du produit.
- Utile pour l'évaluation des performances et les améliorations futures du produit.
- Finition complète (intérieure et extérieure).
- Coût de production éventuellement élevé

Conclusion :

Nous avons donc articulé notre travail autour de la problématique « les objets connectés, une réelle source de progrès ».

Dans ce chapitre nous avons mis en évidence la manière de connectés des objets, les principaux acteurs de l'internet des objets les différents éléments dont l'IoE a besoin, les risques que cours cette dernière en matière de sécurité et aussi les éventuelles solutions qui pourront être apportés.

Cependant, il ne faut pas oublier que l'objectif est de minimiser le temps que l'humain va passer devant l'interface homme-machine. Pour cela il existe de nombreuses technologies telles que des algorithmes permettant de déclencher des automatismes pour que l'être humains n'est à intervenir qu'une seul fois juste pour programmer et configuré les systèmes pour qu'il fonctionne correctement tels est le cas dans la deuxième simulation qu'en verra dans le 3ème chapitre.

Introduction :

S'il n'y a pas de technologie avancée sans avancées technologiques, ces dernières sont le lien entre le réel et l'irréel. Nous vivons en effet actuellement dans une époque d'expansion totale au niveau scientifique et technique. Tout ce qui paraissait impossible il y a un siècle parait aujourd'hui évident, voire banal. A travers le XIXème et le XXème siècle, les inventions se sont succédé : téléphone, télévision, ordinateur, GPS, internet, téléphone portable… Ces innovations ont permis de faciliter la vie, cependant en c'est penché sur deux simulation la première va ce porté sur la domotique, Mais Les objets connectés ne sont pas seulement liés à la domotique. Ces outils peuvent être utilisés dans le domaine de la médecine et, plus largement, dans le domaine de la santé. Nous pouvons appeler cela des « objets connectés portatifs ». L'avantage de tels objets réside en leur petitesse et leur capacité à s'adapter au corps humain.

Le fonctionnement de ces outils est globalement le même, bien que le niveau de sophistication varie. Il y a en général deux parties :

- **Le capteur médical :** c'est la partie qui va, comme son nom l'indique, capter des données et des informations médicales, puis les transmettre.

- **L'appareil connecté :** c'est la partie qui va recevoir l'information transmise, puis l'analyser ou l'envoyer à une base de données plus importante.

L'utilisation de packet tracer va nous permettre de simuler ces objets connectée qu'en a par manque de certains éléments en a pas pu la mettre en pratique donc en va ce limiter a une simulation qui va expliqué le fonctionnements de ce dernier

III.1 Définition de packet tracer :

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc...

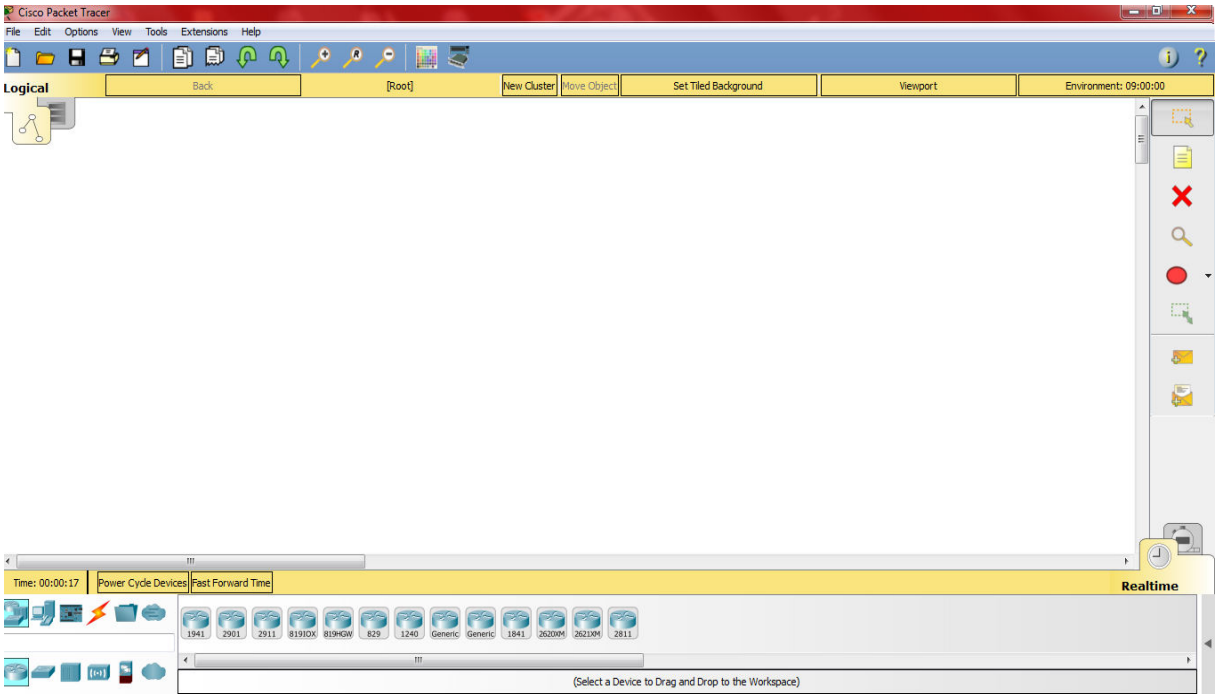

Figure III.1 : fenetre packet tracer

- **Construire un réseau :**

Pour construire un réseau, l'utilisateur doit choisir parmi les 10 catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi-utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée.

- **Configuration d'un équipement :**

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web). Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global).

Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton Fast Ethernet en dessous du bouton INTERFACE).

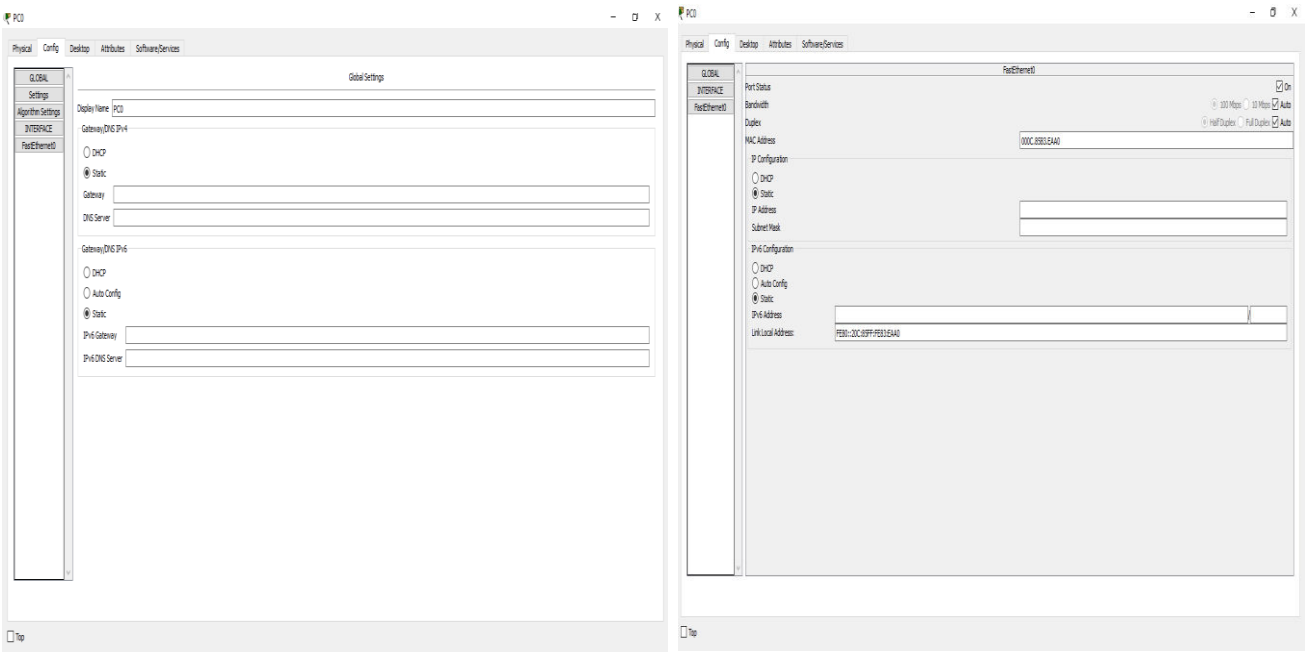

Figure 2 : Configuration d'un équipement.

- **Mode simulation :**

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure 2 montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici HTTP).

- **Invite de commandes :**

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser). L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont

accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

III.2 Installer et configurer les périphériques IoE :

Dans cette activité, vous connecterez les périphériques informatiques et IoE au réseau domestique. Tous les périphériques IoT ont été configurés pour fonctionner avec des commutateurs à bascule connectés à un ordinateur à carte unique (SBC). Les périphériques IoE doivent être connectés à Home Gateway et enregistrés auprès du serveur d'enregistrement (www.register.pka). On a crée déjà un compte avec le serveur d'enregistrement :

Adresse du serveur: ..... www.register.pka

Nom d'utilisateur: ..... admin

Mot de passe: ..... admin

Une fois que les périphériques IoT sont connectés au réseau domestique et enregistrés auprès du serveur d'enregistrement, vous pourrez contrôler les périphériques IoT à la maison ou à l'extérieur du domicile via le serveur d'enregistrement.

Dans notre simulation, nous allons travailler avec la nouvelle version logicielle de packet tracer 7.0.

Le dit logiciel, comporte de nouveaux éléments qui vont nous permettre de traiter notre sujet qu'est internet des objets (les capteurs, les actionneurs…etc.), cette simulation se fera en deux parties :

Partie 1 : Configuration de la maison connectée :

Étape 1 : Configurer le réseau câblé :

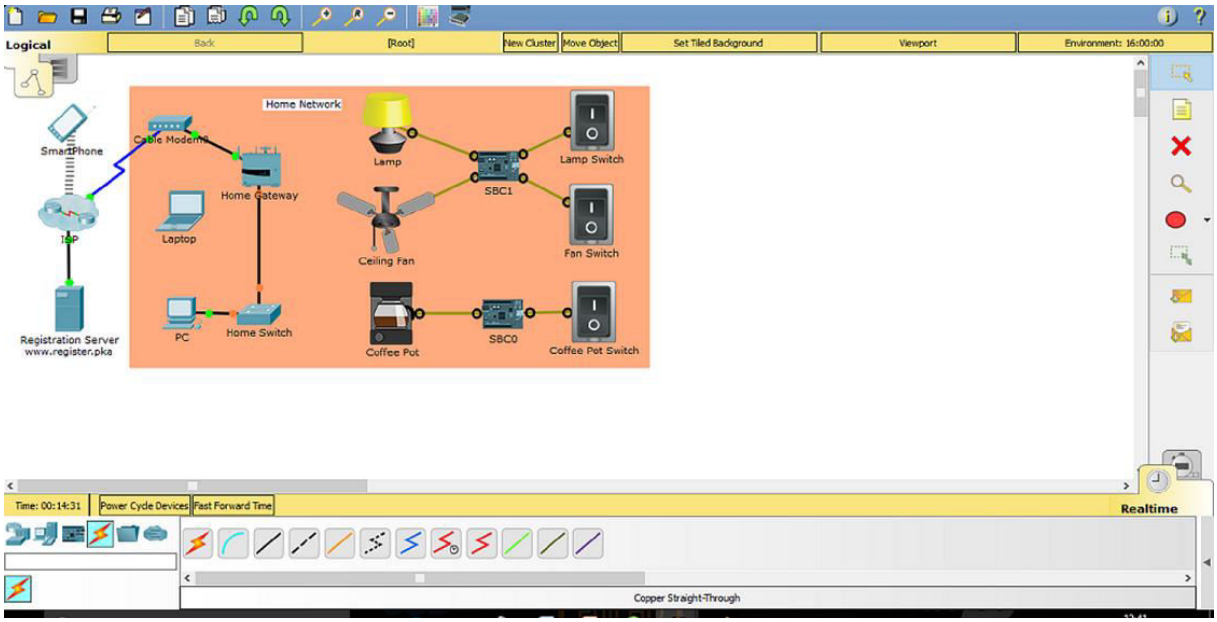

Figure III.3. Configurer le réseau câblé.

- Connecter tous les ports Fast Ethernet disponibles sur le commutateur domestique à n'importe quel port Ethernet disponible sur Home Gateway à l'aide d'un câble direct en cuivre.
- Connecter le port FastEthernet0 sur PC à n'importe quel port FastEthernet disponible sur Home Switch à l'aide d'un câble direct en cuivre.
- Cliquer sur PC, Bureau puis sur IP Configuration. Sélectionner DHCP pour la configuration IP.

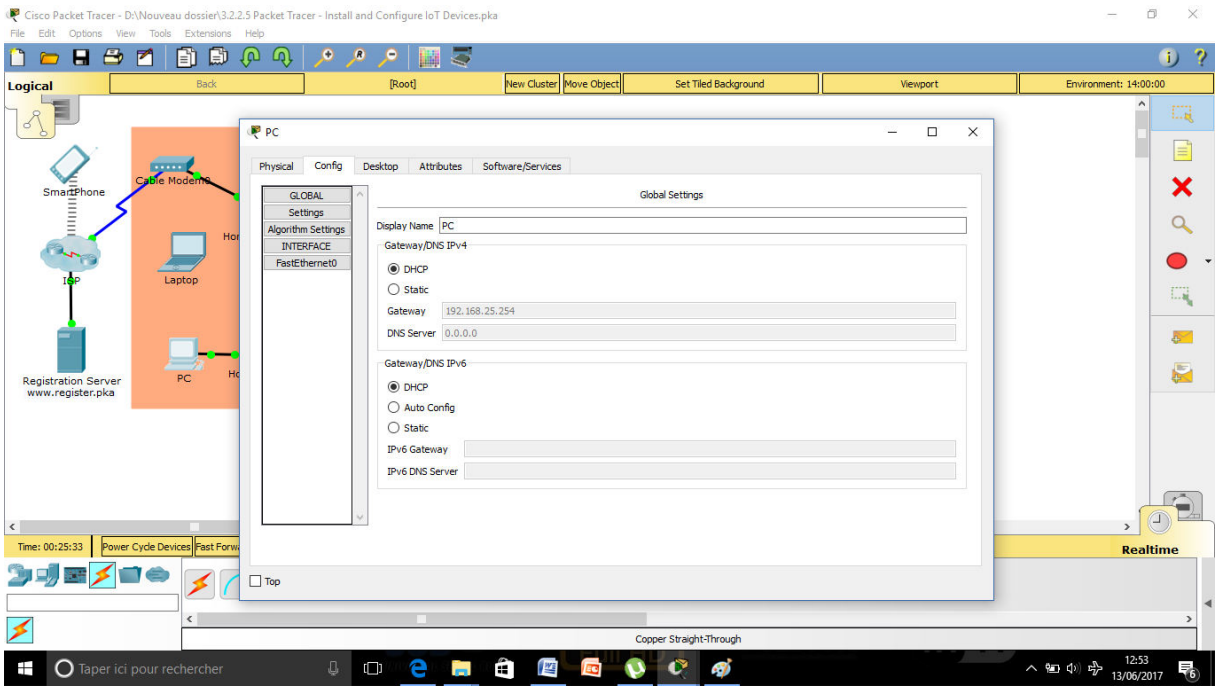

Figure III.4 : configuration DHCP

Étape 2 : Configurer le réseau sans fil

- Cliquer sur Accueil Gateway, onglet Config puis sur Internet dans le panneau de gauche.
- Cliquer sur DHCP dans Paramètres Internet. La passerelle domestique recevra les paramètres du fournisseur de services Internet.

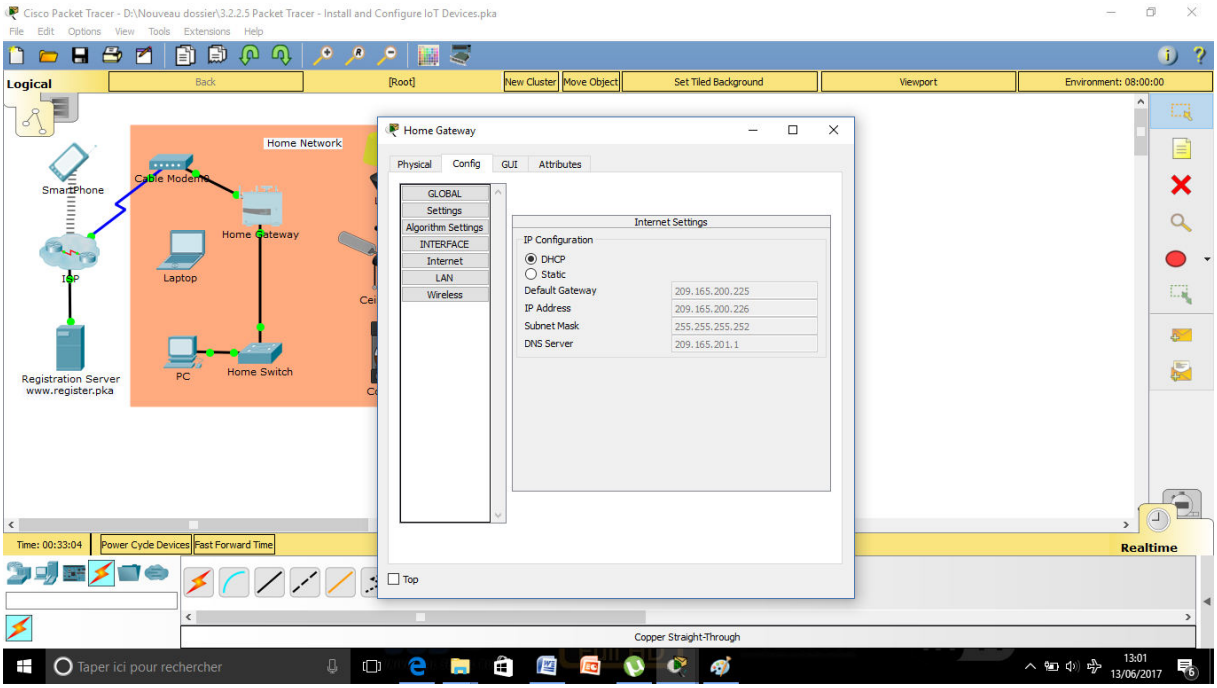

Figure III.5 : Configuration d'un réseau sans fil.

- Dans Home Gateway, cliquer sur Wireless.
- Changer le SSID vers MyHomeGateway. Changer l'authentification en WPA2-PSK. Entrer CiscoIoT en tant que Phrase de passage PSK.

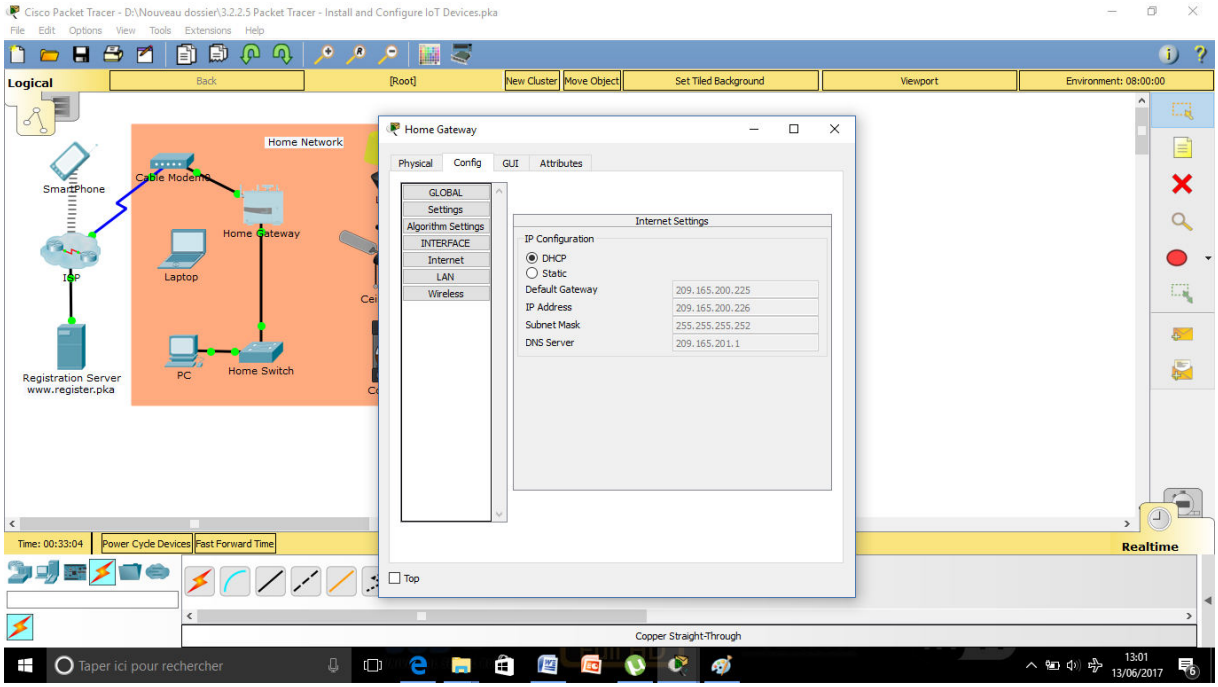

Figure III.6 : Configuration d'un réseau sans fil suite.

- Cliquer sur Ordinateur portable puis sur Bureau. Cliquer sur PC sans fil.
- Cliquer sur l'onglet Connexion. Sélectionner le réseau MyHomeGateway. Si le nom du réseau sans fil n'est pas affiché, cliquer sur Actualiser.

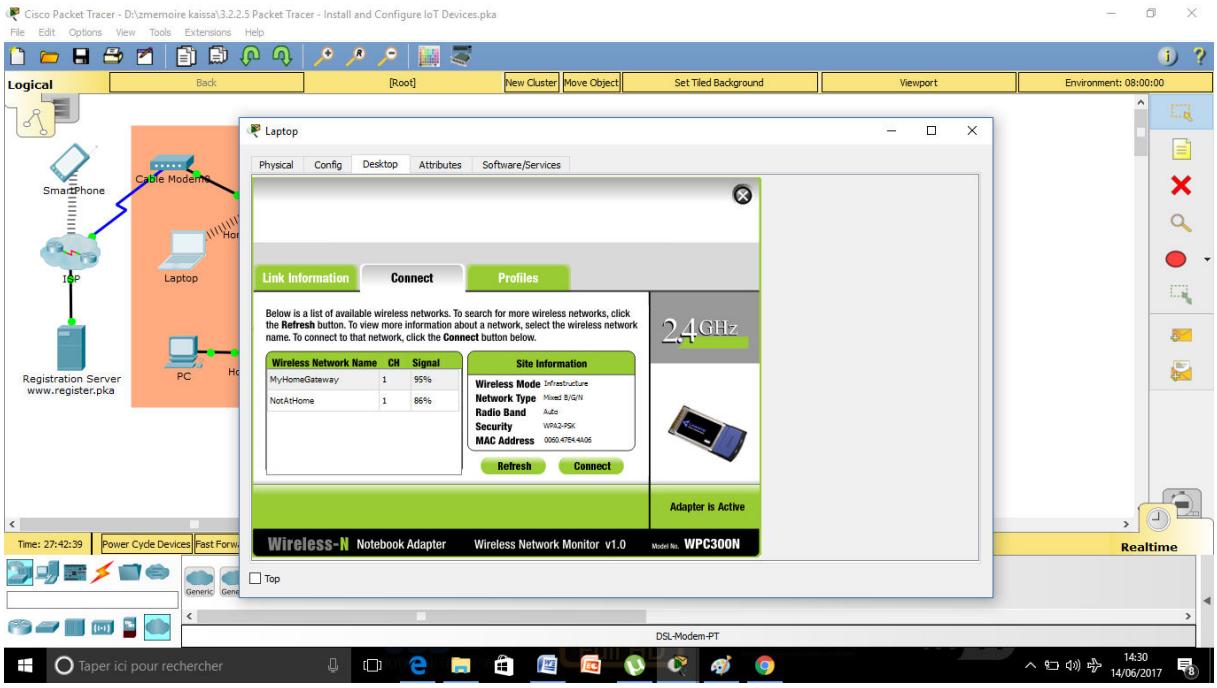

Figure III.7 : Sécuriser la connexion sans fil.

- Cliquer sur Se connecter. EntrerCiscoIoT comme clé pré-partagée. Cliquer sur Se connecter.

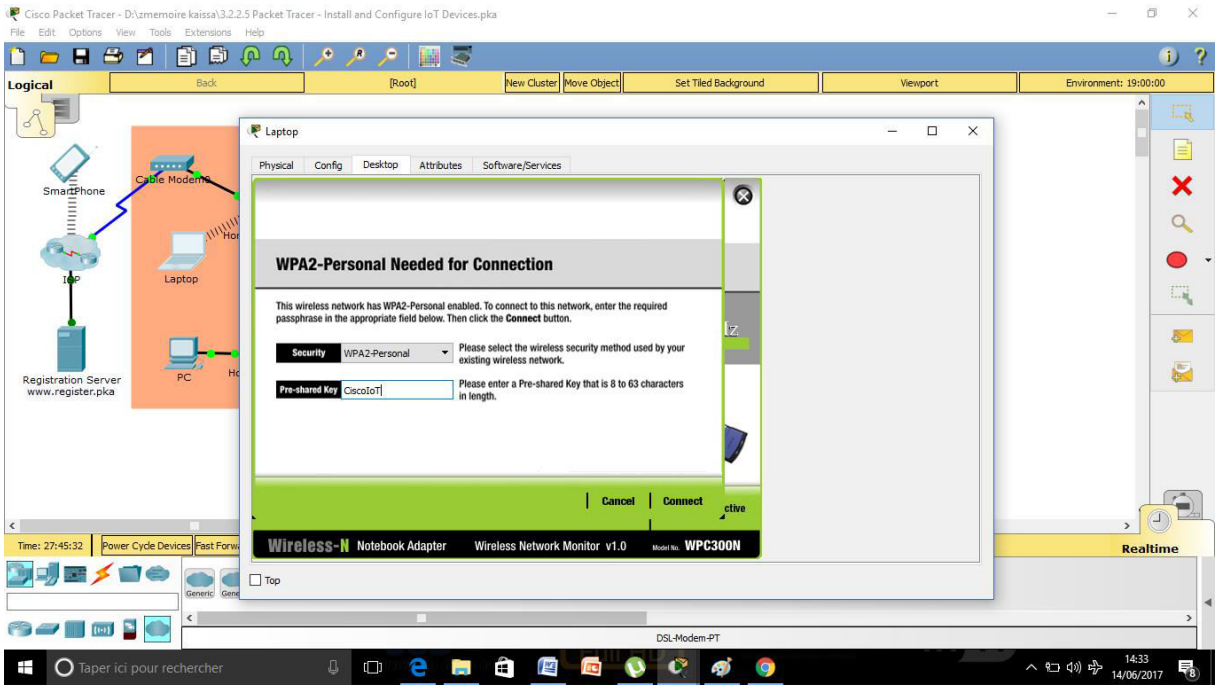

Figure III.8

Étape 3 : connectez les périphériques IoE au réseau :

Les périphériques IoE peuvent être connectés à l'aide de fils ou sans fil. La cafetière sera connectée au réseau à l'aide de câbles Ethernet. La lampe et le ventilateur de plafond seront connectés sans fil.

- Connecter le pot de café à n'importe quel port Fast Ethernet disponible à l'aide d'un câble direct en cuivre.
- Cliquer sur Café Pot, puis sur Config. Cliquer sur FastEthernet0. Sélectionner DHCP pour la configuration IP.

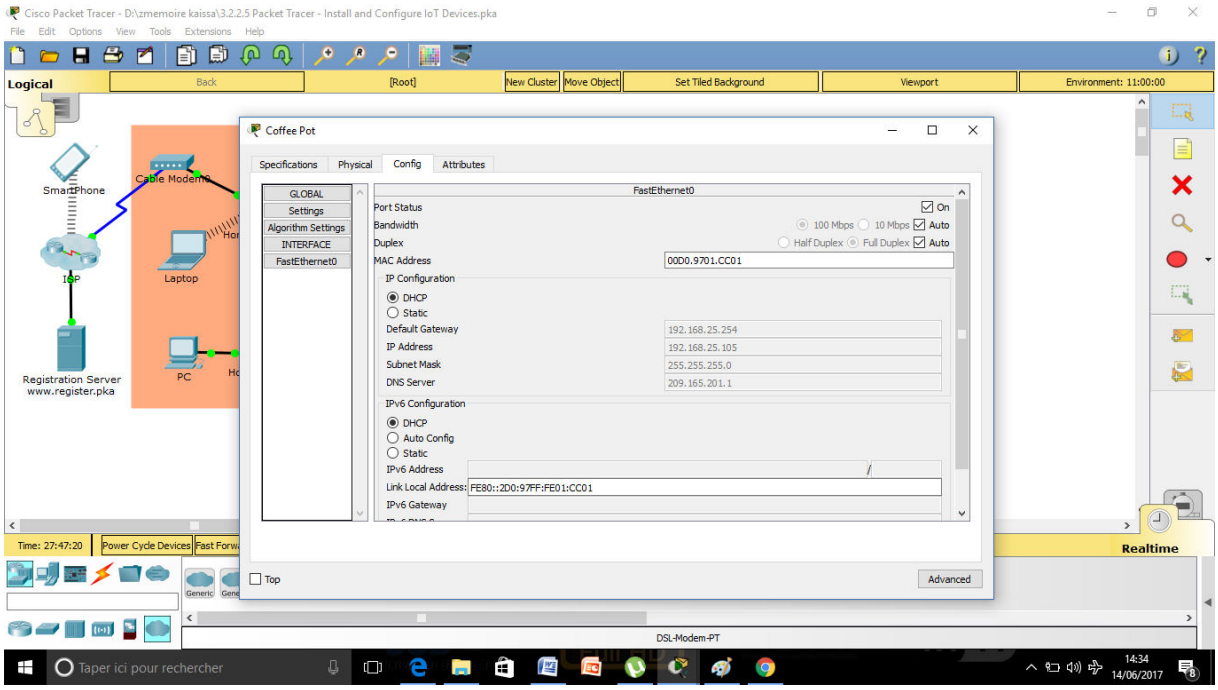

Figure III.9 : Connectes des objets au réseau.

- Cliquer sur Lampe. Cliquer sur Config. Cliquer sur Wireless0. Entrer MyHomeGateway comme SSID. Cliquer sur WPA2-PSK. EntrerCiscoIoT en tant que Phrase de passage PSK. Sélectionner DHCP pour la configuration IP.

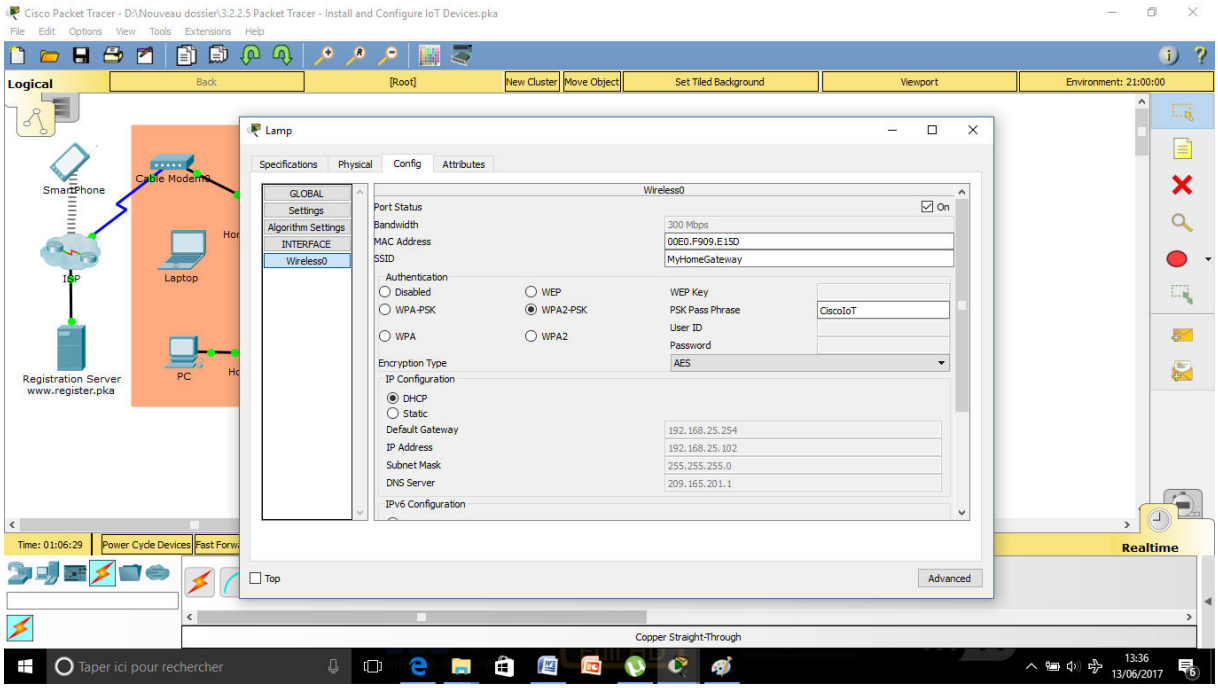

Figure III.10 : Connectes des objets au réseau.

- Répéter l'étape c pour le ventilateur de plafond.

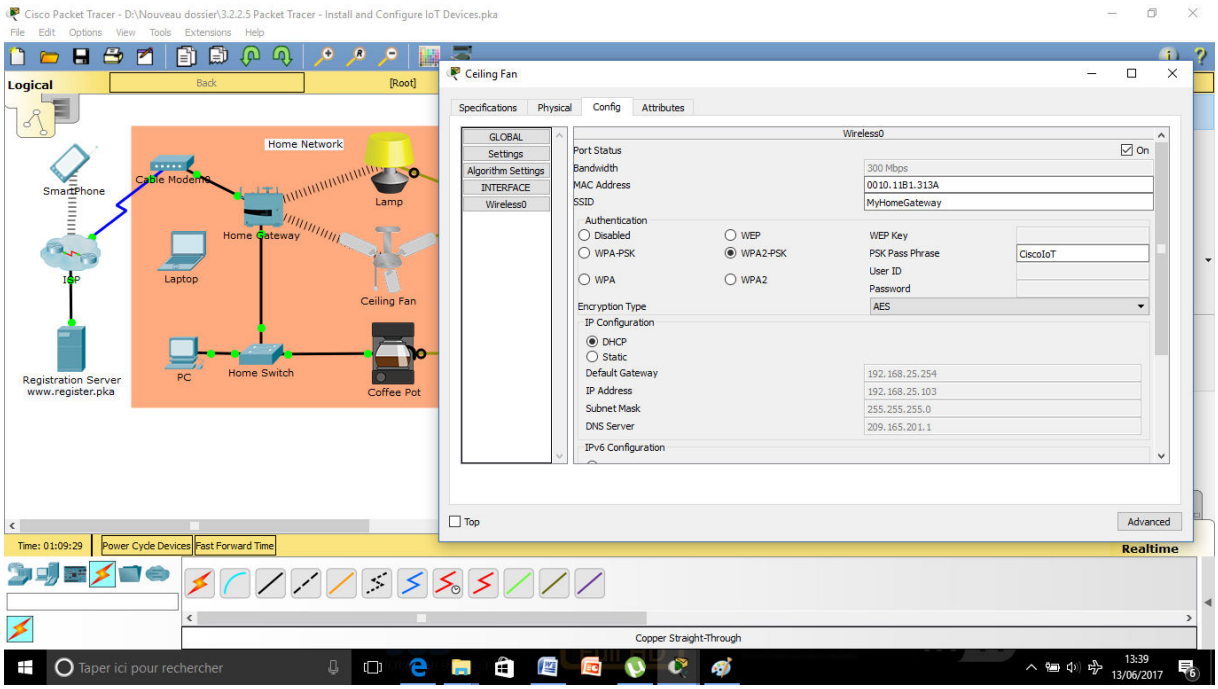

Figure III.11 : Connectes des objets au réseau.

Partie 2 : interagir avec les périphériques IoE :

Les périphériques IoE peuvent être configurés pour être directement contrôlés, avec des commutateurs ou via une interface Web. Dans la partie 2, vous connecterez les périphériques IoE à un serveur d'enregistrement afin que vous puissiez contrôler les périphériques IoE via une interface Web.

Étape 1 : accédez localement aux périphériques IoE :

On peut contrôler les périphériques IoE directement en appuyant sur Alt et en cliquant sur le périphérique en même temps.

- Cliquer sur Alt + Lampe quelques fois. Combien de paramètres a la lampe et quels sont les paramètres ?

  Cliquer sur Alt + Interrupteur de lampe quelques fois. Combien de paramètres le commutateur de lampe a-t-il, et quels sont les paramètres ?

- Répéter avec le ventilateur de plafond et le pot de café.

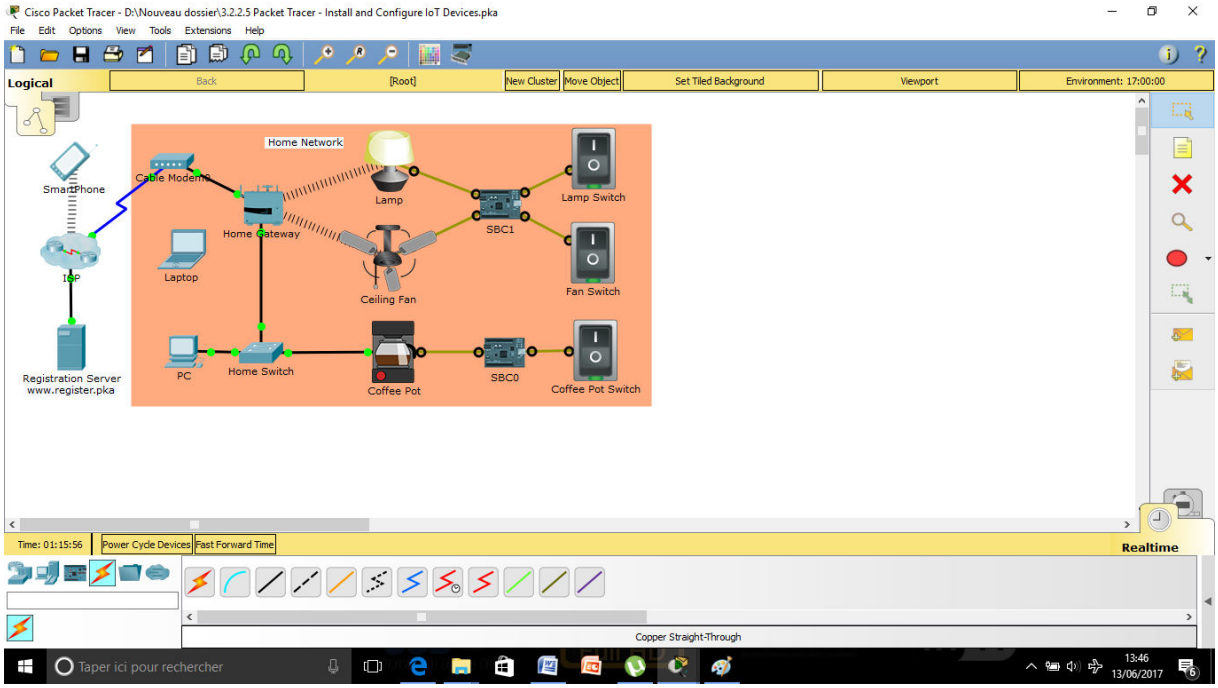

Figure III.12 : Accès local aux périphériques.

Étape 2 : configurez les périphériques IoE pour un accès distant :

Pour contrôler les périphériques IoE à distance via une interface Web, les périphériques doivent être enregistrés auprès d'un serveur d'enregistrement.

- Cliquer sur Lampe. Cliquez sur Config.
- Sous l'en-tête du serveur IoE, cliquer sur Serveur distant. Fournisseur les informations suivantes pour vous connecter au serveur d'enregistrement.

Adresse du serveur: ..... www.register.pka

Nom d'utilisateur: ..... admin

Mot de passe: ..... admin

- Cliquer sur Se connecter pour se connecter au serveur.

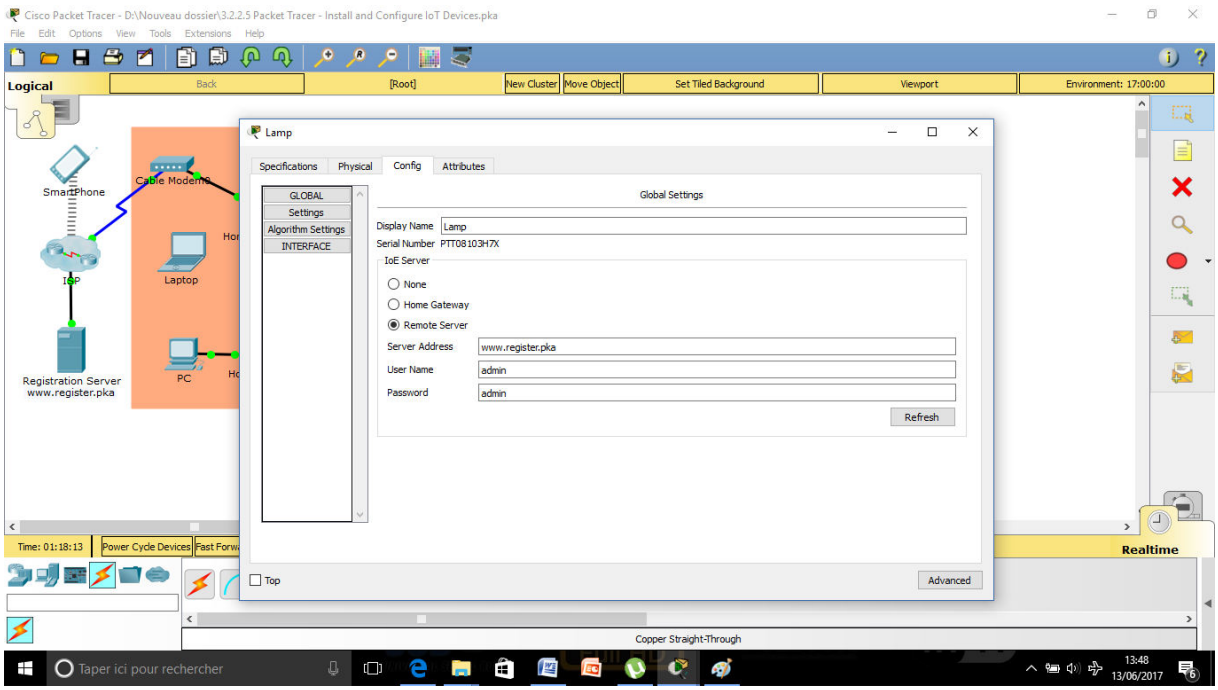

Figure III.13 : La configuration de l'accès a distance aux périphériques.

- Répéter les étapes a-c pour le ventilateur de plafond et le pot de café.

Étape 3 : Accéder à distance aux périphériques IoE :

- Cliquer sur Ordinateur portable. Cliquer sur Bureau.
- Cliquer sur Navigateur Web. Entrez www.register.pka.Entrer l'administrateur en tant que nom d'utilisateur et mot de passe. Cliquer sur Se connecter.

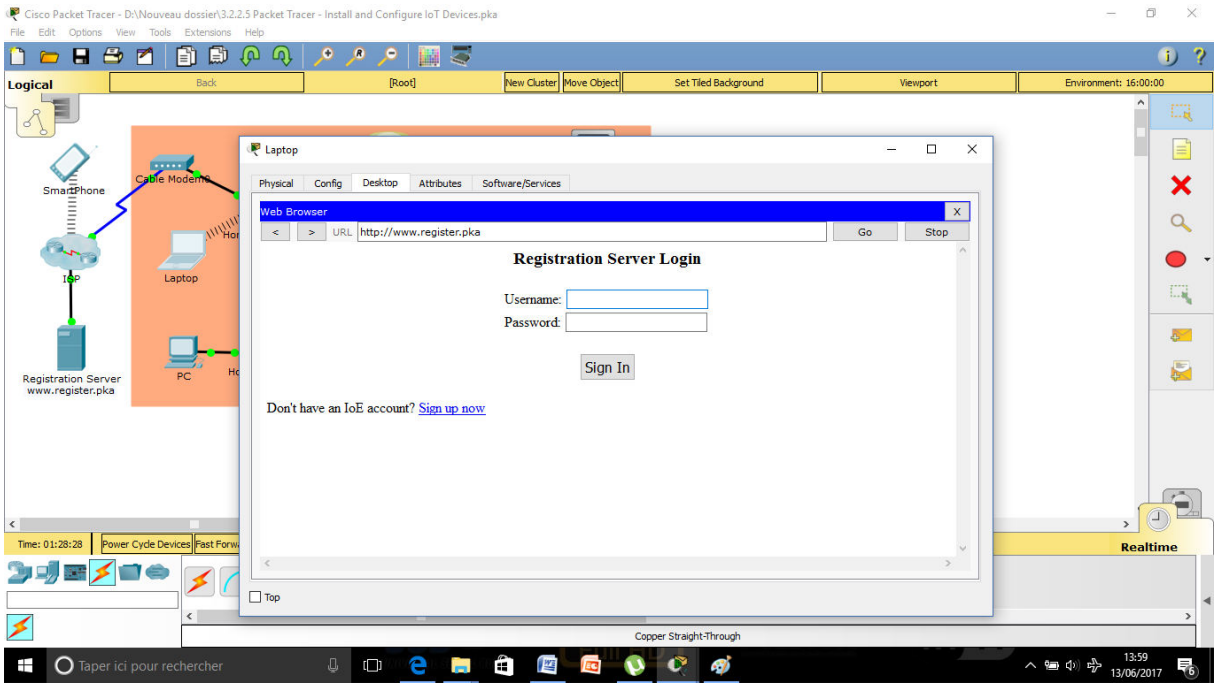

Figure III.14 : Accès a distance aux périphériques.

- Cliquer sur le chevron pour afficher l'état de l'appareil et les contrôleurs.
- Cliquer sur Dim l'intensité de la Lampe dans la topologie diminue
- On peut également contrôler les appareils lorsqu'on est absent de notre domicile en accédant au serveur d'enregistrement. On clique sur SmartPhone, puis sur Bureau. On clique sur Navigateur Web. On fait entrer www.register.pka. Entrez l'administrateur en tant que nom d'utilisateur et mot de passe. Enfin on clique sur Se connecter.

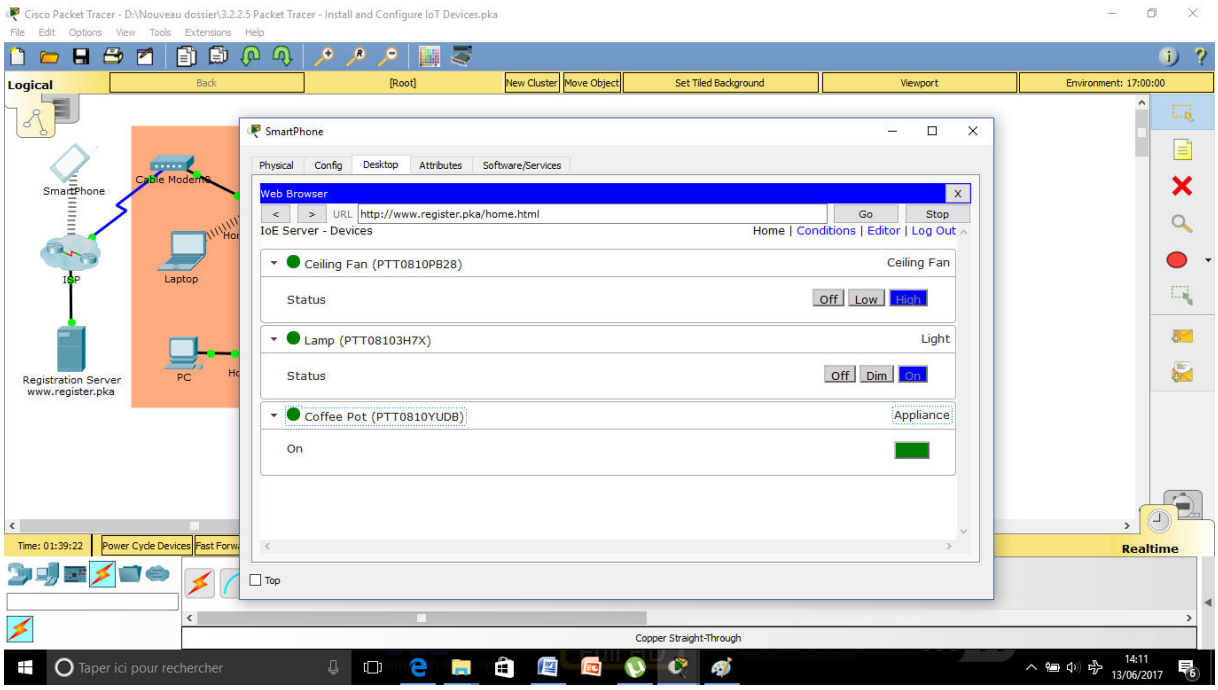

Figure III.15 : Contrôle des appareils a distance via une page web.

Partie 2 : Assistance médicale à temps réel d'un patient diabétique :

John est un diabétique de type 1 qui vit seul. il a du mal à garder son glucose dans une gamme saine. On a décidé de mettre en place une solution IoE pour surveiller en permanence les indicateurs importants de son état et envoyer de l'aide si nécessaire. John va porter une montre intelligente pour surveiller son niveau de respiration et d'exercice. Il utilisera également un moniteur continu de glycémie (CGM) qui signalera ses niveaux de glucose. Les données de ces appareils seront envoyées à sa Société de surveillance de la santé (HMC), qui enverra une assistance médicale si son état devient dangereux pour ça vie.

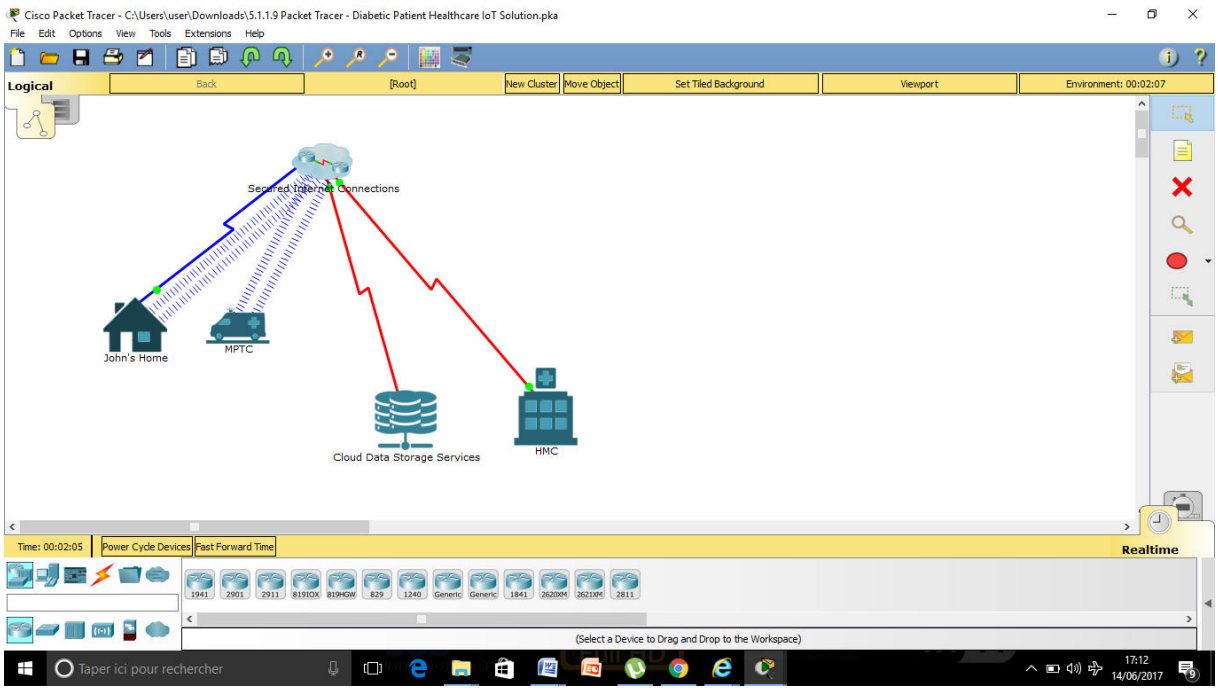

Figure III.15 : Configurer la maison de John.

Partie 1 : Configurer les périphériques pour la connectivité :

En va configurerez le routeur de John on utilisant DHCP pour attribuer des adresses IP à ses périphériques compatibles IP dans sa maison.

- Cliquer sur John's Home.
- Cliquer sur le routeur de la passerelle d'accueil.
- Cliquer sur l'onglet GUI.
- Sous l'en-tête Network Setup, assigner 192.168.0.1 à l'adresse IP du routeur. Choisir 255.255.255.0 pour le masque de sous-réseau.
- Cliquer sur Activé à côté du serveur DHCP pour démarrer le serveur DHCP.
- Cliquer sur Enregistrer les paramètres pour enregistrer les modifications.

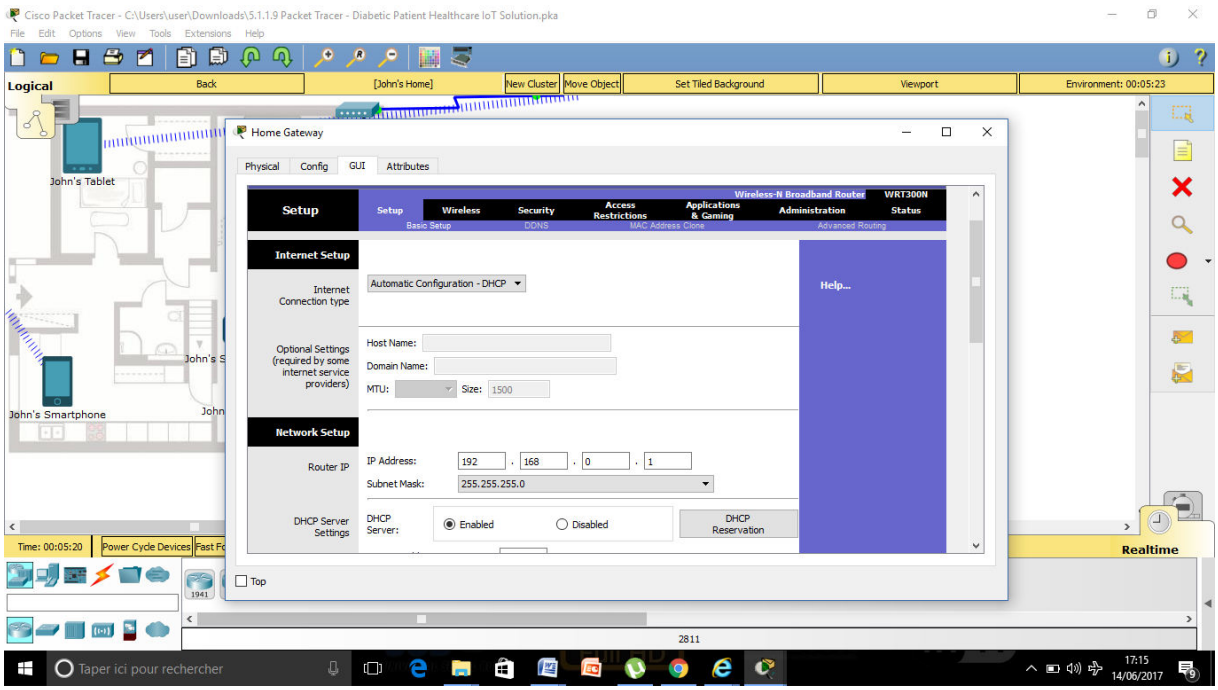

Figure III.17 : Configuration d'un périphérique pour sa connectivite.

Partie 2 : Explorez tous les appareils IoE :

Étape 1 : Regardez les signes vitaux de John sur une tablette MPTC.

Le personnel médical du Centre mobile de traitement des patients (MPTC) peut surveiller les niveaux de John pendant qu'ils se rendent dans la maison de John. Le personnel médical peut également recevoir un code de déverrouillage pour entrer dans la maison de John s'il ne répond pas.

- Accéder au MPTC.
- Cliquer sur l'onglet Application Web de surveillance de HC pour afficher les signaux vitaux de John.

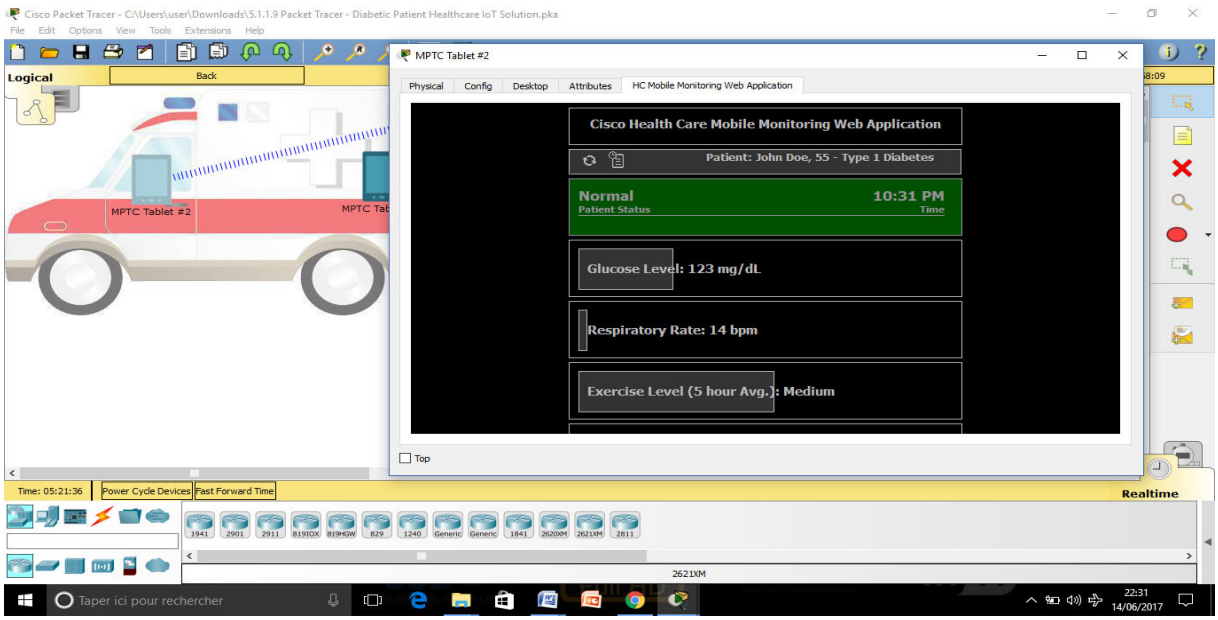

Figure III.18 : L'écran de tablette de l'ambulance.

Étape 2 : Regardez les signes vitaux de John sur sa tablette et sa télévision :

John peut également surveiller ses signes vitaux sur ses appareils, un smartphone, un smartwatch, une tablette et sa télévision.

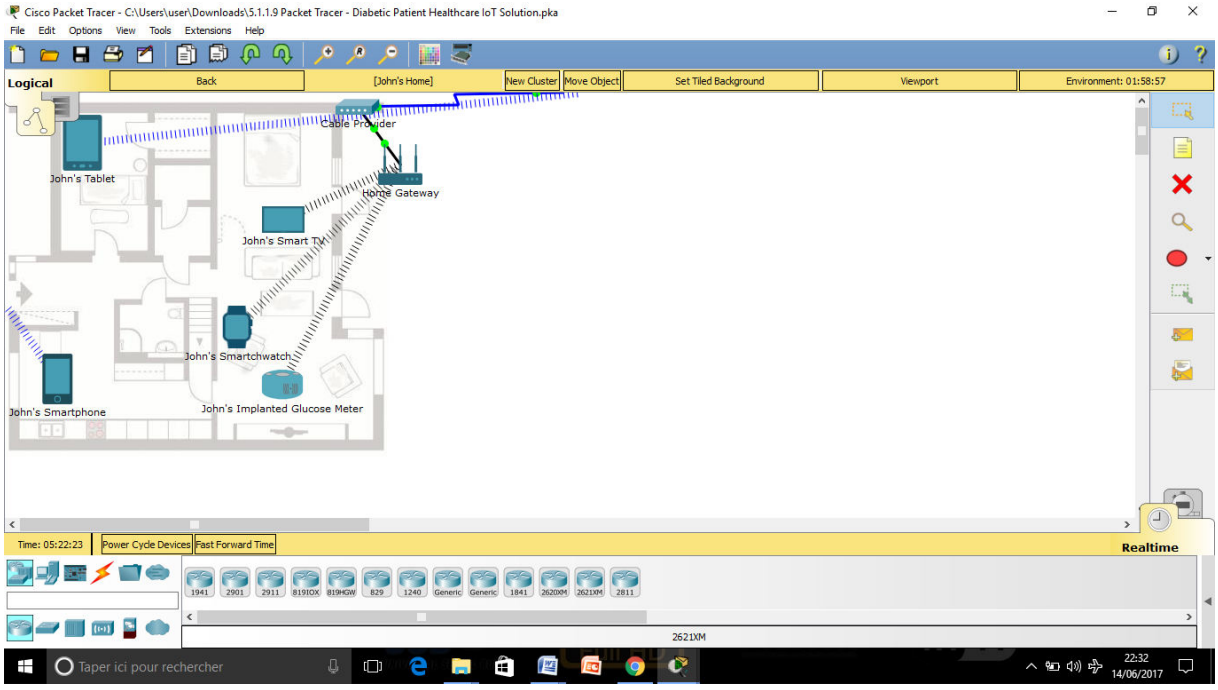

Figure III.19 : Accès sur les donnés de John.

- Accéder à la tablette dans la maison de John.
- Cliquer sur l'onglet Application Web de surveillance de HC pour surveiller ses signaux vitaux.

- Accéder au Smart TV dans la maison de John.
- Cliquer sur l'onglet Application Web de surveillance de HC pour surveiller ses signaux vitaux.

Partie 3 : Créer un événement nécessitant une réponse :

Déclencher un événement qui fera que John exige des soins médicaux.

Étape 1 : Explorer la fenêtre Environnement :

Dans la fenêtre Environnement, vous pouvez influencer le niveau de glucose de John. Lorsque le niveau de glucose de John n'est plus dans sa gamme normale, la HMC enverra des alertes John sur ses appareils connectés pour l'inciter à les appeler afin qu'ils puissent évaluer son état et envoyer de l'aide médicale si nécessaire.

Sur le tableau de bord dans la fenêtre Environnement, vous pouvez induire une hypoglycémie, une hyperglycémie ou restaurer son niveau de glucose à une gamme normale.

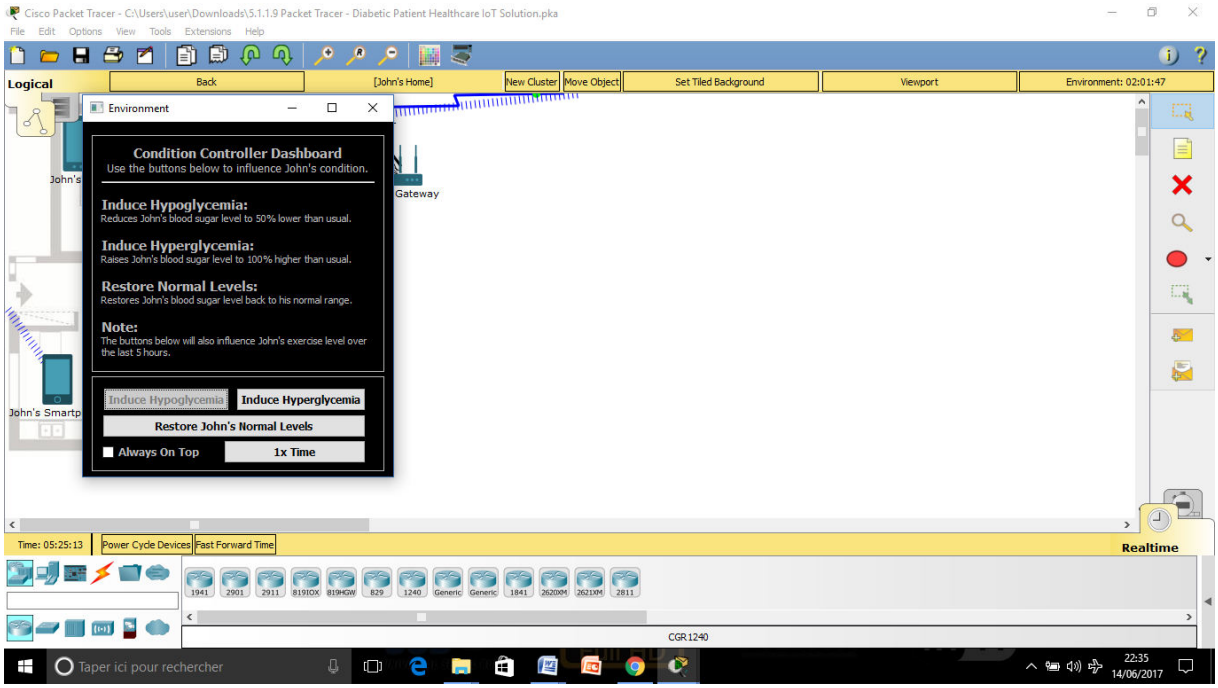

Figure III.20 : augmentation du taux de glycémie.

Remarque :

Les niveaux utilisés pour simuler cet événement sont basés sur les données historiques de John. Les analyses ont déterminé que le modèle et les niveaux rapportés ont conduit au coma diabétique ou aux visites de salles d'urgence pour John dans le passé. Ces niveaux ne signifient pas nécessairement des niveaux dangereux pour tous les patients diabétiques.

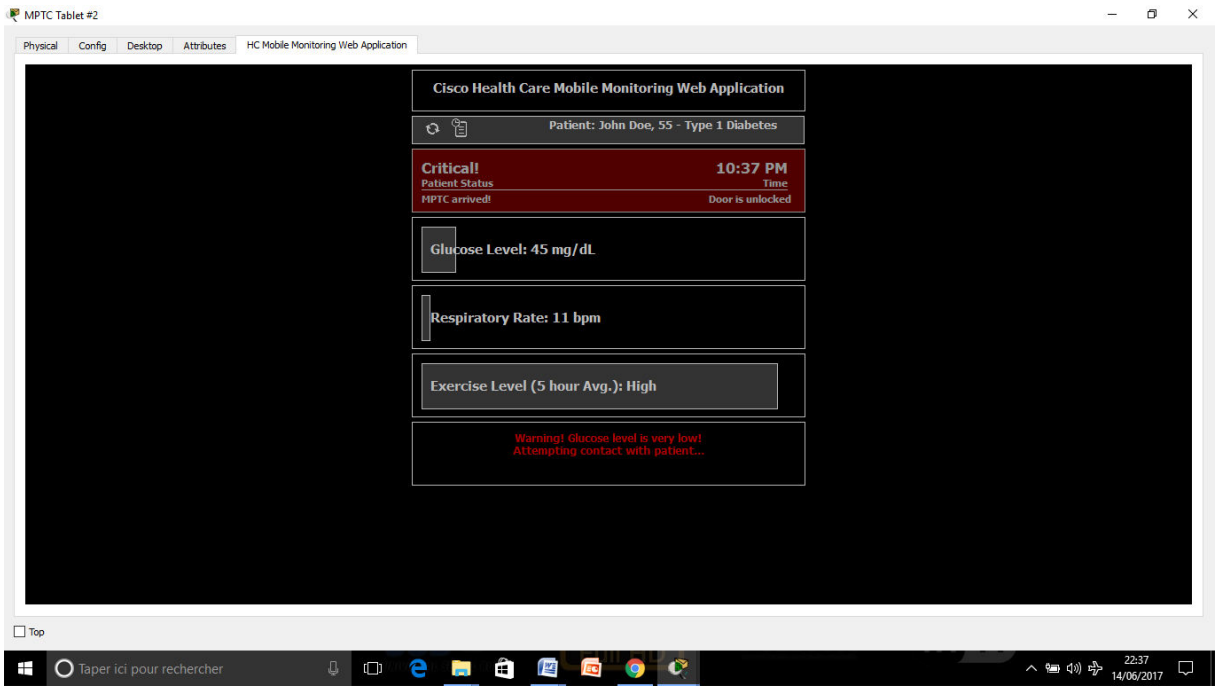

Figure III.21 : Message d'alerte d'hypoglycémie.

Étape 2: Induire l'hyperglycémie :

John a fini un grand repas lors de sa réunion de famille chez lui. Il a négligé de prendre son insuline alors qu'il était engagé avec sa famille.

- Accéder à l'onglet Application Web de surveillance HC Mobile sur sa tablette pour surveiller ses niveaux de glucose.
- Accéder à l'onglet Wearable Watch withSensors de son smartwatch pour surveiller ses niveaux de glucose.
- Dans la fenêtre Environnement, cliquer sur Induire l'hyperglycémie pour augmenter son niveau de glycémie, en simulant un événement hyper glycémique.
- Observer les alertes sur le smartwatch et la tablette de John.

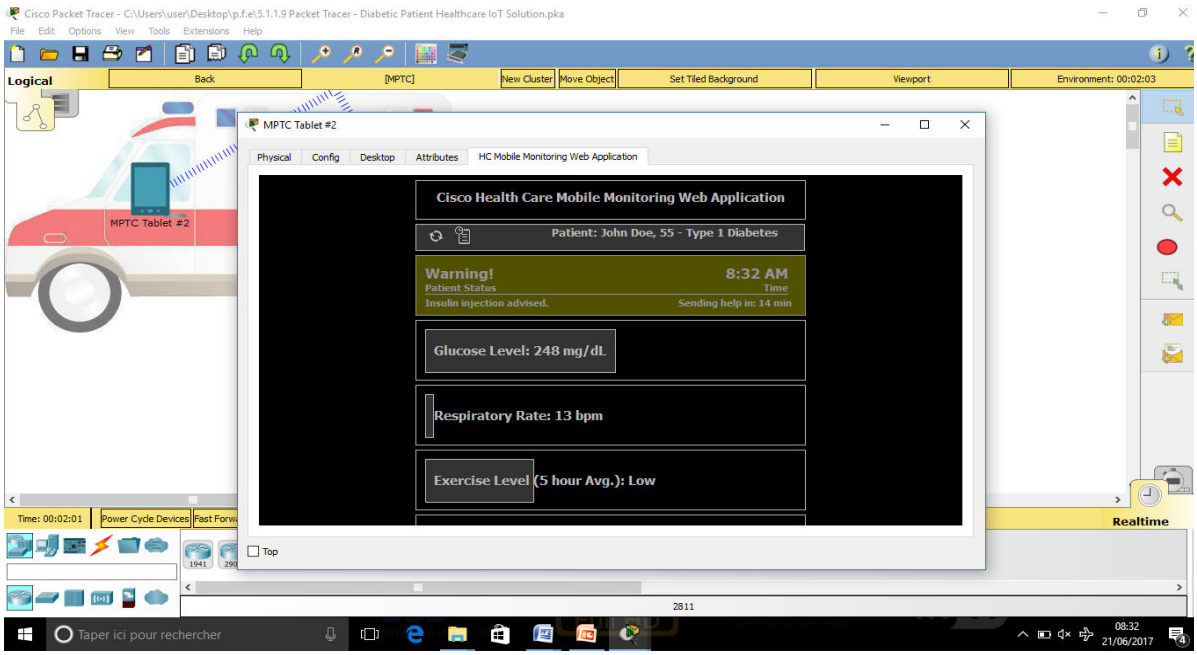

Figure III.22 Message d'alerte d'hyperglycémie.

Conclusion :

Ces deux exemples nous ont permis de prouver l'efficacité des objets connectés dans le milieu de la médecine : rapidité et facilité sont leurs maîtres mots. Il existe cependant encore d'autres domaines où les objets connectés sont utile dans le 1er cas en a pu voir que c'est possible connecter les périphériques informatiques et IoE au réseau domestique. En a interagie avec ces périphériques IoE localement et a distance via des pages web en allumant la lampe ou le ventilateur ou bien la machine a café a distance via une page web d'un pc de bureau ou bien d'un pc portable en accèdent au serveur qu'en a créé au départ pour ce qui est du deuxième cas les serveur sont installer a l'hôpital et les tablette de surveillance sont sur le tableau de bord de l'ambulance. Une fois que L'Hôpital reçois une signalisation via les capteurs installer ou domicile et sur le téléphone ainsi que sur la montre jugent que l'état de santé et critique ils interviennent dans les temps pour évité des dégâts irréversible.

CONCLUSION GENERALE :

Le marché des nouvelles technologies est marqué par une nouvelle discipline : les « objets connectés ». Ces concentrés technologiques sont des objets qui utilisent Internet pour améliorer leur fonctionnement.

Le premier fut la domotique : la technologie du domicile. C'est l'un des domaines les plus importants des objets connectés, où ils jouent un rôle de contrôle à différentes échelles. Ainsi, d'une application de téléphone, il est désormais possible d'allumer ses lumières, d'ouvrir le portail. Le quotidien est alors facilité.

Les objets connectés peuvent aussi avoir des tâches plus importantes et plus complexes, c'est le cas notamment dans le domaine de la santé, où ils deviennent des capteurs précis et facile à transporter. Ces facultés sont très importantes dans le cadre de certaines maladies : épilepsie, diabète, qui nécessite un contrôle permanent, d'un côté de l'activité corporelle, de l'autre de la glycémie.

Cela a permis d'émettre une affirmation : les objets connectés sont une source de progrès. Ils ouvrent des possibilités et faciliteront la vie quotidienne d'ici quelques années.

Nous avons pu voir dans les différents exemple qu'en a présenté comment le progrès technologique a jouer un rôle important dans l'aise de l'humanité a commencé par les réseaux qu'en a vue au premier chapitre qui ont intervenue dans notre configuration ensuite les objet connectés qu'en a traiter dans le deuxième chapitre qu'en a pu reliés a internet

Cependant, l'avenir n'est pas tout rose, et il est nécessaire de rester pragmatique à ce sujet. Bien qu'ils soient intéressants, les objets connectés amènent tout un lot de problèmes qu'il faudra prendre en compte.

Le premier risque provient de l'homme lui-même. Le fait de s'entourer de technologie informatise la vie, le piratage peut alors avoir des conséquences désastreuses. Un cracker pourrait facilement s'infiltrer dans le réseau de votre maison, et la contrôler comme il l'entend : bien que cela puisse faire sourire en premier lieu, au niveau de la sécurité c'est bien différent. Le cracker peut également avoir une surveillance de la vie personnelle, à l'aide par exemple des webcams ou caméras de Smartphones. C'est encore pire pour la santé : la vie des malades entre très rapidement en jeu.

Le second risque est de baser toute la vie aveuglément sur les objets connectés, ce qui, en cas de panne, serait très dangereux : la vie s'arrêterait tout simplement, à petite ou à grande

échelle. La panne a des causes souvent imprévisibles, sauf avec une vérification très précise quotidiennement : cela est impossible. Il est aussi nécessaire de prévoir le besoin énergétique pour que tous ces objets puissent fonctionner : ils se compteront en dizaines de milliards d'ici 2030, et représenteront donc une part non négligeable de la consommation électrique mondiale.

Cependant nous laisserons la parenthèse ouverte pour d'éventuelle recherche sur la sécurité et l'énergie nécessaire nous futur camarade pour travailler les questions

BIBLIOGRAPHIE

Les informations de ce mémoire sont tirées à partir de ces sites internet :

- ✓ Anonyme. 2008. *Internet of Things in 2020. Roadmap for the Future,* 1.1 ed.: 27: Infso D.4 Networked Enterprise & RFID; Infso G.2 Micro & Nanosystems in co-operation with the working group RFID of the EPOSS : 4.
- ✓ *Bureau du recensement des États-Unis, 2010 ; Forrester Research, 2003.*
- ✓ *Cisco IBSG, 2010, Bureau du recensement des États-Unis, 2010*
- ✓ *« Planetary Skin: A Global Platform for a New Era of Collaboration », Juan Carlos Castilla-Rubio et Simon Willis, Cisco IBSG, mars 2009,*
- ✓ « The Discovery of the Molecular Structure of DNA », NobelPrize.org
- ✓ « Augmented Business », The Economist, novembre 2010
- ✓ Fortune at the Bottom of the Pyramid: Eradicating Poverty Through Profits, Dr. C.K. Prahalad
- ✓ *« The Networked Pill », Michael Chorost, MIT Technology Review, 20 mars 2008*
- ✓ *« Researchers Debut One-Cubic-Millimeter Computer, Want to Stick It in Your Eye », Christopher Trout, Endadget, 26 février 2011,*
- ✓ « India Has Its Own Kind of Power Struggle », The Wall Street Journal, Jackie Range, 7 août 2009 Nations unies, 2010
- ✓ « Smart Dust Sensor Network with Piezoelectric Energy Harvesting », Yee Win Shwe and Yung C. Liang, ICITA, 2009,
- ✓ cf. : Preuverneers, D. and Berbers, Y. ‘‘Internet of Things: a Context-Awareness Perspective’’, in L. Yan, Y. Zhang, L. T. Yang and H. Ning (eds.), 2008 : 287-307.
- ✓ « First Practical Nanogenerator Produces Electricity with Pinch of the Fingers », PhysOrg.com, 29 mars 2011
- ✓ http://www.icita.org/papers/34-sg-Liang217.pdf
- ✓ http://www.physorg.com/news/2011-03nanogenerator-electricity-fingers.html
- ✓ http://www.cours-gratuit.com/cours-packet-tracer/
- ✓ *http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT*
- ✓ *http://books.openedition.org/editionsmsh/84?lang=fr*
- ✓ http://2005.jres.org/paper/70.pdf
- ✓ http://books.openedition.org/editionsmsh/docannexe/image/84/img-1.jpg
- ✓ http://books.openedition.org/editionsmsh/docannexe/image/84/img-2.jpg
- ✓

- *http://books.openedition.org/editionsmsh/docannexe/image/84/img-3.jpg*
- 7 http://www.forbes.com/2008/09/10/tonchIdOt-camera-iphone-tech-personal-cx_bc_0910iphone.html?feed=rss_news
- *http://www.physorg.com/news151162452.html ; George Colony, fondateur et directeur général de Forrester Research, 10 mars 2003*
- *http://www.engadget.com/2011/02/26/researchers-debut-one-cubic-millimetercomputer-want-to-stick-i/*
- *http://www.technologyreview.com/biomedicine/20434/?a=f*
- *https://www.netacad.com/*
- *http://www.i3s.unice.fr/~map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf*
- *http://robert.cireddu.free.fr/SIN/Creation%20et%20simulation%20reseau%20informatique.pdf*
- *http://www.cours-gratuit.com/cours-packet-tracer/*
- *http://www.fil.univ-lille1.fr/~sedoglav/RSX/Introduction.pdf*
- *http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-generalites.pdf*
- *http://www.cisco.com/web/about/ac79/docs/pov/Planetary_Skin_POV_vFINAL_spw_jc_2.pdf*

Glossaire:

IoE: Internet of Everything (L'Internet des Objets connectés).

PAN: Places Area Network.

FAN: File Area Network.

VoIP: Voice over Internet Protocol.

PDA : Portable Digital Assistant.

LAN: Local Area Network.

MAN: Metropolitan Area Network.

WAN: Wide Area Network.

OSI: Open System Interconnection.

MAC: Media Access Control.

FTP : File Transfer Protocol.

TCP/IP: Transmission Control Protocol/ Internet Protocol.

UDP: User Datagram Protocol.

IP: Internet Protocol.

Net Id: Network Identification.

FAI: Fournisseur d'Accès a Internet.

DNS : Domain Name System.

DHCP : Dynamic Host Configuration Protocol.

P2P: Person to Person.

M2P: Machine to Person.

M2M: Machine to Machine.

RFID: Radio Frequency Identification.

IaaS : Infrastructure as a Service.

PaaS: Protocol as a Service.

SaaS: Software as a Service.

NIST: National Institute of Standards and Technology.

IEEE: Institute of Electrical and Electronics Engineering.

IPS: Intrusion Prevention System.

OT: Operation Technology.

IT: Information Technology.

HTTP: Hyper Text Transfer Protocol.

SBC: Session Border Controller.

PSK: Phase Shift Keying.

SSID: Service Set IDentifer.

CGM: Compu Group Medical.

HMC: Hardware Management Console.

HC: Management Console.