الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb - Blida 1

Institut d'Aéronautique et des Études Spatiales

Département Études Spatiales

Mémoire de fin d'études

En vue de l'obtention du diplôme de

Master en Aéronautique

***Option :* Télécommunications spatiales**

THEME

Conception d'un raccordement sans fil des objets connectés d'une université intelligente

Proposé et dirigé par

Dr. AZINE Houria

Réalisé par

Mr BENNACER Mohamed A.D

Mr AISSAOUI Ahmed

Soutenu devant le jury composé de

Pr. … … … … … … … … … …	*Professeur*	*Président*
Dr. … … … … … … … … … …	*MCA*	*Examinateur*
Dr. … … … … … … … … … …	*MCB*	*Examinateur*

REMERCIEMENT

A Allah le très Clément et le très Miséricordieux

A nos familles

A nos professeurs

A tous ceux qui nous ont aidés de près ou de loin

Grand Merci à vous tous

الملخّص

تركز هذه الرسالة على تصميم حلاً لتوصيل الأجهزة المتصلة لاسلكيًا في إطار جامعة ذكية باستخدام برنامج سيسكو بَكِت تراسر. تطوّر شبكات الحواسيب فتح إمكانيات جديدة، وخاصة مع ظهور إنترنت الأشياء .في سياق الجامعات الذكية، توفر إنترنت الأشياء فرصًا لتحسين الكفاءة التشغيلية وتجربة متطورة للطلبة الجامعيين.

الهدف الرئيسي لهذه الدراسة هو تطوير حلاً فعّالًا ومناسبًا لتوصيل الأجهزة الذكية في الجامعة بشكل لاسلكي. ستتيح الأجهزة المتصلة جمع البيانات القيمة وجعل المهام المتكررة أوتوماتيكية والتفاعل بسلاسة مع بيئة الجامعة مما يتيح للجامعة أن تعزز عملياتها اليومية وتقدم تجربة طلابية ثرية.

سيظهر هذا المشروع التأثير الإيجابي الذي يمكن أن يحققه مثل هذا الحل على العمل الشامل لمؤسسات التعليم العالي.

كلمات مفتاحية: إنترنت الأشياء، جامعة ذكية، أوتوماتيكية، أجهزة الاستشعار، سيسكو بَكِت تراسر، التصميم، توصيل لاسلكي.

PREFACE

Cette mémoire se concentre sur la conception d'un raccordement sans fil des objets connectés dans le cadre d'une université intelligente en utilisant Cisco Packet Tracer. L'évolution des réseaux informatiques a ouvert de nouvelles possibilités, notamment avec l'émergence de l'Internet des Objets (IoT). Dans le contexte des universités intelligentes, l'IoT offre des opportunités pour améliorer l'efficacité opérationnelle et créer une expérience étudiante immersive.

L'objectif principal de cette étude est d'élaborer une solution efficace et adaptée permettant de connecter sans fil les objets intelligents d'une université, Les objets connectés permettront de collecter des données précieuses, d'automatiser des tâches récurrentes et d'interagir de manière transparente avec l'environnement universitaire. L'université pourra non seulement améliorer ses opérations quotidiennes, mais également offrir une expérience étudiante enrichie.

Ce projet démontrera l'impact positif qu'une telle solution peut avoir sur le fonctionnement global d'une institution d'enseignement supérieur.

Mots-clés : Internet des objets, Université intelligente, Automatisation, Capteurs, Cisco packet tracer, Conception, Raccordement sans fil.

ABSTRACT

This thesis focuses on the design of a wireless connectivity solution for connected objects in the context of a smart university using Cisco Packet Tracer. The evolution of computer networks has opened up new possibilities, particularly with the emergence of the Internet of Things (IoT). In the context of smart universities, IoT offers opportunities to improve operational efficiency and create an immersive student experience.

The main objective of this study is to develop an efficient and suitable solution for wirelessly connecting the smart objects in a university. Connected objects will enable the collection of valuable data, automation of recurring tasks, and seamless interaction with the university environment. The university will not only be able to enhance its daily operations but also provide an enriched student experience.

This project will demonstrate the positive impact that such a solution can have on the overall functioning of a higher education institution.

Keywords: Internet of Things, Smart University, Automation, Sensors, Cisco Packet Tracer, Design, Wireless Connectivity.

TABLE DE MATIERE

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABBREVIATIONS

- **2G** *: Deuxième Génération*
- **3G** *: Troisième Génération*
- **4G** *: Quatrième Génération*
- **5G** *: Cinquième Génération*
- **6LoWPAN** *: IPv6 over Low power Wireless Personal Area Networks (IPv6 sur les Réseaux Personnels sans Fil à Faible Consommation d'Énergie)*
- **API** *: Application Programming Interface (Interface de Programmation Applicative)*
- **AMQP** *: Advanced Message Queuing Protocol (Protocole de File d'Attente de Messages Avancé)*
- **ARPAnet** *: Advanced Research Projects Agency Network (Réseau de l'Agence pour les Projets de Recherche Avancée)*
- **BNC** *: Bayonet Neill-Concelman (Connecteur BNC)*
- **BGP** *: Border Gateway Protocol (Protocole de Passerelle de Frontière)*
- **Bluetooth** *: Bluetooth (Technologie de Communication sans Fil à Courte Portée)*
- **BLE** *: Bluetooth Low Energy (Bluetooth à Faible Consommation d'Énergie)*
- **CIDR** *: Classless Inter-Domain Routing (Routage Inter-Domaine Sans Classe)*
- **CoAP** *: Constrained Application Protocol (Protocole d'Application Contrainte)*
- **DHCP** *: Dynamic Host Configuration Protocol (Protocole de Configuration Dynamique des Hôtes)*
- **DNS** *: Domain Name System (Système de Noms de Domaine)*
- **DDoS** *: Distributed Denial-of-Service (Attaque par Déni de Service Distribué)*
- **DDS** *: Data Distribution Service (Service de Distribution de Données)*
- **DEL** *: Data Encryption Standard (Standard de Cryptage des Données)*
- **EIGRP** *: Enhanced Interior Gateway Routing Protocol (Protocole de Routage Amélioré pour les Passerelles Intérieures)*
- **FTP** *: File Transfer Protocol (Protocole de Transfert de Fichiers)*
- **FDII** *: Fully Distributed Internet Infrastructure (Infrastructure Internet Entièrement Distribuée)*
- **FFD** *: Full Function Device (Appareil Pleinement Fonctionnel)*

- **GSM** *: Global System for Mobile Communications (Système Global pour les Communications Mobiles)*
- **IoT :** *Internet of Things (Internet des Objets)*
- **IP** *: Internet Protocol (Protocole Internet)*
- **IPv4** *: Internet Protocol version 4 (Version 4 du Protocole Internet)*
- **IPv6** *: Internet Protocol version 6 (Version 6 du Protocole Internet)*
- **ISO** *: International Organization for Standardization (Organisation Internationale de Normalisation)*
- **IS-IS** *: Intermediate System to Intermediate System (Système Intermédiaire vers Système Intermédiaire)*
- **IRS** *: Intelligent Routing System (Système de Routage Intelligent)*
- **IDS** *: Intrusion Detection System (Système de Détection d'Intrusion)*
- **IPS** *: Intrusion Prevention System (Système de Prévention d'Intrusion)*
- **IAM** *: Identity and Access Management (Gestion des Identités et des Accès)*
- **IEEE** *: Institute of Electrical and Electronics Engineers (Institut des Ingénieurs en Électricité et Électronique)*
- **LPWAN** *: Low-Power Wide Area Network (Réseau Étendu à Faible Consommation d'Énergie)*
- **LAN** *: Local Area Network (Réseau Local)*
- **LoRaWAN** *: Long Range Wide Area Network (Réseau Étendu à Longue Portée)*
- **LC** *: Lucent Connector (Connecteur LC)*
- **LED** *: Light Emitting Diode (Diode Électroluminescente)*
- **MAN** *: Metropolitan Area Network (Réseau Métropolitain)*
- **MAC** *: Media Access Control (Contrôle d'Accès au Média)*
- **MQTT** *: Message Queuing Telemetry Transport (Transport de Télémétrie par File d'Attente de Messages)*
- **MMS** *: Multimedia Messaging Service (Service de Messagerie Multimédia)*
- **NFC** *: Near Field Communication (Communication en Champ Proche)*
- **NIC** *: Network Interface Card (Carte d'Interface Réseau)*
- **OSPFv2** *: Open Shortest Path First version 2 (Version 2 du Protocole du Chemin le Plus Court d'Abord Ouvert)*
- **OSI** *: Open Systems Interconnection (Interconnexion de Systèmes Ouverts)*
- **PDU** *: Protocol Data Unit (Unité de Données de Protocole)*

- **Ping** *: Packet Internet Groper (Interrogation de Paquets sur Internet)*
- **PAN :** *Personal Area Network (Réseau Personnel)*
- **QoS** *: Quality of Service (Qualité de Service)*
- **RIPv2** *: Routing Information Protocol version 2 (Version 2 du Protocole d'Information de Routage)*
- **RFD** *: Reduced Function Device (Appareil à Fonction Réduite)*
- **RFID** *: Radio Frequency Identification (Identification par Radiofréquence)*
- **RF** *: Radio Frequency (Radiofréquence)*
- **RJ45** *: Registered Jack 45 (Connecteur Jack Enregistré 45)*
- **SMTP** *: Simple Mail Transfer Protocol (Protocole Simple de Transfert de Courrier)*
- **SMS** *: Short Message Service (Service de Messages Courts)*
- **SIM** *M2M : Machine-to-Machine Subscriber Identity Module (Module d'Identification d'Abonné Machine à Machine)*
- **SSID** *: Service Set Identifier (Identifiant de l'Ensemble de Services)*
- **STP** *: Shielded Twisted Pair (Paire Twisted Blindée)*
- **SBC** *: Single Board Computer (Ordinateur à Carte Unique)*
- **TCP/IP** *: Transmission Control Protocol/Internet Protocol (Protocole de Contrôle de Transmission/Protocole Internet)*
- **UTP** *: Unshielded Twisted Pair (Paire Twisted Non Blindée)*
- **UDP** *: User Datagram Protocol (Protocole de Datagramme d'Utilisateur)*
- **VPN** *: Virtual Private Network (Réseau Privé Virtuel)*
- **WAN** *: Wide Area Network (Réseau Étendu)*
- **Wifi** *: Wireless Fidelity (Fidélité Sans Fil)*
- **WAP :** *Wireless Access Point (Point d'Accès sans Fil).*

INTRODUCTION GENERALE

INTRODUCTION GENERALE

L'évolution des réseaux informatiques a été spectaculaire, transformant fondamentalement notre façon de communiquer, d'accéder à l'information et d'interagir avec le monde qui nous entoure. Autrefois limités à des connexions entre ordinateurs, les réseaux sont devenus des systèmes interconnectés complexes, capables de connecter des milliards d'appareils à travers le globe.

L'un des développements les plus marquants de cette évolution est l'émergence de l'Internet des Objets (IoT). L'IoT représente une nouvelle frontière dans la connectivité, où des objets du quotidien sont connectés à Internet et peuvent communiquer entre eux, collecter des données et interagir avec leur environnement.

L'IoT présente également des opportunités sans précédent dans le domaine de l'éducation, et plus spécifiquement dans le contexte des universités intelligentes.

En utilisant des dispositifs IoT, les universités peuvent améliorer l'efficacité de leurs opérations, optimiser la gestion des ressources et offrir une expérience étudiante plus immersive et personnalisée.

Dans le cadre de cette mémoire, nous nous concentrons sur l'exploration des fondements des réseaux informatiques ainsi que sur l'application de l'IoT dans un contexte spécifique, à savoir celui d'une université intelligente.

Ce mémoire est structuré en quatre chapitres :

- Dans le premier chapitre, nous aborderons les notions de base des réseaux informatiques, en définissant brièvement les différents types de réseaux. . Nous discuterons également des modèles d'architecture réseau tels que l'OSI et TCP/IP, ainsi que les topologies réseaux, le routage et la sécurité des réseaux.
- Le deuxième chapitre est consacré à l'Internet des objets (IoT) et à son application dans le contexte universitaire. Nous définissons l'IoT et présenterons son histoire. Nous explorons également les différentes technologies utilisées dans l'IoT, notamment les composants des objets connectés et les réseaux IoT.
- Le troisième chapitre se concentre sur les équipements et les interconnexions nécessaires pour mettre en place une université intelligente. Nous discuterons des équipements réseau et les différents médias réseau. De plus, nous identifierons les équipements spécifiques nécessaires dans différents départements de l’université.

- Le quatrième chapitre est le chapitre de simulation, les tests et les résultats de l'université intelligente. Nous dériverons ensuite la configuration des différents réseaux de l'université et nous évaluons également la connectivité des appareils IoT et les performances globales du réseau.

Enfin, nous discuterons des résultats obtenus et des recommandations pour l'amélioration continue du système.

Enfin, nous conclurons ce travail par une conclusion générale et des perspectives.

CHAPITRE1

NOTIONS DE BASE SUR LES RESEAUX

CHAPITRE 1

NOTIONS DE BASE SUR LES RESEAUX

Dans ce chapitre, nous allons explorer les notions fondamentales des réseaux informatiques. Les réseaux jouent un rôle essentiel dans notre monde moderne, en permettant la communication, le partage d'informations et l'accès à des ressources distantes.

En explorant ces notions de base sur les réseaux, nous aurons une compréhension solide des principes fondamentaux qui sous-tendent les communications informatiques.

Ces connaissances seront essentielles pour la suite de notre étude.

1.1 - DEFINITION DU RESEAU INFORMATIQUE

Un réseau informatique est une collection d'ordinateurs autonomes interconnectés par une seule technologie. Deux ordinateurs sont dits interconnectés s'ils sont capables d'échanger des informations.

La connexion ne doit pas juste se faire via un fil de cuivre ; les fibres optiques, les micro-ondes, l'infrarouge et les satellites de communication peuvent également être utilisés.

Les réseaux existent sous différentes tailles et formes, comme nous le verrons plus tard. Ils sont généralement connectés les uns aux autres pour former des réseaux plus grands, Internet étant l'exemple le plus connu. **[1]**

1.2 – CLASSIFICATION DES RESEAUX (PAR DIMENSION)

Le langage courant distingue les réseaux selon différents critères. La classification traditionnelle, fondée sur la notion d'étendue géographique, correspond à un ensemble de contraintes que le concepteur devra prendre en compte lors de la réalisation de son réseau.

Généralement, on adopte la terminologie suivante **[2]** :

1.2.1 – RESEAU PAN (PERSONAL AREA NETWORK)

Un réseau personnel (PAN) est un réseau informatique permettant d'interconnecter des dispositifs électroniques centrés sur l'espace de travail individuel d'une personne, tels qu'une souris sans fil, un clavier et un ordinateur.

La figure 1.1 montre un exemple du réseau.

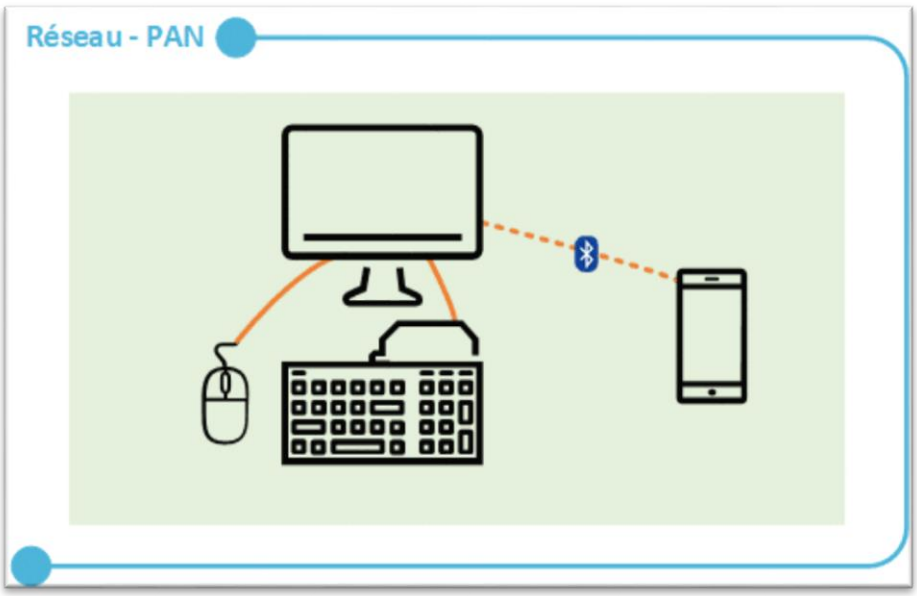


Figure 1.1 : Réseau PAN

1.2.2 - RESEAU LAN (LOCAL AREA NETWORK)

Le réseau LAN désigne un réseau s'étendant sur quelques mètres jusqu'à plusieurs kilomètres. C'est un réseau à la taille d'une entreprise (un étage, un bâtiment, une boutique...etc.),

Il peut s'étendre sur plusieurs centaines de mètres. Son débit varie aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde (Mbps). Voici un schéma d'un réseau LAN très simple qui reproduit ce qu'on peut avoir à la maison.

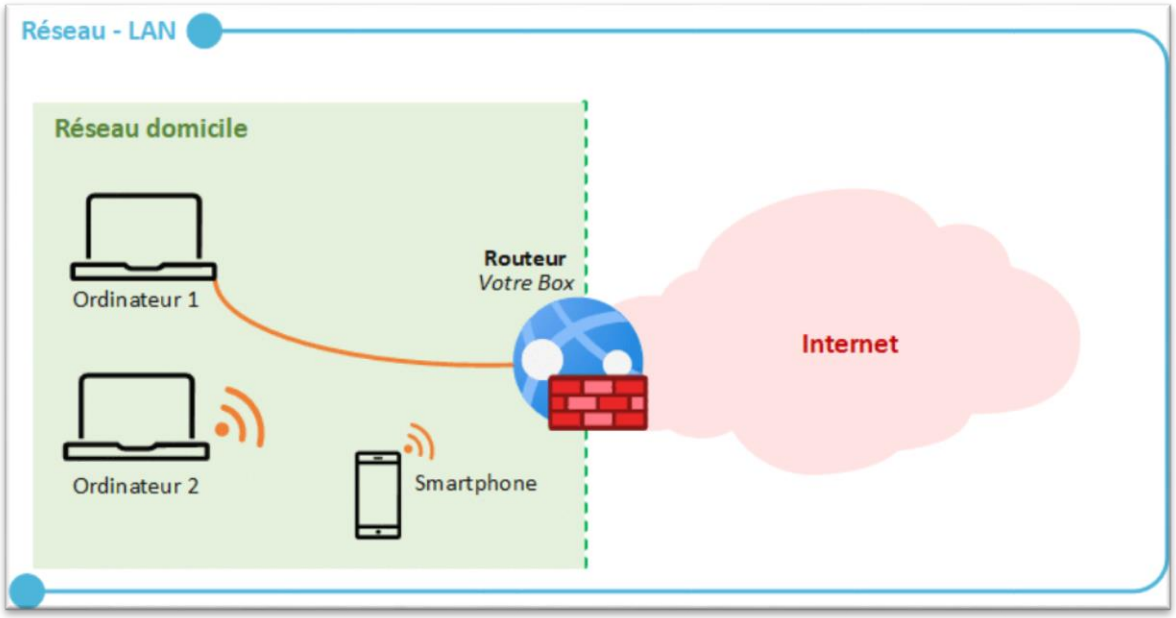


Figure 1.2 : Réseau LAN

1.2.3 - RESEAU MAN (METROPOLITAIN AREA NETWORK)

Le réseau MAN traduit par réseau métropolitain, intègre les réseaux d'interconnexions des entreprises ou des réseaux particuliers à l'échelle d'une ville ou d'une région. En général, il permet de véhiculer les données entre les réseaux locaux d'entreprises.

La figure 1.3 illustre un exemple du réseau.

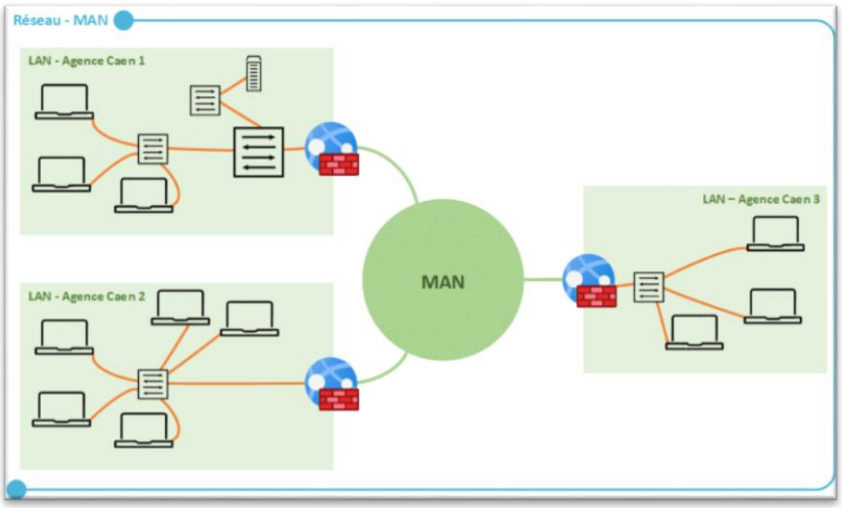


Figure 1.3 : Réseau MAN

1.2.4 - RESEAU WAN (WIDE AREA NETWORK)

Appelé aussi réseau étendu, le réseau WAN englobe des sites géographiquement éloignés les uns des autres (figure 1.4). Il est destiné à transporter les informations sur des distances à l'échelle d'un pays. Il sert surtout pour désigner tout réseau dépassant l'étendue d'un seul établissement physique et constitué par l'interconnexion de plusieurs réseaux élémentaires **[3]**.

Figure 1.4 : Réseau WAN **[26]**

1.2.5 - COMPARAISON ENTRE LES RESEAUX PAN, LAN, MAN ET WAN

Le tableau 1.1 illustre la différence entre les classes réseaux :

Réseau / Paramètres	PAN	LAN	MAN	WAN
Zone couverte	Petite zone (Rayon 10 m)	Quelques mètres à quelques kilomètres (Rayon 10 km)	Une ville et ses environs (Rayon 100 km)	Pays entier, continent ou globe entier
Vitesse de transmission	Haute vitesse	Haute vitesse	Vitesse modérée	Faible vitesse
Coût	Négligeable	Peu coûteux	Équipements modérément coûteux	Coûteux
Exemple	Bureau de travail	Écoles, maisons, collèges, hôpitaux	Plusieurs campus universitaires dans une ville donnée	Internet

Tableau 1.1 : Comparaison entre les classes réseau

1.3 – LES ADRESSES MACHINES (IDENTIFICATION)

On désigne par technique d'adressage l'ensemble des moyens utilisés pour identifier les correspondants.

Pour assurer la communication, le système d'extrémité source doit fournir au réseau l'adresse du système d'extrémité destinataire, et celui-ci doit pouvoir identifier son correspondant.

Une adresse est une suite de caractères désignant sans ambiguïté un point physique de raccordement à un réseau (adressage physique) ou identifiant un processus, une machine (adressage logique). Ces deux notions sont complémentaires, l'une désigne l'objet (adresse logique), l'autre sa localisation (adresse physique). **[2]**

1.3.1 – ADRESSE IP (INTERNET PROTOCOL)

Une adresse IP (Internet Protocol) est une étiquette numérique unique attribuée à chaque périphérique connecté à un réseau informatique. Elle permet la communication entre les périphériques sur le réseau en identifiant leur source et leur destination.

Il est important de noter qu'une adresse IP ne se réfère pas réellement à un hôte. Elle se réfère en réalité à une interface réseau, donc si un hôte est sur deux réseaux, il doit avoir deux adresses IP.

L'adresse IP est généralement affichée en 4 nombres (entre 0 et 255) séparés par des points. **[1]**

1.3.2 - VERSION D'ADRESSE IP :

On distingue deux versions principales d'adresse IP comme illustrer dans la figure 1.5 :

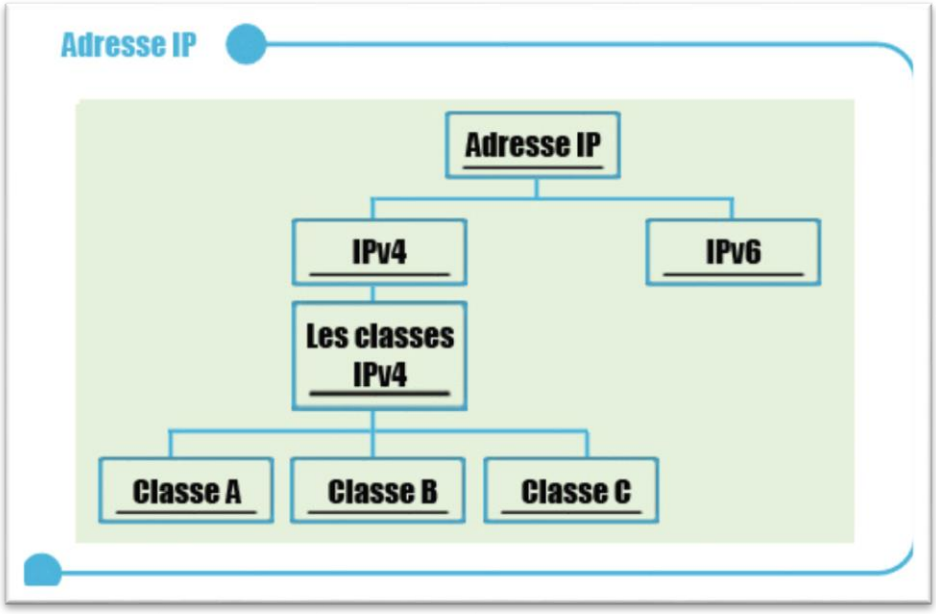


Figure 1.5 : Schéma adresse IP

1.3.2.1 - IPv4 (Internet Protocole version 4)

Une caractéristique fondamentale d'IPv4 est ses adresses de 32 bits. Souvent représentées sous la forme de quatre nombres décimaux séparés par des points. La version 4 domine l'Internet aujourd'hui. **[1]**

1.3.2.2 - IPv6 (Internet Protocole version 6)

La prochaine version d'IP, utilise des adresses de 128 bits, qui sont beaucoup plus longues que les adresses IPv4. Elle a été définie il y a plus d'une décennie, mais commence seulement à être déployée.

Son utilisation sera éventuellement obligatoire lorsque chacun des presque 231 millions de personnes en Chine aura un ordinateur de bureau, un ordinateur portable et un téléphone IP.

À titre d'information sur la numérotation, IPv5 était un protocole expérimental de flux en temps réel qui n'a jamais été largement utilisé. **[1]**

1.3.3 - LES CLASSES DES ADRESSES IPV4

Avant 1993, les adresses IP étaient divisées en cinq catégories répertoriées dans la figure 1.6. Cette allocation est devenue ce que l'on appelle l'adressage en classe. **[1]**

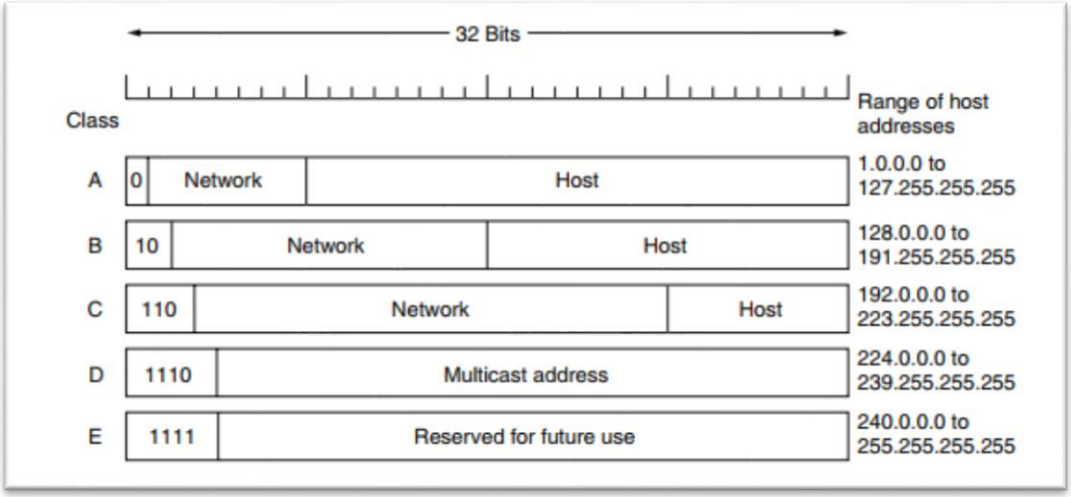


Figure 1.6 : Les classes IPv4

Les adresses IP sont divisées en fonction de leur plage d'adresses et de leur structure. Le but de cette division est de faciliter la recherche d'un ordinateur sur le réseau. Elles sont maintenant remplacées par des systèmes plus flexibles, tels que le CIDR (Classless Inter-Domain Routing).

- **Les adresses de classe A** : s'étendent de 1.0.0.1 à 126.255.255.254. Elles permettent d'adresser 126 réseaux (27 – 2) et plus de 16 millions de machines (224 – 2, soit 16 777 214).
- **Les adresses de classe B** : vont de 128.0.0.1 à 191.255.255.254, ce qui correspond à plus de 16 384 réseaux de 65 533 machines. Cette classe est la plus utilisée et les adresses sont aujourd'hui pratiquement épuisées.
- **Les adresses de classe C** : couvre les adresses 192.0.0.1 à 223.255.255.254, elle adresse plus de 2 millions de réseaux (2 097 152) de 254 machines. **[2]**

1.3.4 - LE MASQUE DE SOUS RESEAU (SUBNET MASK)

Le masque de sous-réseau définit le nombre de bits d'hôte dans une adresse IP. Les bits de valeur 0 indiquent quels bits de l'adresse IP correspondent à l'adresse d'hôte. Le masque est un élément important dans la formule pour diviser une adresse IP, ainsi que dans la connaissance du nombre de bits de réseau impliqués pour les réseaux de classe A, B et C.

Le masque de sous-réseau fournit une définition claire de la taille du réseau et des parties d'hôtes d'une adresse. **[4]**

Le masque de sous-réseau est souvent exprimé sous forme de notation décimale pointée, où chaque octet du masque de sous-réseau est représenté par un nombre décimal compris entre 0 et 255. Dans la figure 1.7 en trouve le SUBNET MASK des classes IP.

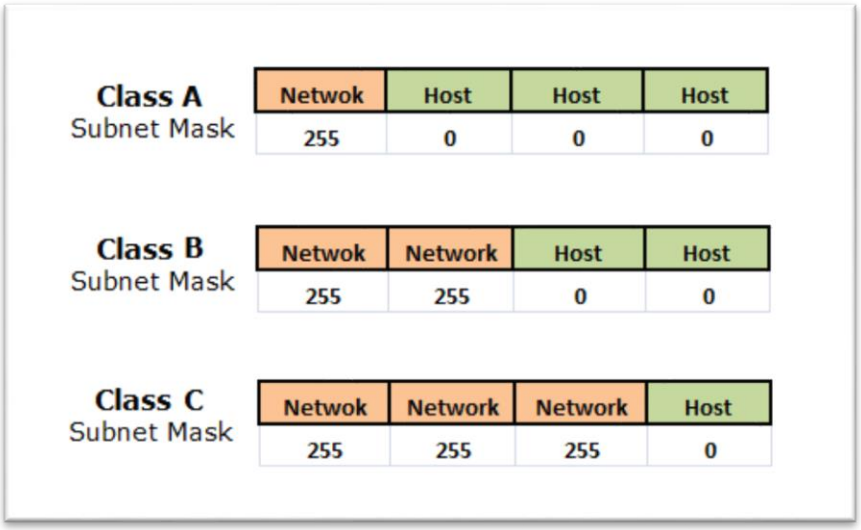


Figure 1.7 : Les masques de sous-réseau pour chaque classe d'adresses IPv4 **[27]**

1.3.5 - ADRESSE MAC :

L'adresse MAC (pour Media Access Control) est l'adresse physique attribuée par le fabricant à une carte réseau ou à un périphérique réseau.

Utilisée pour identifier de manière unique un périphérique sur un réseau local. Elle est représentée par un nombre hexadécimal de 12 chiffres (0-9 et A-F) et chaque périphérique dans le monde à une adresse MAC unique.

Les adresses MAC sont généralement utilisées pour diriger les paquets d'un périphérique à l'autre lorsque les données circulent sur un réseau.

1.3.6 - DHCP PROTOCOLE (DYNAMIQUE HOST CONFIGURATION PROTOCOL)

Traditionnellement, un utilisateur pouvait soit configurer manuellement l'adresse de son appareil, soit laisser l'hôte acquérir son adresse de manière dynamique grâce à des méthodes dynamiques telles que le protocole de configuration dynamique des hôtes (DHCP).

Le serveur DHCP est l'infrastructure réseau la plus importante.

Il est considéré comme un composant essentiel utilisé pour fournir de manière dynamique des adresses IP et des paramètres de configuration d'hôte aux appareils utilisateurs. **[5]**

Le protocole fonctionne en permettant aux clients de réseau de demander une adresse IP auprès d'un serveur DHCP centralisé.

Le serveur DHCP reçoit alors la demande et attribue une adresse IP disponible à partir d'une plage d'adresses IP prédéfinie, ainsi que d'autres paramètres de configuration réseau.

1.3.7 - DNS PROTOCOLE

Le DNS facilite la navigation sur le Web en permettant aux utilisateurs de se connecter à des sites Web en utilisant des noms de domaine familiers, nous remplaçons les adresses IP numériques par une série de mots simples et significatifs séparés par des points.

Par exemple, le nom de domaine "www.ndhu.edu.tw" est un point d'accès au serveur WWW de l'Université nationale Dong Hwa, un établissement d'enseignement à Taiwan.

Chaque fois que vous souhaitez accéder aux ressources de ce serveur, entrez simplement "www.ndhu.edu.tw", et le serveur de nom de domaine le résoudra à l'adresse IP "203.64.88.52" pour vous. Vous n'avez pas besoin de vous souvenir de ces adresses IP numériques compliquées. **[6]**

1.4 - MODELE D'ARCHITECTURE DES RESEAUX

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication.

Pour que les données arrivent correctement au destinataire, avec la qualité de service, ou QoS (Quality of Service), exigée, il faut en outre une architecture logicielle chargée du contrôle des paquets dans le réseau.

Les deux grandes architectures suivantes se disputent actuellement le marché mondial des réseaux :

- l'architecture OSI (Open Systems Interconnection), ou interconnexion de systèmes ouverts, provenant de la normalisation de l'ISO (International Standardization Organization).
- l'architecture TCP/IP utilisée dans le réseau Internet. **[7]**

1.4.1 - MODELE OSI (OPEN SYSTEMS INTERCONNECTION)

Le modèle OSI est basé sur une proposition élaborée par l'Organisation internationale de normalisation (ISO) comme première étape vers la normalisation internationale des protocoles utilisés dans les différentes couches.

Le modèle est appelé modèle de référence OSI ISO car il traite la connexion de systèmes ouverts, c'est-à-dire de systèmes ouverts à la communication avec d'autres systèmes.

Le modèle regroupe les fonctions de communication en sept couches logiques présenté dans la figure1.8. **(1)**

Figure1.8 : Les couches du modèle OSI **[28]**

Couche	Description
Couche Physique (*Physical Layer*)	Assure un transfert de **bits** sur le canal physique (support). À cet effet, elle définit les supports et les moyens d'y accéder
Couche liaison de données (*Data Link Layer*)	Assure, sur la ligne, un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités.
Couche Réseau (Network Layer)	Assure, lors d'un transfert à travers un système relais, l'acheminement des données (paquets) à travers les différents nœuds d'un sous-réseau (routage).
Couche Transport (*Transport Layer*)	C'est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (messages) entre les deux systèmes d'extrémité.
Couche Session (*Session Layer*)	Gère l'échange de données (transaction) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges et la définition de points de reprise
Couche Présentation (Présentation *Layer*	Interface entre les couches qui assurent l'échange de données et celle qui les manipule, cette couche assure la mise en forme des données, les conversions de code nécessaires pour délivrer à la couche supérieure un message dans une syntaxe compréhensible par celle-ci. En outre, elle peut, éventuellement, réaliser des transformations spéciales, comme la compression de données.
Couche Application (Application *Layer*)	C'est la dernière du modèle de référence, fournit au programme utilisateur, l'application proprement dite, un ensemble de fonctions (entités d'application) permettant le déroulement correct des programmes communicants (transferts de fichiers, courrier électronique...) **[2]**

Tableau 1.2 : Description des couches du modèle OSI

1.4.2 - L'ARCHITECTURE TCP/IP :

L'architecture TCP/IP porte le nom des protocoles principaux qui la constituent, à savoir TCP et IP ; On l'a définie dans les années 1960 pour le réseau ARPAnet.

Elle s'est considérablement développée avec le succès d'Internet. La conception de l'architecture TCP/IP compte quatre couches représenter dans la figure 1.9 et diffère de celle du modèle OSI.

Contrairement aux normes de l'ISO qui sont très complexes en raison de leur vocation universelle, les concepteurs de TCP/IP ont cherché à fournir une solution opérationnelle rapidement, même si elle ne résout pas l'ensemble du problème. [8]

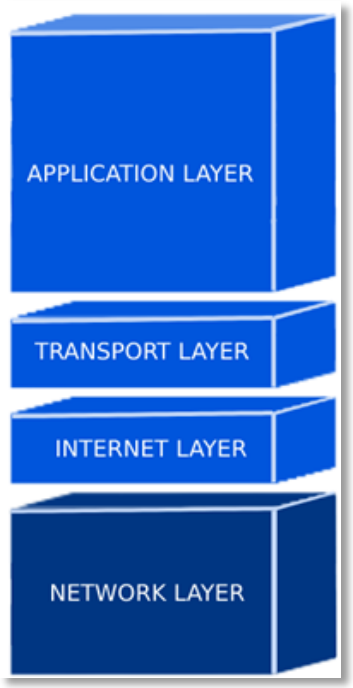


Figure1.9 : les couches du modèle TCP/IP

Couche	Description
Couche Accès réseau	Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé
Couche Internet	Elle est chargée de fournir le paquet de données (datagramme)
Couche Transport	Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission
Couche Application	Elle englobe l'application standard du réseau (Telnet, SMTP, FTP, ...) [9]

Tableau 1.3 : Description des couches du modèle TCP/IP

1.5 - TOPOLOGIE DES RESEAUX

1.5.1 - DEFINITION DE LA TOPOLOGIE RESEAU

La topologie de réseau désigne la façon dont les dispositifs et les câbles sont connectés dans un réseau informatique. Elle définit la structure et les schémas de communication d'un réseau, en déterminant comment les nœuds, les dispositifs et les liaisons sont organisés.

La topologie d'un réseau peut avoir un impact sur la vitesse, la fiabilité et la facilité de gestion du réseau.

1.5.2 - LES DIFFERENTES TOPOLOGIES

Voici quelques-unes des topologies de réseau les plus couramment utilisées :

1-5-2-1- la topologie en bus

La topologie en bus, également appelée topologie linéaire, est l'une des topologies les plus simples, ce qui en fait un choix économique pour les petits réseaux.

Elle se compose d'un support central (le "bus"), une ligne avec deux extrémités, à laquelle tous les nœuds sont connectés.

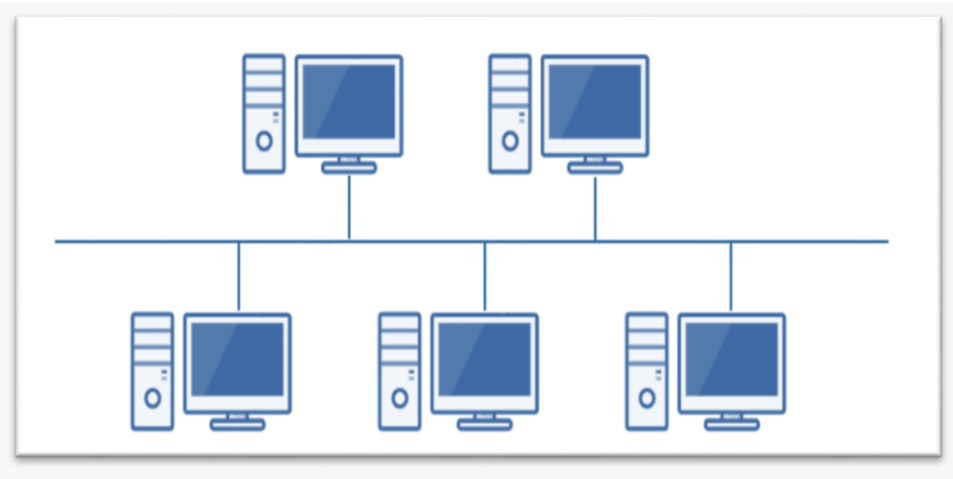


Figure 1.10 : la topologie en bus

1-5-2-2- la topologie en étoile

La topologie en étoile est l'une des topologies de réseau les plus courantes.

Dans cette topologie, chaque nœud du réseau est connecté individuellement à un concentrateur central, qui gère et contrôle l'ensemble du réseau.

Ensemble, les nœuds s'étendent depuis ce concentrateur central comme les branches d'une étoile.

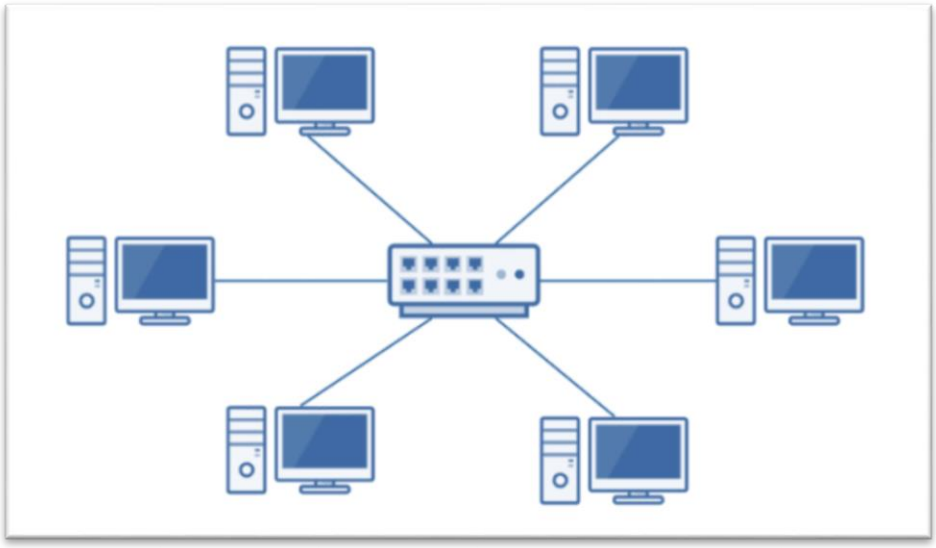


Figure 1.11 : la topologie en Etoile

1-5-2-3- la topologie anneau

Dans une topologie en anneau, chaque nœud est connecté à deux autres pour former un réseau fermé en forme de cercle. Les informations sont envoyées d'un nœud à un autre à travers l'anneau jusqu'à ce qu'elles atteignent leur destination.

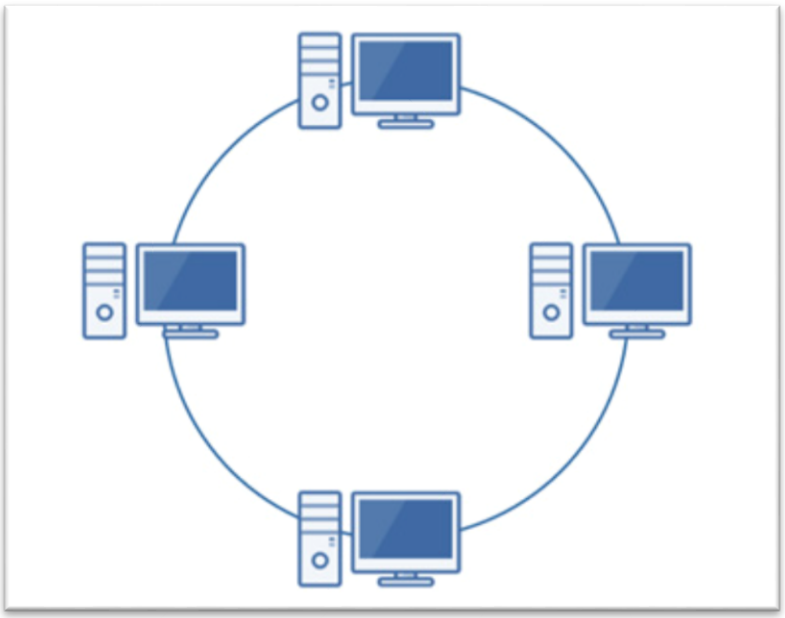


Figure 1.12 : la topologie en anneau

1-5-2-4- la topologie maillée

La topologie maillée (Mesh Topology en anglais) existe sous deux formes. L'une est la topologie maillée complète (illustrée ci-dessous), où chaque nœud est interconnecté.

En revanche, la topologie maillée partielle signifie que les nœuds ne sont connectés qu'aux autres nœuds avec lesquels ils interagissent le plus souvent. **[29]**

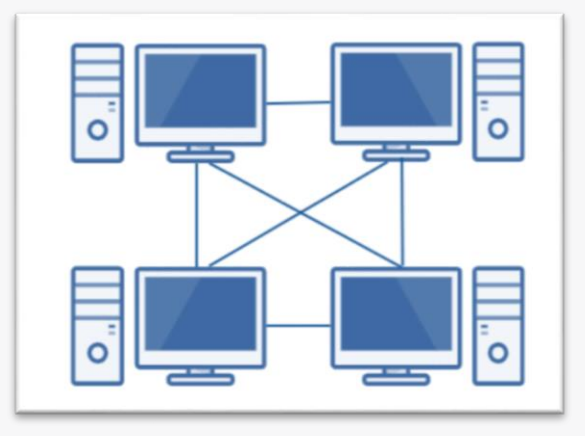


Figure1.13 : la topologie maillée

1.5.3 - LES AVANTAGES ET LES INCONVENIENTS DE CHAQUE TOPOLOGIE :

Topologies réseaux	Avantages	Inconvénients
Topologie en bus	* Simplicité * Interconnexion de tous les ordinateurs * Une seule ligne de communication * Si un hôte tombe en panne, le réseau n'est pas affecté	* Disparition du signal aux extrémités. * Problèmes graves si coupure de la ligne.
Topologie en Etoile	* Efficacité * Economie * Concentrateur qui relie et assure la communication entre tous les ordinateurs	* Risque ; Le nœud central ne doit jamais tomber en panne
Topologie en anneau	* Simplicité (Boucle) * Relativement économique * Répartiteur qui gère la communication entres les ordinateurs. * Temps de parole imparties * Utilisé par les topologies logiques : Token ring & FDII	* Peu efficace * Peu fiable * Dés que deux (2) lignes ne marchent pas, le réseau est coupé
Topologie hiérarchique	* Présence de plusieurs niveaux permettant une connexion hiérarchique * Arborescence	* Peu efficace * Les nœuds intermédiaires peuvent être des goulets d'étranglement
Topologie maillée	* Topologie la plus fiable * Chaque terminal est relie a tous les autres * Possibilité d'utiliser divers itinéraires. * Contrôle effectué par de puissants superviseurs de réseau.	* Topologie la plus couteuse * Nécessité d'avoir nombres de liaison très élevé.

Tableau 1.4 : avantages et inconvénients des topologies

1-6- LE ROUTAGE DES RESEAUX

1.6.1 – DEFINITION DU ROUTAGE :

Un environnement internet résulte de l'interconnexion de plusieurs réseaux physique par des routeurs, chaque routeur est connecté directement à deux ou plusieurs réseaux.

Le routage est le processus qui permet de trouver le meilleur chemin pour transmettre les paquets informations d'un réseau à un autre en utilisant des routeurs et des tables de routage.

Cela permet d'acheminer les données vers la destination souhaitée, même si elle se trouve sur un réseau distant. **[10]**

1.6.2 – DEFINITION DE LA TABLE DE ROUTAGE :

La table de routage est un élément essentiel stocké sur un routeur, qui est un équipement utilisé pour connecter différents réseaux informatiques et assurer le routage des paquets de données.

Cette table conserve des informations sur les chemins menant à des destinations spécifiques du réseau, ainsi que des métriques de routage qui déterminent la préférence ou la qualité de chaque chemin. **[30]**

Voici un exemple simplifié d'une table de routage :

Réseau de destination	Masque de sous-réseau	Prochain saut (adresse du routeur)
192.168.1.0	255.255.255.0	192.168.1.1

Tableau 1.5 : exemple table de routage

Dans cet exemple, la table de routage comprend une entrée. Le masque de sous-réseau indique la portée du réseau.

Le prochain saut est l'adresse IP du routeur vers lequel les paquets doivent être envoyés pour atteindre le réseau de destination.

Dans cette entrée, tous les paquets destinés au réseau 192.168.1.0 avec un masque de sous-réseau de 255.255.255.0 seront dirigés vers le routeur dont l'adresse est 192.168.1.1

1.6.3 - LES TYPES DE ROUTAGE :

Il existe deux types principaux de routage : le routage statique et le routage dynamique comme illustre la figure 1.14.

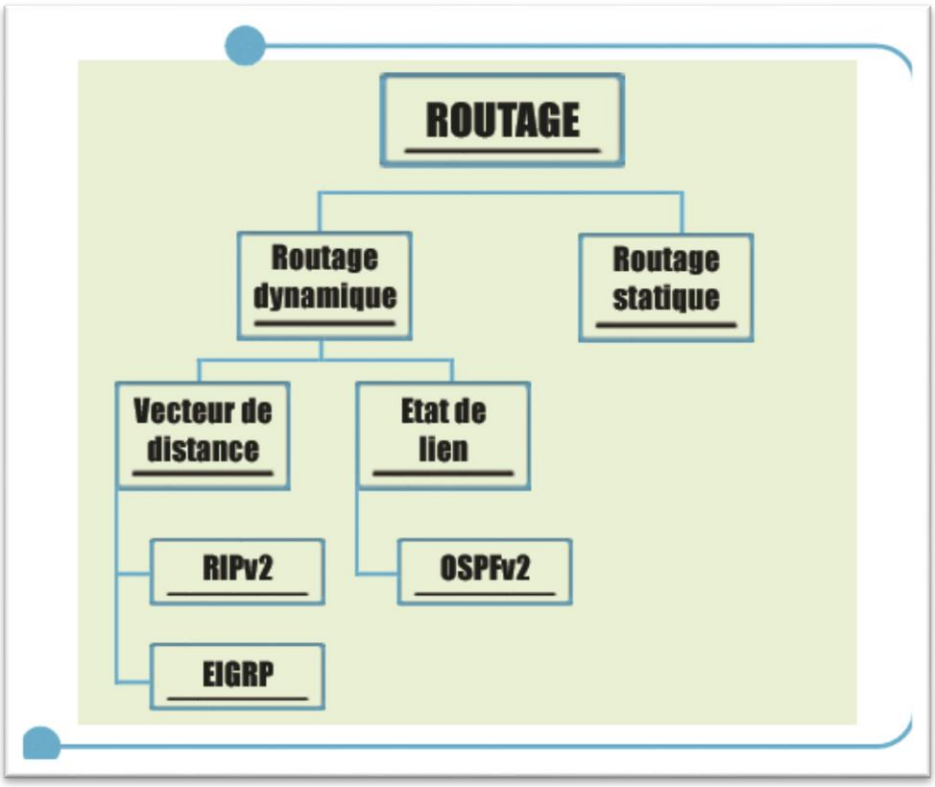


Figure 1.14 : type de routage

1-6-3-1- Routage statique

Le routage statique consiste à configurer manuellement les chemins de routage dans chaque nœud du réseau. Pour chaque destination, l'administrateur du réseau spécifie l'adresse du prochain nœud vers lequel les paquets doivent être envoyés. Cela nécessite une configuration préalable et des mises à jour manuelles en cas de changements de la topologie du réseau. **[11]**

Le routage statique convient aux petits réseaux où la topologie est stable et où il n'y a pas de redondance dans les routes

1-6-3-2- Routage Dynamique :

Contrairement au routage statique, Le routage dynamique permet d'éviter le processus fastidieux de configuration de routes statiques. Avec ce type de routage, les routeurs peuvent réagir aux changements survenus sur le réseau et modifient leurs tables de routage sans intervention de la part de l'administrateur réseau. **[12]**

Le routage dynamique utilise des protocoles de routage permettent aux routeurs de découvrir automatiquement les routes disponibles et de mettre à jour leurs tables de routage en fonction des changements dans le réseau.

Les protocoles de routage dynamique couramment utilisés incluent RIP (Routing Information Protocol), OSPF (Open Shortest Path First) et BGP (Border Gateway Protocol).

1-6-3-3- Comparaison entre le routage statique et le routage dynamique

	STATIQUE	DYNAMIQUE
Utilisation	Petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les Routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonction du changement de topologie.
La construction de la table de routage	Les routes sont remplies à la main	Les routes sont remplies dynamiquement dans la table.
Algorithmes de routage	N'utilise pas d'algorithmes de routage complexes.	Utilise des algorithmes de routage complexes pour effectuer des opérations de routage.
Sécurité	Fournit une haute sécurité.	Moins sécurisé en raison de l'envoi de diffusions et de multidiffusions.
Cout	Cout initial faible	Cout initial plus élevé

Tableau 1.6 : comparaison entre routage statique et dynamique

1.6.4 - LES PROTOCOLES DE ROUTAGE

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Les protocoles de routage établissent des règles d'échange entre routeurs pour mettre à jour leurs tables selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit. Ils améliorent ainsi l'efficacité du routage. **[8]**

Les protocoles de routage peuvent être classés en deux catégories principales :

- les protocoles de routage à état de lien (link-state routing protocols) ;
- les protocoles de routage à vecteur de distance (distance-vector routing protocols).

1-6-4-1- les protocoles de routage à vecteur de distance

Les protocoles de routage à vecteur de distance, tels que RIP (Routing Information Protocol) et EIGRP (Enhanced Interior Gateway Routing Protocol), se basent sur la distance (comptage des sauts) pour déterminer les meilleures routes.

Ce protocole s'appuie sur l'algorithme de Ford-Bellman. Les algorithmes de routage à vecteur de distance requièrent que chaque nœud s'échange des informations entre voisins, chaque nœud peut maintenir à jour une table en y ajoutant des informations sur tous ses voisins. Cette table donne la distance à laquelle se trouvent chaque nœud et chaque réseau à atteindre.

1-6-4-2- les protocoles de routage à état de lien

Les protocoles de routage à état de lien, tels qu'OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System), reposent sur la connaissance détaillée de la topologie du réseau.

Il avait au départ pour objectif de pallier les défauts du routage par vecteur de distance. Lorsqu'un routeur démarre, il évalue le coût de chacun de ses liens connectés à d'autres nœuds.

Ces informations sont ensuite diffusées à tous les nœuds du système autonome, et non seulement aux voisins directs. À partir de ces informations complètes, les nœuds peuvent calculer une table de routage indiquant le coût nécessaire pour atteindre chaque destination.

Chaque nœud dispose donc de la topologie complète du réseau et des coûts de chaque lien, ce qui permet de calculer les chemins les plus courts. **[7]**

1.7 – SECURITE DES RESEAUX

1.7.1 – DEFINITION DE LA SECURITE DES RESEAUX

Pendant les premières décennies de leur existence, les réseaux informatiques étaient principalement utilisés par des chercheurs universitaires pour envoyer des e-mails et par des employés d'entreprises pour partager des imprimantes.

Dans ces conditions, la sécurité ne recevait pas beaucoup d'attention. Cependant, maintenant que des millions de citoyens ordinaires utilisent des réseaux pour effectuer des opérations bancaires, des achats et déposer leurs déclarations de revenus, et que de nombreuses vulnérabilités ont été découvertes, la sécurité des réseaux est devenue un problème d'ampleur massive. **[1]**

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. **[13]**

1.7.2 - OBJECTIFS DE LA SECURITE INFORMATIQUE

La sécurité est un sujet vaste et couvre de nombreux problèmes. Dans sa forme la plus simple, elle vise à :

- ⇨ S'assurer que les personnes curieuses ne peuvent pas lire, ou pire encore, modifier secrètement des messages destinés à d'autres destinataires.
- ⇨ Elle concerne les personnes qui tentent d'accéder à des services distants auxquels elles ne sont pas autorisées à utiliser.
- ⇨ Elle traite également des moyens de déterminer si ce message prétendument envoyé par l'IRS ("Payez avant vendredi, sinon...") provient réellement de l'IRS et non de la Mafia.
- ⇨ La sécurité traite également des problèmes de capture et de relecture de messages légitimes, ainsi que des personnes qui tentent ensuite de nier qu'elles ont envoyé certains messages. **[1]**

1.7.3 - SERVICES PRINCIPAUX DE LA SECURITE RESEAU

Les problèmes de sécurité des réseaux peuvent être divisés en quatre domaines étroitement liés :

- ❖ **La confidentialité** : également appelée confidentialité, concerne le fait de garder les informations hors des mains des utilisateurs non autorisés. C'est ce à quoi les gens pensent généralement lorsqu'ils envisagent la sécurité des réseaux.
- ❖ **L'authentification** : concerne la détermination de l'identité de la personne avec qui vous communiquez avant de divulguer des informations sensibles ou de conclure une transaction commerciale.
- ❖ **La non-répudiation** : concerne les signatures : comment prouver que votre client a réellement passé une commande électronique de dix millions de "doohickeys" gauchers à 89 cents chacun lorsqu'il prétend plus tard que le prix était de 69 cents ? Ou peut-être prétend-il n'avoir passé aucune commande du tout.
- ❖ **le contrôle de l'intégrité** : concerne la manière dont vous pouvez être sûr qu'un message que vous avez reçu est réellement celui qui a été envoyé et non quelque chose qu'un adversaire malveillant a modifiée en transit ou inventé.
- ❖ **La disponibilité** : Permettant de maintenir le bon fonctionnement du système informatique. **[1]**

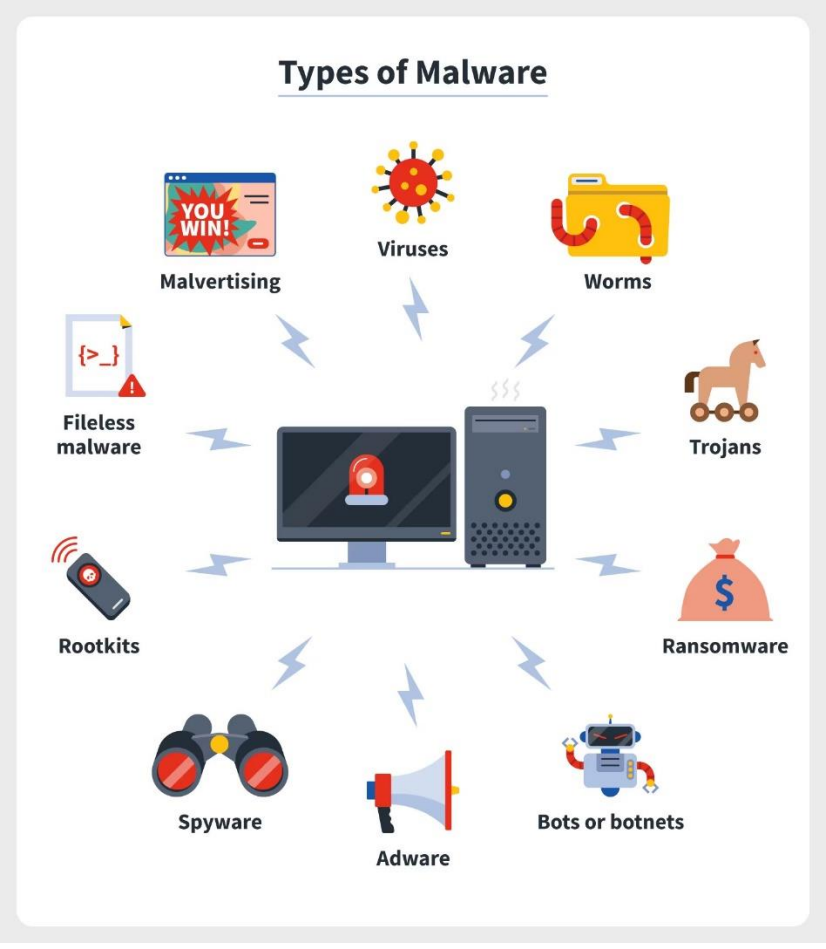
1.7.4 - LES MENACES DE SECURITE LES PLUS COURANTES POUR LES RESEAUX

Voici un tableau récapitulatif et non exhaustif des menaces de sécurité les plus courantes pour les réseaux :

Menace de sécurité	Description
Malwares	Logiciels malveillants conçus pour causer des dommages ou voler des informations sensibles.
Attaques par déni de service (DDoS)	Inondation d'un réseau ou d'un service avec un trafic excessif pour le rendre indisponible aux utilisateurs légitimes.
Attaques de phishing	Techniques de manipulation pour obtenir des informations confidentielles en se faisant passer pour une entité de confiance.
Attaques de force brute	Essai systématique de toutes les combinaisons possibles pour accéder à un compte ou un système.
Attaques d'injection	Injection de code malveillant dans des applications web pour exploiter leurs vulnérabilités et accéder à des données sensibles.
Attaques de l'homme du milieu	Interception et manipulation des communications entre deux parties pour accéder à des informations ou les altérer.
Espionnage et interception	Interception des communications pour accéder à des informations confidentielles ou sensibles.
Vulnérabilités des logiciels	Exploitation de failles dans les logiciels utilisés sur les réseaux pour compromettre la sécurité du système.

Tableau 1.7 : Les menaces de sécurité les plus courante [14]

La figure ci-dessous illustre les différents types de menaces les plus courantes :



1-7-5- LES METHODES DE PROTECTION DES RESEAUX

Le tableau 1.8 nous donne les différentes méthodes de protection des réseaux.

Méthode de protection	Description
Pare-feu (Firewall)	Un pare-feu est un dispositif de sécurité qui contrôle le trafic réseau entre un réseau interne et un réseau externe. Il filtre les paquets en fonction de règles prédéfinies pour prévenir les accès non autorisés et les attaques.
Systèmes de détection d'intrusion (IDS)	Les IDS surveillent le trafic réseau pour détecter des comportements suspects ou des activités malveillantes. Ils signalent les tentatives d'intrusion ou les violations de sécurité pour une réponse rapide.
Systèmes de prévention d'intrusion (IPS)	Les IPS sont similaires aux IDS, mais ils sont capables de prendre des mesures automatiques pour bloquer ou prévenir les attaques détectées. Ils réagissent en temps réel pour protéger le réseau
VPN (Virtual Private Network)	Un VPN établit une connexion sécurisée entre des sites distants ou des utilisateurs à distance et le réseau interne. Il utilise des protocoles de chiffrement pour garantir la confidentialité et l'intégrité des données.
Cryptographie	Le mot cryptographie est un terme générique désignant l'ensemble de techniques permettant de chiffrer des messages. Chiffrer un message consiste à le transformer au moyen d'un algorithme mathématique afin de le rendre inintelligible. sauf pour celui qui possède le moyen (une clé) de le déchiffrer
Gestion des identités et des accès (IAM)	L'IAM gère les identités des utilisateurs, leurs droits d'accès et les autorisations associées. Il garantit que seules les personnes autorisées peuvent accéder aux ressources réseau et aux données sensibles
Sécurité physique	La sécurité physique comprend des mesures telles que la surveillance vidéo, les systèmes de contrôle d'accès et la protection des équipements réseau contre le vol ou les dommages physiques
Mot de passe	Une personne peut être authentifiée par une combinaison d'une identification et d'un mot de passe, (code secret personnel).Le mot de passe doit posséder certaines caractéristiques qui sont : non trivial, difficile à deviner, régulièrement modifié. Cependant si l'attaquant accède au fichier de mot de passe, il pourra s'introduire dans le système sécurisé

***Tableau 1.8 : Les méthodes de protection* (15)**

1.8 – CONCLUSION

En conclusion, Ce chapitre a donc fourni une introduction complète et cohérente aux fondamentaux des réseaux informatiques.

Les connaissances acquises ici seront essentielles pour la suite de ce mémoire, où nous aborderons des sujets plus avancés et spécifiques liés à la conception d'un raccordement sans fil des objets connectés d'une université intelligente.

CHAPITRE 2

NOTIONS DE BASE SUR L'INTERNET DES OBJETS

2.1 – INTRODUCTION A L'IOT

Le développement rapide des technologies de l'information a conduit à une évolution majeure dans le domaine de la connectivité et de l'intercommunication.

L'Internet des Objets (IoT) est l'un des domaines les plus dynamiques et prometteurs de cette évolution. L'IoT est en train de transformer la manière dont nous interagissons avec le monde qui nous entoure, offrant de nouvelles opportunités pour améliorer l'efficacité, la sécurité et la qualité de vie. Ce chapitre se concentre sur l'IoT, en explorant sa définition, son histoire, ses avantages et ses inconvénients, ainsi que les technologies sous-jacentes, les réseaux, les applications et les enjeux associés.

2.1.1 – DEFINITION DE L'IOT

L'Internet des objets (IoT) est un système interconnecté d'objets physiques, d'appareils, de véhicules, de bâtiments et d'autres éléments intégrant des capteurs, des logiciels et des réseaux pour collecter et échanger des données.

Tous appareils doivent avoir des identifiants uniques et utiliser des technologies intégrées pour détecter et collecter des données sur eux-mêmes et sur leur environnement et transférer ces données à d'autres appareils ou à d'autres systèmes. Ces objets sont capables de communiquer entre eux et avec les systèmes informatiques sans intervention humaine directe, permettant ainsi de fournir des informations en temps réel pour la prise de décision.

2.1.2 – HISTOIRE DE L'IOT

Le premier « objet » connecté à Internet remonte à 1982 : il s'agissait d'un distributeur de boissons installé à l'université Carnegie-Mellon de Pittsburgh, en Pennsylvanie, qui indiquait le niveau de remplissage de l'appareil et la température des boissons.

L'histoire s'est ensuite accélérée. L'Internet des objets a enregistré une croissance exponentielle. En 2008-2009, le nombre d'objets connectés à Internet dépassait pour la première fois la population mondiale.

On compte aujourd'hui quelque 15 milliards d'appareils connectés, qu'il s'agisse de capteurs, d'appareils ménagers, de machines, d'éoliennes, de dispositifs médicaux ou de voitures.

Ce chiffre devrait continuer à augmenter, il va dépasser les 27 milliards d'objets en 2030, passant d'une valeur estimée à 248 milliards de dollars en 2020 à près de 1 600 milliards en 2025. **[31]**

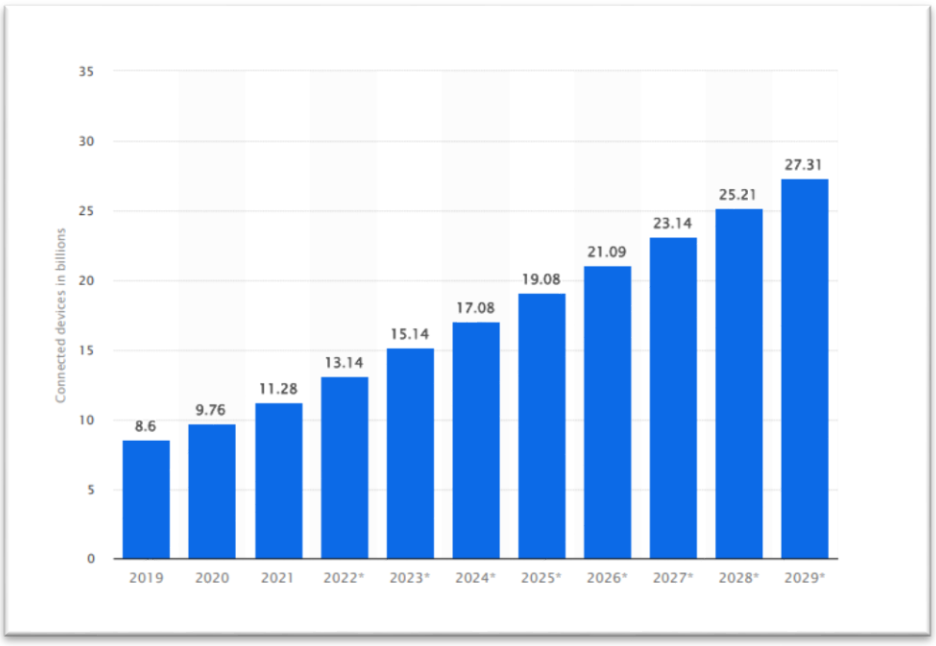


Figure 2.1 : Nombre d'appareils connectés à l'internet des objets (IoT) dans le monde de 2019 à 2021 avec des prévisions de 2022 à 2030 [16]

2.1.3 – LES AVANTAGES & LES INCONVENIANTS DE L'IOT

La figure 2.2 montre les avantages et les inconvénients de l'IoT :

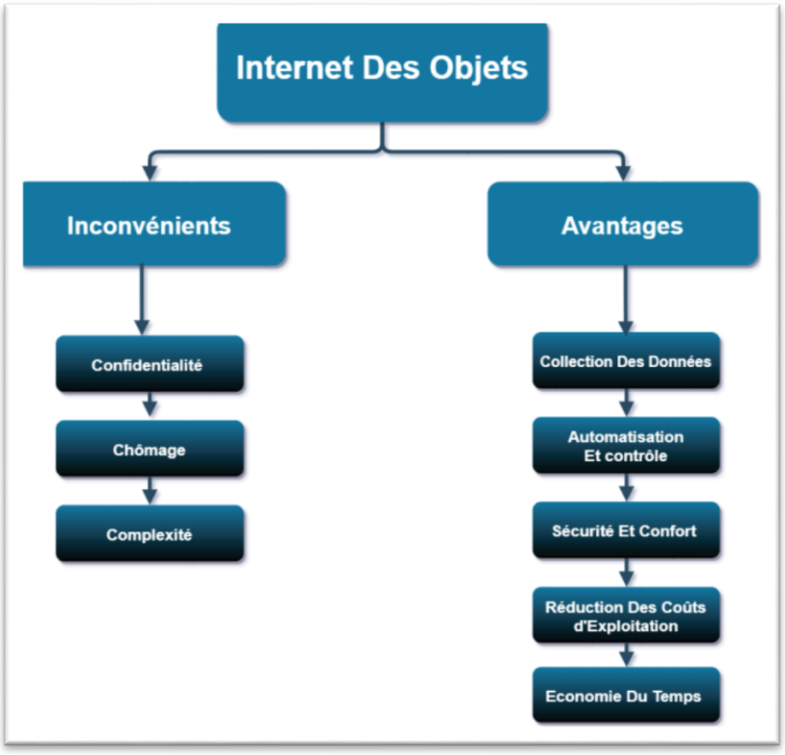


Figure 2.2 : Diagramme des avantages et des inconvénients [17]

2.1.3.1 Avantages

2.1.3.1.1 - collection des données

Plus d'informations sur les processus de travail/d'opération et des ensembles de données riches obtenues à partir de capteurs connectés conduisent à l'optimisation des processus.

L'IoT permet un partage de données important, et la manipulation de ces données selon les besoins aide les systèmes à fonctionner plus efficacement et à prendre des décisions plus intelligentes et informées en temps réel.

2.1.3.1.2 - Automatisation et contrôle

L'internet des objets permet de connecter et de contrôler numériquement Les objets physiques, ce qui nécessite une automatisation et un contrôle importants au sein du réseau.

Sans intervention humaine, les machines communiquent entre elles, ce qui permet de gagner du temps.

L'automatisation garantit également l'exécution uniforme des tâches et la qualité des services fournis. L'intervention humaine ne peut être requise qu'en cas d'urgence.

2.1.3.1.3 - Economie du Temps

L'intégration de l'IOT peut permettre de gagner beaucoup de temps, ce qui est précieux pour tout le monde.

2.1.3.1.4 - La sécurité et le confort

L'utilisation de la technologie IoT dans la surveillance peut aider à améliorer les normes de sécurité dans l'organisation et également à détecter toute activité suspecte.

Dans l'organisation, il peut être utile de suivre les activités d'un employé, peut être utilisé pour maintenir son dossier quotidien.

Il peut être difficile d'imaginer que la gestion et la surveillance des environnements dangereux nécessitant la prise en compte de multiples facteurs, notamment la sécurité des personnes et l'optimisation de l'environnement pour la productivité et le confort.

2.1.3.1.5 - Réduction des coûts d'exploitation

Le plus grand avantage de l'IoT est le montant de l'argent économisé, moins d'erreurs, la fidélisation des employés, l'amélioration des processus et l'efficacité énergétique sont autant des éléments qui permettent de réduire les coûts.

L'IoT sera plus largement utilisé tant que le coût des équipements de surveillance est inférieur aux économies potentielles.

L'intégration de l'IOT s'avère très utile dans la vie quotidienne, car les appareils communiquent entre eux, ce qui permet d'économiser de l'énergie et de réduire les coûts.

2. 1.3.2 - Inconvénients

2.1.3.2.1 - La confidentialité

Avec l'avancement de la technologie et des médias sociaux, les données des utilisateurs sont toujours disponibles sur Internet et avec les choses connectées à Internet, les pirates disposent d'un autre outil pour pouvoir pénétrer le réseau et voler les informations.

On peut vouloir un espace personnel dans la vie, il n'est donc pas facile de toujours rester connecté avec sa famille et ses amis et de leur donner tous les aspects de notre vie.

Il y a toutes les chances que vos données soient utilisées à mauvais escient.

2.1.3.2.2 - Chômage

De plus en plus d'appareils interconnectés entre eux et à Internet entraîneront une diminution des besoins en main-d'œuvre et, éventuellement, des pertes d'emplois. L'IoT et l'IA favoriseront l'automatisation de chaque travail nécessitant de la main-d'œuvre. Des tâches comme le support client sont déjà automatisées et la plupart du travail est effectué par des chatbots.

L'automatisation aura un impact dévastateur sur les travailleurs peu et moyennement qualifiés.

2.1.3.2.3 - Complexité

Les systèmes IoT peuvent être complexes à déployer, à configurer et à maintenir, nécessitant des compétences techniques et une gestion appropriée.

2.2 – LES TECHNOLOGIES DE L'IOT

2.2.1 – LES COMPOSANTS D'UN OBJET CONNECTE

Un objet connecté est un objet qui possède la capacité d'échanger des données avec d'autres entités physiques ou numériques, le plus souvent au travers d'internet.

La figure ci-dessous nous montre les différents composants d'un objet connecté :

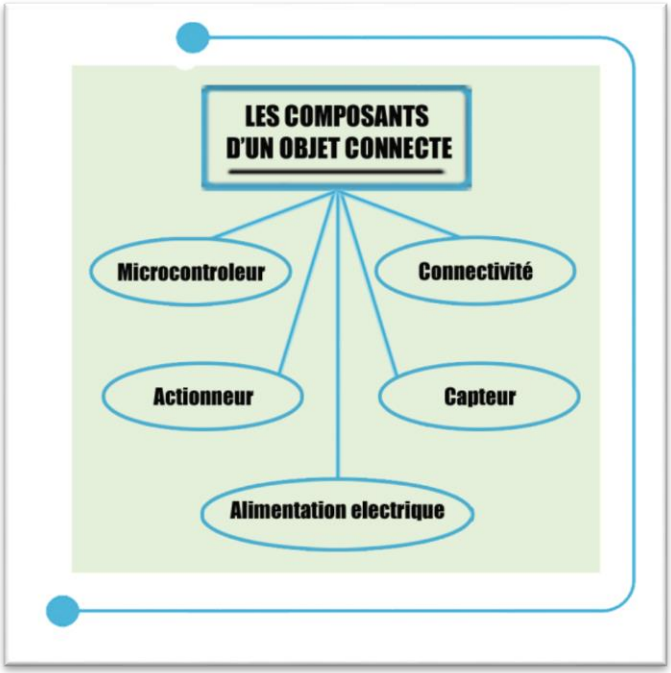


Figure 2.3 : les composant d'un objet connecter

2.2.1.1 - Le microcontrôleur

Utilisée pour obtenir des données et traiter et analyser les informations des capteurs, synchronise les signaux de commande de l'actionneur et contrôle les fonctions des objets intelligents comme les systèmes d'alimentation et de communication. Le microcontrôleur est utilisée dans les objets IoT en raison de sa petite taille, facile à Programmé, flexible, économe en énergie et à faible coût. **[16]**

Figure 2.3 : Schéma fonctionnel des objets intelligents typiques (smart objet) dans l'IOT **[32]**

2.2.1.2 - Le capteur

Le capteur est le composant qui transforme une information physique (température, pression, débit...) en un signal électronique. Il en existe plusieurs types selon l'information que l'on souhaite récupérer.

2.2.1.3 - L'actionneur

L'actionneur est chargé d'utiliser l'énergie pour produire du mouvement. Il transforme les signaux électriques en mouvements physiques. Les capteurs et les actionneurs sont des transducteurs qui convertissent une forme d'énergie à l'autre.

L'échange de données est le facteur clé le plus important dans l'IoT. D'où les capteurs et les actionneurs jouent ici un rôle essentiel

2.2.1.4 - L'alimentation électrique

Tous les objets intelligents contiennent des éléments qui nécessitent de l'énergie.

Les possibilités d'alimentation électrique d'un objet connecté font partie des conditions prépondérantes dans le choix de la solution IoT.

Selon qu'une alimentation électrique continue soit possible ou bien qu'une batterie soit nécessaire, cela impacte le choix de la connectivité de la masse et de la fréquence de données pouvant être remontées. **[33]**

2.2.1.5 - Connectivité

Le capteur envoie un signal décodé par le micro-ordinateur, que l'on doit maintenant envoyer sur le réseau pour que les données soient récupérées et analysées à distance. C'est le rôle du module de connectivité, la voie du dispositif.

Selon la connectivité choisie, le module de connectivité prendra des formes différentes. Il peut faire partie intégrante du micro-ordinateur (soudé dans la carte) ou prendre la forme d'un module séparé relié par un câble. Par exemple, un module Wifi peut être directement intégré dans la carte mère du micro-ordinateur ou bien prendre la forme d'une antenne déportée. **[33]**

2.2.2 – LES RESEAUX D'IOT

La différence entre un objet quelconque et un objet connecté repose sur la connectivité de ce dernier. Pour connecter un objet à Internet, il existe plusieurs possibilités :

- le **Wifi**
- le **Bluetooth**
- le **réseau cellulaire (3G, 4G)**

Ce sont des modes de connexion extrêmement répandus et grand public.

Toutefois, certaines technologies comme le **LPWAN** ont été développées spécifiquement pour connecter les objets connectés. Elles ont pour but de minimiser la consommation énergétique, de maximiser la portée et de s'adapter au volume de données échangées.

Le diagramme de la figure 2.4 montre les différents types de réseaux IoT :

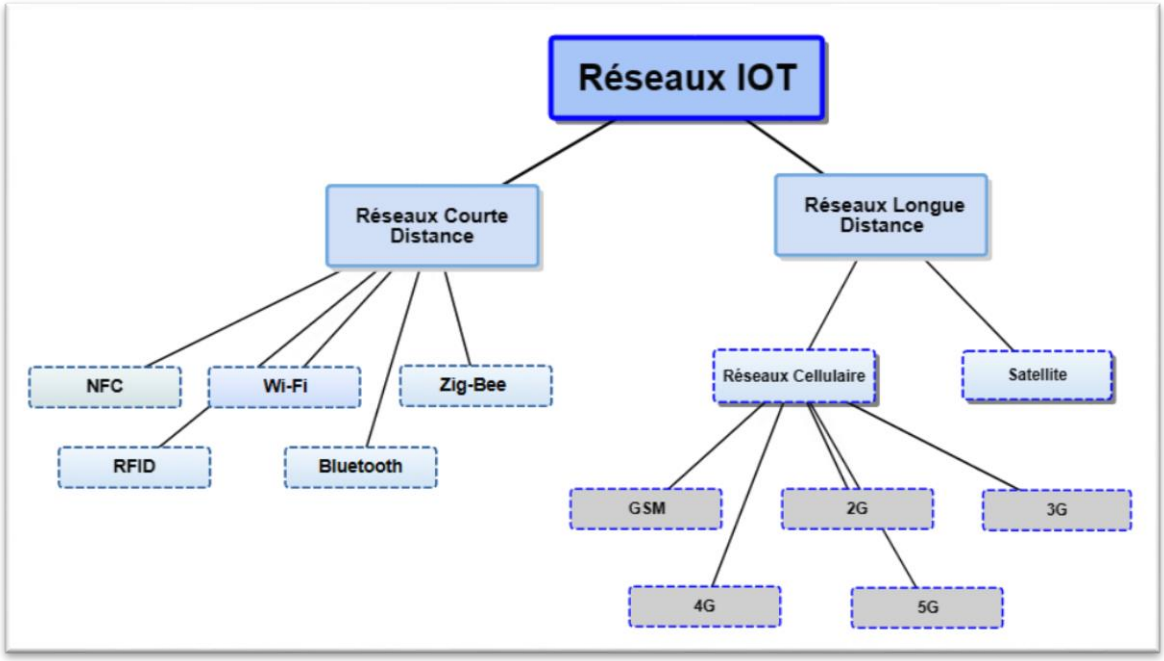


Figure 2.4 : Diagramme des types de réseaux IoT

2.2.2.1 - Les réseaux IoT courte distance

2.2.2.1.1 -Bluetooth

La technologie sans fil Bluetooth est une technologie radio peu coûteuse à courte portée qui élimine le besoin de câblage propriétaire entre des appareils tels que les ordinateurs portables, les ordinateurs de poche, les appareils photo et les imprimantes et une portée effective de 10 à 100 mètres. Et communiquent généralement à moins de 1 Mbps et Bluetooth utilise la spécification de la norme IEEE 802.15.1.

Au début, en 1994, la société Ericsson Mobile Communication a lancé un projet appelé «Bluetooth». Il est utilisé pour la création de réseaux personnels (PAN). Un ensemble d'appareils Bluetooth partageant un canal commun de communication est appelé Pico-net.

Figure 2.5 : Logo Bluetooth [34]

Ce Pico-net est capable de 2 à 8 appareils à la fois pour le partage de données, et ces données peuvent être du texte, de l'image, de la vidéo et du son. Le groupe d'intérêt spécial Bluetooth comprend plus de 1000 entreprises avec Intel, Cisco, HP, Aruba, Intel, Ericsson, IBM, Motorola et Toshiba. **[18]**

2.2.2.1.2 - Zigbee

ZigBee est une technologie sans fil basé sur la norme de protocole de communication IEEE 802.15.4 et est utilisé pour les réseaux personnels ou PAN. La norme IEEE 802.15.4 a des couches MAC et physiques de faible puissance. Zigbee a été développé par l'alliance Zigbee, qui travaille pour des solutions de communication fiables, à faible consommation d'énergie et bon marché. La portée de communication des appareils Zigbee est très petite (10 à 100 mètres).

Il existe trois types d'appareils dans un réseau Zigbee:

- FFD (Fully Functional Device),
- RFD (Reduced Functional Device)
- et un coordinateur Zigbee

Un nœud FFD peut également jouer le rôle de routeur. Zigbee prend en charge les topologies en étoile, en arbre et en maillage.

***Figure 2.6 : Zigbee Logo** [32]*

Le schéma de routage dépend de la topologie. Les autres fonctionnalités de Zigbee sont la découverte et la maintenance des routes, la prise en charge des nœuds rejoignant / quittant le réseau, les adresses 16 bits courtes et le routage multi-sauts. **[19]**

2.2.2.1.3 -Wifi

Le Wifi est une technologie de connectivité de réseau utilisée pour le transfert de données à haut débit sur de courtes distances en utilisant des dispositifs basés sur les ondes radio (routeur, ordinateur portable, Smartphones, etc.) Ces dispositifs sont basés sur les normes IEEE 802.11 de 1997. Les différents types des normes de Wifi sont utilisés par les appareils basés sur les ondes. Ces normes sont 802.11a, 802.11b, 80.2.11 g et 802.11n. Aujourd'hui, cette connectivité sans fil est un fait partie intégrante de la vie quotidienne. Tous les appareils intelligents comme les Smartphones, les ordinateurs portables, les tablettes.

Figure 2.7 : Logo Wifi [32]

Les appareils photo et bien d'autres dispositifs sont utilisés pour la connectivité Wifi. En raison du haut débit, par sa nature, le transfert de données, la technologie Wifi est très bien acceptée par les hôtels, les foyers, les aéroports et les cafés de la société en utilisant des points d'accès sans fil. **[20]**

2.2.2.1.4 - RFID

L'identification par radiofréquence, également connue sous le nom de RFID, désigne à une technologie permettant d'identifier et de suivre automatiquement les étiquettes attachées à des objets. Un système RFID est généralement constitué d'une étiquette (ou un label) et un lecteur. Les étiquettes ou étiquettes RFID sont intégré avec un émetteur et un récepteur.

La RFID sur les étiquettes a deux parties :

- une micro-puce qui stocke et traite l'information
- et une antenne pour recevoir et transmettre un signal

La figure 2.8 illustre les principes de fonctionnement de la technologie RFID. Pour lire les informations encodées sur une étiquette, le lecteur émet un signal à l'étiquette à l'aide d'une antenne. L'étiquette répond avec le des informations écrites dans sa banque de mémoire. L'interrogateur puis transmettre les résultats de la lecture à un programme informatique RFID. **[21]**

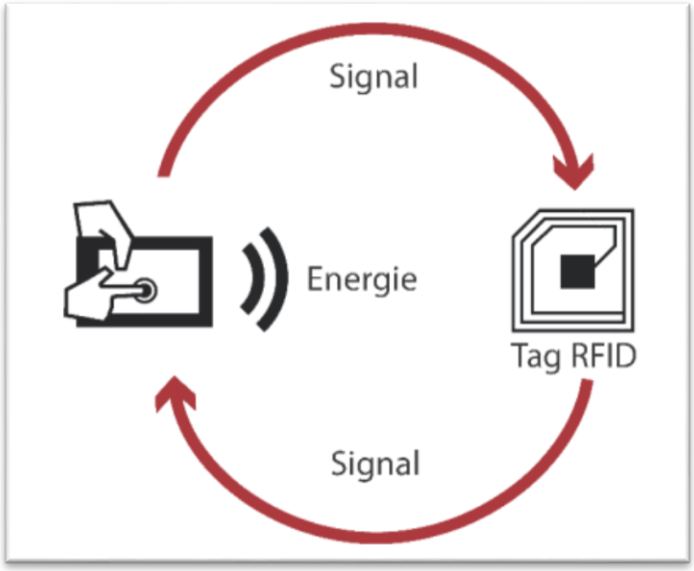


Figure 2.8 : Principes de fonctionnement de la technologie RFID

2.2.2.1.5 - NFC (Communication en champ proche)

La communication en champ proche (NFC) est un ensemble de normes pour les téléphones intelligents et les appareils mobiles similaires afin d'établir la communication entre eux en les touchant ensemble ou en les réunissant sur quelques centimètres.

NFC peuvent être utilisés dans les systèmes de paiement sans contact, similaires à celles utilisées actuellement dans les cartes de crédit et les cartes à puce pour les billets électroniques, et permettent le paiement mobile remplacer ou compléter ces systèmes.

Le système d'exploitation mobile Androïde Beam utilise la NFC pour réaliser les étapes de permettre, coupler et établir une connexion Bluetooth lors d'un transfert de fichiers. **[22]**

***Figure 2.9 : Logo NFC* (35)**

Le Tableau 2.1 montre la Comparaison entre les technologies de communication en IOT

	Courte portée			***Moyenne portée***		
Technologie	**NFC**	**Bluetooth**	**ZigBee**	**Z-Wave**	Wifi	BLE
Portée moyenne (En intérieur)	< 10 cm	10 m	10 m	50 m	50 m	50 m
Débit (Mbit/s)	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-2}$	$1*10^{-2}$	$1*10^{-2}$	$1*10^{-3}$
Autonomie	mois	jours	années	années	jours	mois
Fréquence	2.4 GHz	2.4 GHz	2.4 GHz 868 MHz	868 MHz	2.4 GHz 5 GHz	2.4 GHz
Usages	Téléphonie Cartes de payement	Périphériques informatiques et multimédia	Domotique		Navigation Internet Transfert important de données	Périphériques informatiques et multimédia

Tableau 2.1 : Comparaison entre les technologies de communication en IOT

2.2.2.2 - Les réseaux IoT longue distance

2.2.2.2.1 – Les Réseaux cellulaires

La technologie qui équipe nos téléphones portables depuis 30 ans. Plusieurs générations se sont succédé :

- **GSM** : supportant uniquement les appels et SMS
- **2G** : rendant possible l'envoi de MMS
- **3G** : initiant l'utilisation de l'Internet mobile
- **4G** : permettant le haut débit sur mobile, par exemple le streaming vidéo HD)
- **5G** en cours de commercialisation (particulièrement adapté à l'IoT très gourmand en data, comme les voitures autonomes).

Pour connecter votre objet au réseau cellulaire, il faut l'équiper, comme un téléphone, d'une carte SIM. Cependant, les cartes SIM M2M ne sont pas celles vendues pour le grand public.

Elles sont appelées cartes **M2M** (machine to machine).

Elles ont plusieurs spécificités, par exemple de pouvoir résister à des températures extrêmes. **[33]**

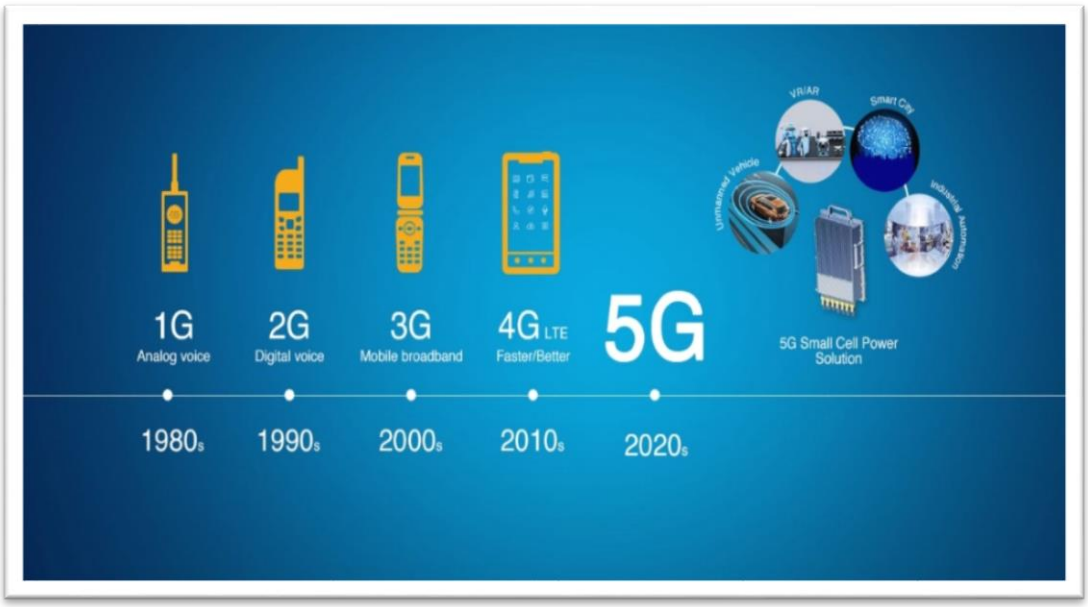


Figure 2.50 : Evolution des Générations mobiles **[36]**

2.2.2.2.2 - Satellite

Le réseau satellite reste encore l'unique solution pour les **zones reculées** (haute mer, désert, haute montagne), où il n'y a aucune alternative.

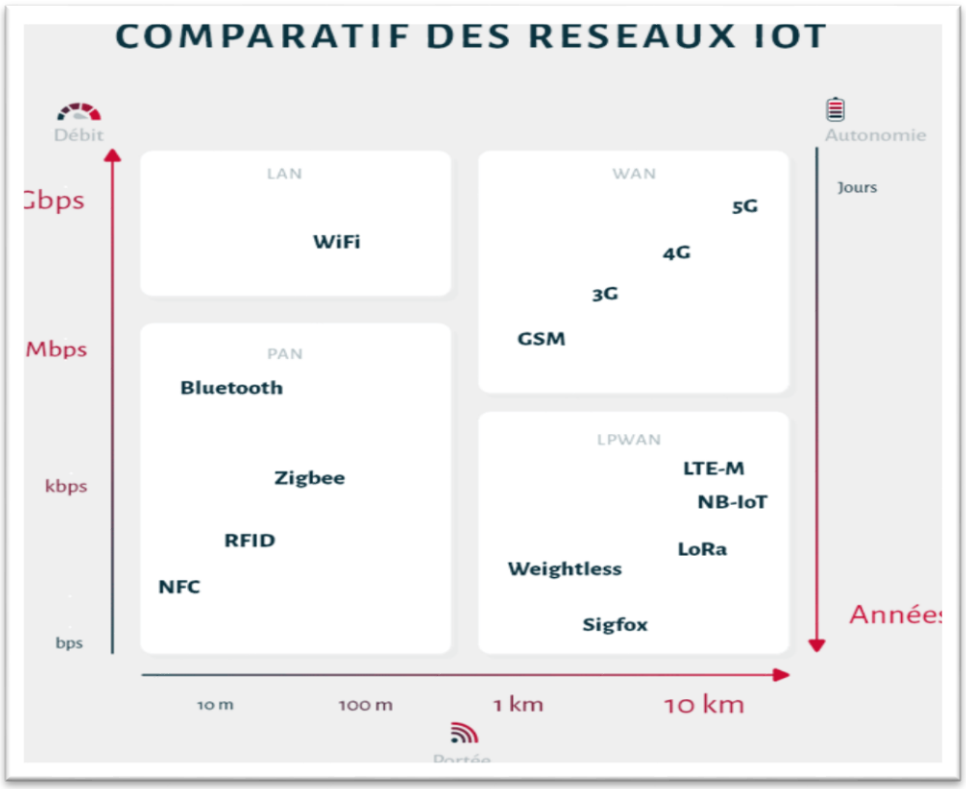


Figure 2.11 : schéma Comparatif des réseaux IoT

Les entreprises communément appelées du *New Space* (Space X, Blue Origin…) développent des projets de constellations qui ont pour but de connecter toute la planète à un réseau Internet haut débit.

Si la disponibilité commerciale de ce projet prend plusieurs années, la principale conséquence est d'avoir considérablement abaissé le prix du lancement de satellites, avec une répercussion sur le prix des services associés.

2.2.2.2.3 -Les avantages d'utilisation du réseau cellulaire pour l'IoT

Les antennes sont déjà installées et dense, la couverture d'une antenne s'étend sur plusieurs dizaines de kilomètres et la configuration est minimale.

La part de la connectivité dans le coût de l'IoT est beaucoup plus faible que pour d'autres technologies. L'utilisation du réseau cellulaire par L'IOT est limitée par le fait qu'il est gourmand en énergie.

Le choix du cellulaire est moins évident dans des zones sans accès au réseau électrique. Les robots agricoles sont équipés de cartes M2M pour pouvoir circuler à travers plusieurs hectares tout en restant connectés.

Leur autonomie dure jusqu'à 10 heures et ils sont rechargés la nuit. Il ne s'agit donc pas d'avoir un branchement électrique continu mais un accès régulier à une recharge.

Enfin, le cellulaire est un mode de connectivité beaucoup plus sécurisé. C'est donc une solution particulièrement adaptée aux services publics, comme la connexion de bornes de vélos en libre-service ou encore dans le domaine de la santé et de la sécurité. **[33]**

2.3 - LES APPLICATIONS DE L'IOT

2.3.1 –TRANSPORT

Dans le domaine de la conduite assistée, les véhicules intelligents, à détection et interconnectés et les routes pourraient minimiser les risques de collision et permettre une planification plus fluide du trafic et le flux. L'IOT dans les transports permettra un contrôle dynamique de l'itinéraire origine-destination.

***Figure 2.12 : IoT Transportation*(37)**

Le comportement de choix pour un flux de circulation optimal dans une zone. Il est également probable que Les solutions de type IOT remplaceront les systèmes de capteurs existants dans les centres de contrôle de la lumière les carrefours.

À l'heure actuelle, la solution standard consiste à utiliser des boucles inductives des détecteurs de véhicules qui suivent le trafic en approche et transmettent uniquement les données au feu le plus proche par communication filaire.

Les données échangées entre tous les carrefours dans une zone pourraient permettre de meilleures décisions et réduire les embouteillages. **[38]**

2.3.2 – VILLES INTELLIGENTES

L'inclusion de l'IOT modifie systématiquement l'intelligence des villes en prenant en compte de nombreux paramètres comme espace de surveillance pour le stationnement des véhicules, la surveillance et la détection des vibrations dans les bâtiments et les ponts, l'observation du volume sonore dans les zones sensibles, contrôler intelligemment l'éclairage public en fonction des conditions météorologiques, détection des déchets et de collecte des déchets, en indiquant les messages d'alerte en vue les conditions météorologiques inconditionnelles, les embouteillages ou les accidents. **[23]**

2.3.3 - L'ENERGIE

L'introduction de la solution IoT au cœur du domaine de l'énergie mènera certainement à son développement et à sa prospérité, et cela grâce aux nouvelles techniques et méthodes qui ont contribuées à la réalisation de différents projets pour l'intérêt des institutions et les individus à la fois.

Ces projets permettent de profiter pleinement de l'énergie renouvelable surtout l'énergie solaire qui a devenu avec la solution IoT un grand générateur d'électricité.

La solution IoT intégrée permet aussi de collecter instantanément toutes les informations liées au réseau énergétique commençant par sa mise en œuvre, son fonctionnement et finalement son contrôle et entretient mais cette fois-ci avec un usage intelligent

2.3.4 – LA SANTE

L'inclusion de l'IOT dans la gestion des soins de santé offre de nombreux avantages :

- Ce sont des entretiens électroniques complets et corrects sur les témoignages des patients.
- Le suivi et la reconnaissance des patients pour faire progresser le flux de travail des hôpitaux ;
- L'identification et l'authentification des patients afin de réduire les incidents préjudiciables aux patients individuels ;
- La collecte automatique de données et la transformation des données vers d'autres hôpitaux, ce qui réduit l'audit des temps de traitement et des procédures ;
- Les capteurs qui permettent de transférer les soins de santé à un autre niveau, où des capteurs sont intégrés au corps du patient pour assurer un suivi en temps réel sur l'état de santé des patients, en plus d'alerter sur le comportement des patients ;

- Les capteurs intelligents, tels que les ganglions, surveillent avec précision la pression artérielle, le rythme cardiaque, la température corporelle et le taux de glycémie, etc... **[23]**

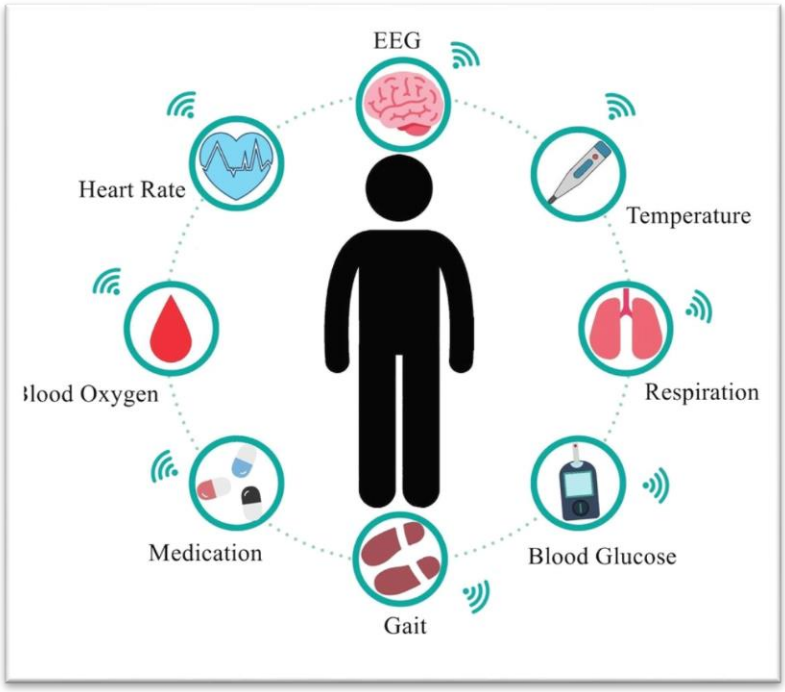


Figure 2.14 : Un réseau IOT médical

2.3.5 - L'AGRICULTURE

L'agriculture avec l'IOT renforce le travail et la productivité de l'agriculture déposée un contrôle approfondi de la température, de l'humidité et de la quantité de vitamines de produit.

Examiner les conditions météorologiques dans les champs pour prévoir la pluie, la neige et le vent changements.

L'IOT en matière d'approvisionnement en eau examine l'état de l'eau des rivières et de la mer pour déterminer s'il est utilisable à des fins de boisson ou d'agriculture. Détection des variations de pression dans l'alimentation des tuyaux, les niveaux d'eau des réservoirs et des rivières, les barrages**(23)**.

Il existe des projets qui tentent de surveiller les paramètres associés aux plantes et aux cultures tels que le niveau d'humidité, l'humidité, la température, etc. et de les télécharger dans une base de données cloud et en outre d'alerter et de mettre à jour les données au propriétaire de la plantation à ce sujet.

La figure ci-dessous nous résume comment se fait le Système de surveillance d'une ferme à distance.

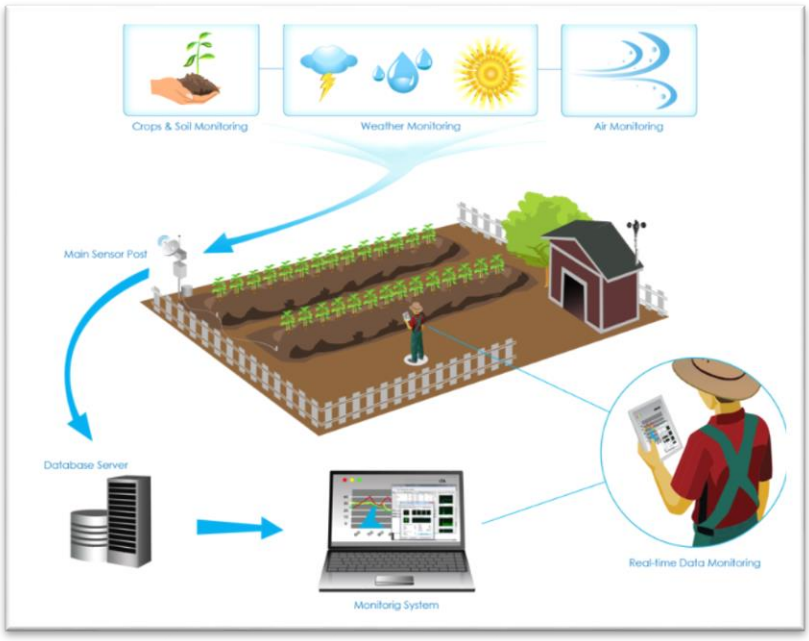


Figure 2.15 : Système de surveillance d'une ferme à distance [39]

2.4 –LES PROTOCOLE DE L'IOT

Les appareils IoT communiquent à l'aide des protocoles IoT. Le protocole IP (Internet Protocol) est un ensemble de règles qui détermine la façon dont les données sont envoyées à Internet.

Les protocoles IoT garantissent que les informations d'un appareil ou d'un capteur seront lisibles et compréhensibles par un autre appareil, une passerelle, un service. Différents protocoles IoT ont été conçus et optimisés pour différents scénarios et utilisations.

Compte tenu de la diversité des appareils IoT disponibles, il est important d'utiliser le bon protocole dans le bon contexte.

2.4.1 – LA COUCHE APPLICATION

La couche Application sert d'interface entre l'utilisateur et l'appareil avec un protocole IoT donné.

2.4.1.1 - AMQP (Advanced Message Queuing Protocol)

Est une couche logicielle qui assure l'interopérabilité entre les différents logiciels de messagerie est appelée "middleware". Cette couche permet à un large éventail de systèmes et d'applications de travailler ensemble, créant ainsi une messagerie normalisée à l'échelle industrielle.

2.4.1.2 - CoAP (Constrained Application Protocol)

Protocole optimisé pour les bandes passantes et réseaux contraints, et conçu pour les appareils dont la capacité de connexion est limitée dans le cadre d'une communication machine à machine.

CoAP est également un protocole de transfert de documents qui s'exécute sur le protocole UDP (User Datagram Protocol).

2.4.1.3 - DDS (Data Distribution Service)

Protocole de communication pair à pair polyvalent qui fait tout, de l'exécution de petits appareils à la connexion de réseaux hauts performances. DDS rationalise le déploiement, renforce la fiabilité et réduit la complexité.

2.4.1.4 -MQTT (Message Queue Telemetry Transport)

Protocole de messagerie conçu pour une communication machine à machine légère, et principalement utilisé pour les connexions à faible bande passante vers des emplacements distants. MQTT utilise un modèle éditeur-abonné et est idéal pour les petits appareils qui nécessitent une utilisation efficace de la bande passante et de la batterie.

2.4.2 – LA COUCHE TRANSPORT

Dans un protocole IoT, la couche Transport permet la communication et protège les données lorsqu'elles circulent entre les couches.

2.4.2.1 - TCP (Transmission Control Protocol)

Protocole utilisé pour la majorité des connexions Internet. Il offre une communication d'hôte à hôte, en divisant de grands ensembles de données en paquets individuels, et en renvoyant et réassemblant les paquets en fonction des besoins.

2.4.2.2 - UDP (User Datagram Protocol)

Protocole de communication qui permet la communication entre processus et s'exécute sur IP. UDP améliore les taux de transfert de données sur TCP et répond aux exigences des applications qui ont besoin d'une transmission de données sans perte.

2.4.3 – LA COUCHE RESEAU

La couche Réseau d'un protocole IoT permet à des appareils individuels de communiquer avec le routeur.

2.4.3.1 -IP (internet protocole)

De nombreux protocoles IoT utilisent IPv4, tandis que les exécutions plus récentes utilisent IPv6. Cette récente mise à jour du protocole IP achemine le trafic sur Internet, et identifie et localise les appareils sur le réseau.

2.4.3.2 - 6LoWPAN

Ce protocole IoT fonctionne mieux avec les appareils de faible puissance qui ont des capacités de traitement limitées.

2.4.4 – LA COUCHE LIAISON DES DONNEES

La couche Données fait partie d'un protocole IoT qui transfère les données au sein de l'architecture système, en identifiant et en corrigeant les erreurs trouvées dans la couche physique.

2.4.4.1 - IEEE 802.15.4

Norme radio relative aux connexions sans fil à faible consommation. Elle est utilisée avec ZigBee, 6LoWPAN et d'autres normes pour créer des réseaux sans fil incorporés.

2.4.4.2 - Liaison sans fil à faible consommation énergétique (LPWAN)

Les réseaux étendus à basse consommation (LPWAN) permettent la communication sur des distances de 500 mètres à plus de 10 kilomètres à certains endroits. LoRaWAN est un exemple de LPWAN optimisé pour une faible consommation d'énergie.

2.4.5 – LA COUCHE PHYSIQUE

La couche physique constitue un canal de communication entre des appareils dans un environnement spécifié. Ces canaux on en a déjà parlé dans le chapitre de réseau sont **:** Ethernet, Bluetooth, NFC, Radio-identification (RFID), zig-Bee, wifi ...etc.

2.5 - LES ENJEUX DE L'IOT

2.5.1- LA NORMALISATION

L'absence de la normalisation a un impact plus important que la simple limitation du potentiel des objets IoT.

Dans l'absence de ces normes, les produits créés sont parfois des fonctionnellement perturbant sur Internet. La nécessité d'une normalisation des outils, méthodes et interfaces de configuration, sera essentielle à l'avenir

2.5.2 -LA CONFIDENTIALITE

Toutes les données collectées doivent être conservées de manière sécurisée et anonyme si nécessaire. **[39]**

2.5.3 –L'ANALYSE

Les données doivent être correctement interprétées et analysées avec fidélité à leur sens, surtout si des actions automatisées sont prises en fonction des résultats des données. [39]

2.5.4 –LA SECURITE

La sécurité est un pilier essentiel de l'Internet et elle est considérée essentiellement comme le défi le plus important pour l'IoT.

L'accroissement du nombre d'objets connectés accroit en résultat la possibilité d'en profiter des failles de sécurité, tout comme les objets mal conçus, qui peuvent exposer les données des utilisateurs au piratage.

2.5.5 –L'AUTONOMIE

Pour que ce potentiel d'objets connectés reste en service durant la durée de vie attendue du projet IoT, Les fabricants et les développeurs doivent penser à trouver un moyen très pratique pour générer de l'électricité et assurer une autonomie suffisante. [40]

2.6 - CONCLUSION

En conclusion, le chapitre sur l'Internet des Objets (IoT) a exploré les différentes dimensions de cette technologie émergente. L'IoT représente une technologie prometteuse qui offre de vastes possibilités de transformation dans divers domaines.

Toutefois, il est crucial de trouver un équilibre entre les avantages et les défis de l'IoT afin de garantir son utilisation responsable et bénéfique dans notre société connectée et intelligente.

CHAPITRE 3

EQUIPEMENTS ET INTERCONNEXIONS D'UNE SMART UNIVERSITE

3.1 –INTRODUCTION

Un réseau est constitué de plusieurs équipements informatiques répartis sur différents sites, tous connectés les uns aux autres.

La transmission d'informations entre ces équipements est un aspect essentiel de l'établissement d'un réseau fonctionnel. Les supports de transmission jouent un rôle essentiel dans l'acheminement des données entre les éléments distants du réseau.

Dans ce chapitre, nous allons explorer les différents types d'équipements et de supports de transmission utilisés dans les réseaux. En comprenant ces composants, nous pouvons établir les bases d'une infrastructure de réseau efficace et fiable.

3.2 –EQUIPEMENT RESEAU

L'interconnexion des réseaux peut se faire localement, lorsque les réseaux se trouvent sur le même site géographique. Dans ce cas, des équipements standards tels que des concentrateurs (hubs), des commutateurs (switch) et des routeurs suffisent pour établir une liaison physique.

Cependant, l'interconnexion peut également concerner des réseaux distants. Dans ce cas, il est nécessaire de connecter ces réseaux à l'aide d'une liaison téléphonique utilisant des modems.

3.2.1 CONCENTRATEUR DE RESEAU (HUB)

Un concentrateur sert de point central auquel tous les hôtes d'un réseau se connectent. Un concentrateur est un périphérique OSI de couche 1 et n'a aucun concept de trames ou d'adressage Ethernet. Il reçoit simplement un signal d'un port et l'envoie à tous les autres ports. Voici un exemple de concentrateur Ethernet à 4 ports. [41]

Figure 3.6 : Concentrateur de réseau (Hub) [41]

En fait, pour notre projet, nous n'avons pas utilisé de concentrateurs, mais des commutateurs afin d'éviter les collisions et le trafic inutile qui pourrait retarder le processus.

3.2.2 – COMMUTATEUR DE RESEAU (SWITCH) :

Un commutateur est utilisé pour connecter plusieurs hôtes ensemble, mais il présente de nombreux avantages par rapport à un concentrateur.

Figure 3.2 : Un Commutateur De Réseau (Switch) **[41]**

Le commutateur est un périphérique OSI de couche 2, ce qui signifie qu'il peut inspecter le trafic reçu et prendre des décisions de transfert. Chaque port d'un commutateur est un domaine de collision distinct et peut fonctionner en mode full duplex.

Il gère le flux de données à travers un réseau en inspectant l'adresse MAC de destination de la trame entrante et en transmettant la trame uniquement à l'hôte auquel le message est destiné.

Chaque commutateur possède une table dynamique (appelée table d'adresses MAC) qui associe les adresses MAC aux ports, Avec ces informations, un commutateur peut identifier quel système se trouve sur quel port et où envoyer la trame reçue. **[41]**

3.2.3 - ROUTEUR

Un routeur est un dispositif réseau qui achemine les paquets d'un réseau à un autre. Il est généralement connecté à deux ou plusieurs réseaux différents.

Lorsqu'un paquet arrive sur le port d'un routeur, celui-ci lit les informations d'adresse contenues dans le paquet afin de déterminer le port sur lequel le paquet sera envoyé.

Figure 3.3 : Routeur sans fil

Par exemple, un routeur vous permet d'accéder à l'internet en connectant votre réseau local à l'internet.

Un routeur est considéré comme un périphérique de couche 3 du modèle OSI car sa décision de transmission principale est basée sur les informations de la couche 3 OSI (l'adresse IP de destination). Si deux hôtes de réseaux différents veulent communiquer entre eux, ils auront besoin d'un routeur entre eux. **[41]**

Pour ce projet, un routeur est utilisé pour créer le réseau et connecter plusieurs LAN entre eux.

3.2.4 - SERVEUR

Le terme de « serveur » possède **deux significations** en informatique. On qualifie par serveur non seulement l'ordinateur qui fournit les ressources d'un réseau informatique, mais aussi le programme fonctionnant sur cet ordinateur. Nous vous donnons les deux définitions d'un « serveur » ci-dessous **[42]**:

- **Définition Serveur (Hardware) :** un serveur matériel (hardware) est un réseau d'ordinateurs reliés par une machine physique et sur lequel fonctionnent un ou plusieurs serveurs logiciels (software). Une alternative au terme de serveur (Hardware) est « hébergeur » (Host en anglais). En principe chaque ordinateur est utilisé avec un serveur logiciel.
- **Définition Serveur (Software) :** un logiciel serveur est un programme effectuant des interactions en réseau avec d'autres programmes appelés logiciels clients. Le service apporté dépend du type de logiciel serveur. La base de la communication en réseau est cette relation Client-serveur. Lors de l'échange de données, différents protocoles de transmission entrent en jeu.

Figure 3.4 : Exemple d'un serveur

3.2.5 – POINT D'ACCES SANS FIL

Un point d'accès sans fil (WAP) est un appareil de mise en réseau permettant aux appareils sans fil de se connecter à un réseau filaire. Il est plus simple d'installer un point d'accès sans fil pour connecter tous les ordinateurs ou appareils à un réseau que d'utiliser des fils.

Il est possible d'utiliser un point d'accès ou des modules d'extension maillés pour étendre la portée du signal et la puissance du réseau pour fournir une couverture sans fil complète et éviter les « zones mortes », en particulier dans les espaces de travail ou les bâtiments plus grands. **[43]**

Figure 3.5 : Point d'accès

Remarque :

Pour notre projet, Le point d'accès utilisé dispose de 2 interfaces **: le port 0** et **le port 1**.

Le port 0 est utilisé pour connecter les appareils clients au point d'accès, ainsi que pour le relier au commutateur.

Le port 1 est dédié à la gestion et à la configuration du point d'accès lui-même, permettant de définir les paramètres de sécurité, les canaux Wi-Fi, les SSID (identifiants de réseau sans fil) et autres fonctionnalités spécifiques au point d'accès.

3.3 - MEDIAS RESEAUX

Le support est le milieu physique réel à travers lequel les données voyagent lorsqu'elles se déplacent d'un composant à un autre, et il connecte les périphériques réseau. Les types de supports réseau les plus courants sont le câble à paire torsadée, le câble coaxial, le câble à fibre optique et le sans fil. Chaque type de média a des capacités spécifiques et sert des objectifs spécifiques.

Comprendre les types de connexions qui peuvent être utilisées au sein d'un réseau permet de mieux comprendre comment les réseaux fonctionnent dans la transmission de données d'un point à un autre.

3.3.1 - CABLE A PAIRE TORSADEE (ETHERNET):

Un câble à paire torsadée comporte quatre paires de fils. Ce type de câblage est courant dans les réseaux locaux actuels.

Le câblage à paires torsadées peut être utilisé pour le câblage téléphonique et réseau. Il existe en deux versions, UTP (Unshielded Twisted-Pair) et STP (Shielded Twisted-Pair). La différence entre ces deux est qu'un câble STP a une couche supplémentaire d'isolation qui protège les données des interférences extérieures. **[41]**

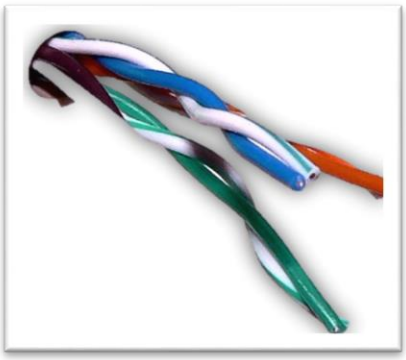


Figure 3.6 : Câble à paire torsadée

3.3.2 - CABLE COAXIAL :

Un câble coaxial a un conducteur interne qui est au milieu du câble. Ce type de câblage se décline en deux types : thinnet et thicknet. Les deux types ont une vitesse de transmission maximale de 10 Mbps. Le câblage coaxial était auparavant utilisé dans les réseaux informatiques, mais il est aujourd'hui largement remplacé par le câblage à paire torsadée. **[41]**

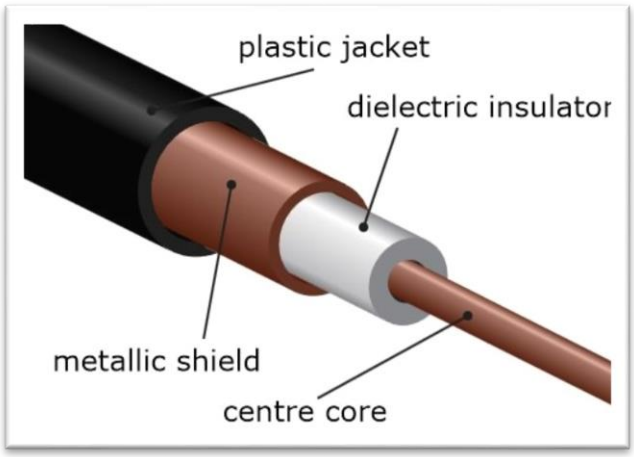


Figure 3.7 : Câble coaxial

3.3.3 - FIBRE OPTIQUE

Ce type de câblage utilise des fibres optiques pour transmettre des données sous forme de signaux lumineux. Les câbles ont des brins de verre entourés d'un matériau de gainage.

Ce type de câblage peut supporter des longueurs de câble plus importantes que tout autre type de câblage (jusqu'à quelques kilomètres). Les câbles sont également insensibles aux interférences électromagnétiques.

Il existe deux types de câbles fibre optique qui sont :

3.3.3.1 - Monomode

Le câble à fibre optique monomode permet à un seul mode (ou longueur d'onde) de lumière de se propager à travers la fibre. Ce type de câble est capable d'une bande passante plus élevée et de plus grandes distances que les autres types de câbles.

Le câble monomode utilise des lasers comme méthode de génération de lumière et est plus cher que le câble multimode. La longueur maximale du câble monomode est de 60+ km (37+ miles). **[24]**

3.3.3.2 - Multimode

Le câble à fibre optique multimode permet à plusieurs modes de lumière de se propager à travers la fibre.

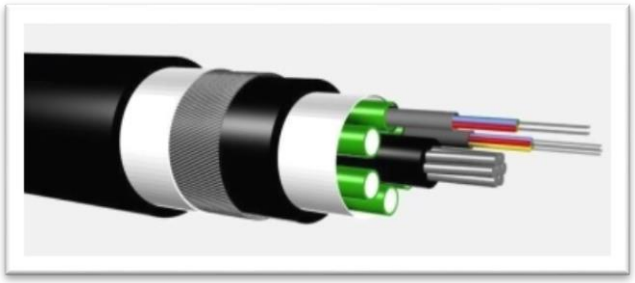


Figure 3.8 : Fibre optique

Le câble multimode est souvent utilisé pour les applications de groupe de travail, utilisant des diodes électroluminescentes (DEL) comme dispositifs générateurs de lumière. La longueur maximale du câble multimode est de 2 km (1,2 miles). **[24]**

3.3.4 - COMMUNICATION SANS FIL

Les réseaux sans fil deviennent de plus en plus populaires et utilisent un type de technologie différent. La communication sans fil utilise des fréquences radio (RF) ou des ondes infrarouges pour transmettre des données entre des appareils sur un réseau local.

Pour les réseaux locaux sans fil, un élément clé est le concentrateur sans fil, ou point d'accès, utilisé pour la distribution du signal.

Pour recevoir les signaux du point d'accès, un PC ou un ordinateur portable doit installer une carte adaptateur sans fil ou une carte d'interface réseau sans fil (NIC).

Ils utilisent des portions du spectre RF pour transmettre la voix, la vidéo et les données. Les fréquences sans fil vont de 3 kHz à 300 GHz. Les débits de transmission de données vont de 9 kbps à 54 Mbps.

	Câble à paires torsadées	Coaxial	Fibre optique	Communication sans fil
Bandwidth	Jusqu'à 1 Gbps	10-100 Mbps	Jusqu'à 10 Gbps ou plus	Jusqu'à 54 Mbs
Distance	Jusqu'à 100 m	Jusqu'à 500 m	Jusqu'à 60 km	Jusqu'à 100 m
Cout	Le moins chère	Peu couteux	Le plus chère	Modéré

Tableau 3.1 : Comparaison des types de médias

3.4 – CONNECTEUR DE RESEAU :

Les connecteurs de réseau sont généralement conçus pour des types spécifiques de câbles et de médias de transmission, tels que les câbles Ethernet, les câbles à fibre optique ou les câbles coaxiaux.

Ils offrent une interface standardisée pour assurer une compatibilité entre les différents équipements réseau.

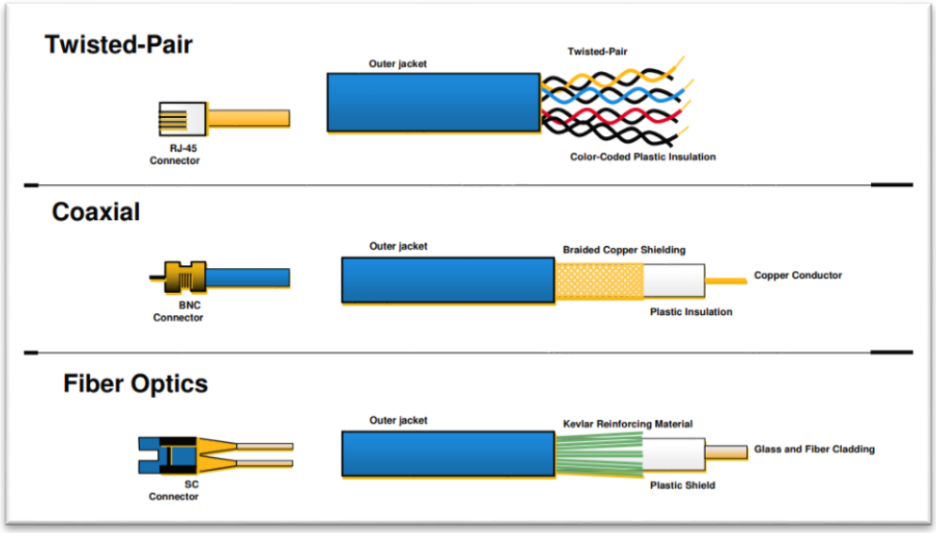


Figure 3.9 : types de supports physiques

Ces connecteurs peuvent prendre différentes formes et tailles, en fonction du type de câble et de la technologie utilisée.

Certains exemples courants de connecteurs de réseau comprennent le connecteur RJ45 pour les câbles Ethernet, le connecteur LC pour les câbles à fibre optique, le connecteur BNC pour les câbles coaxiaux, et bien d'autres. **[43]**

3.5 - ÉQUIPEMENTS REQUIS POUR L'UNIVERSITÉ INTELLIGENTE

Dans notre projet, l'université est constituée de six (6) départements sont :

- Administration
- Parking
- Amphithéâtre
- Bibliothèque
- Laboratoire
- Stade

La figure ci-dessus montre notre université avant l'installation du réseau :

Figure 3.10 : Notre université avant l'installation du réseau [44]

Dans le cadre de la configuration des réseaux de notre université, notre configuration réseau comprend :

⇨ cinq réseaux LANs, un pour chaque département de l'université sauf le stade et l'amphithéâtre, ainsi qu'un réseau MAN qui relie tous les départements.

Cette architecture de réseau garantit une connectivité fiable, une communication fluide et une gestion efficace des ressources au sein de notre université.

La figure ci-dessus montre notre université après l'installation du réseau :

Figure 3.11 : Notre université après l'installation du réseau

Le schéma synoptique ci-dessous nous donne les équipements utilisés dans chaque département.

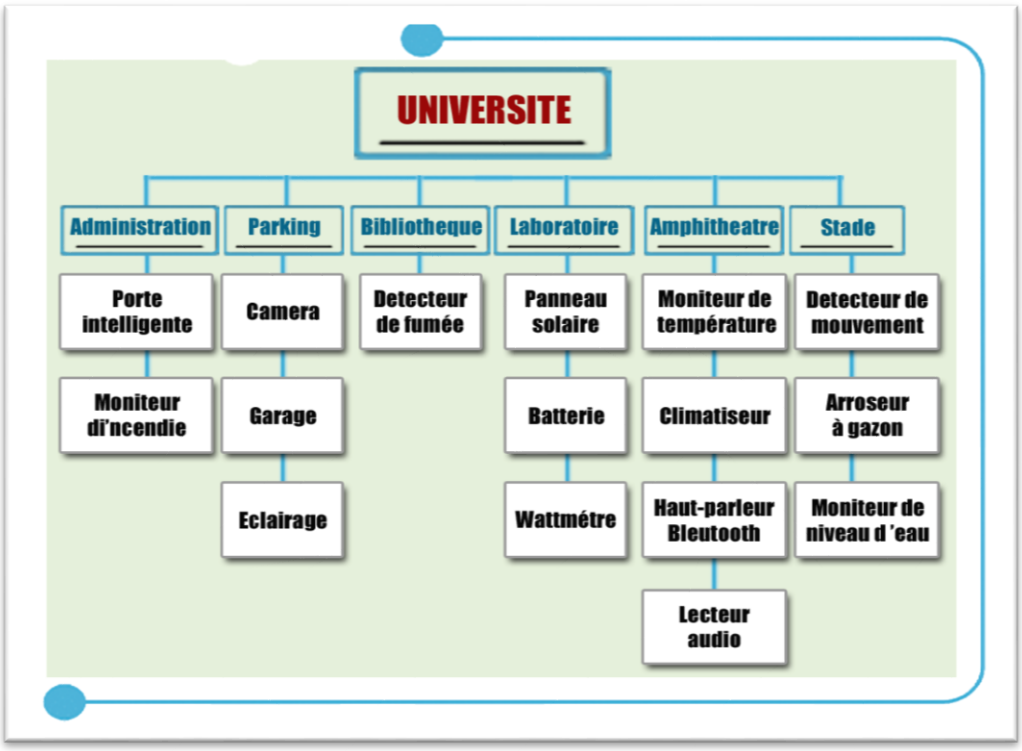


Figure 3.12 : Equipements de chaque département

Nous allons expliquer le principe de fonctionnement de chaque équipement de notre université :

3.5.1 - ADMINISTRATION

Cette figure montre les équipements de l'administration :

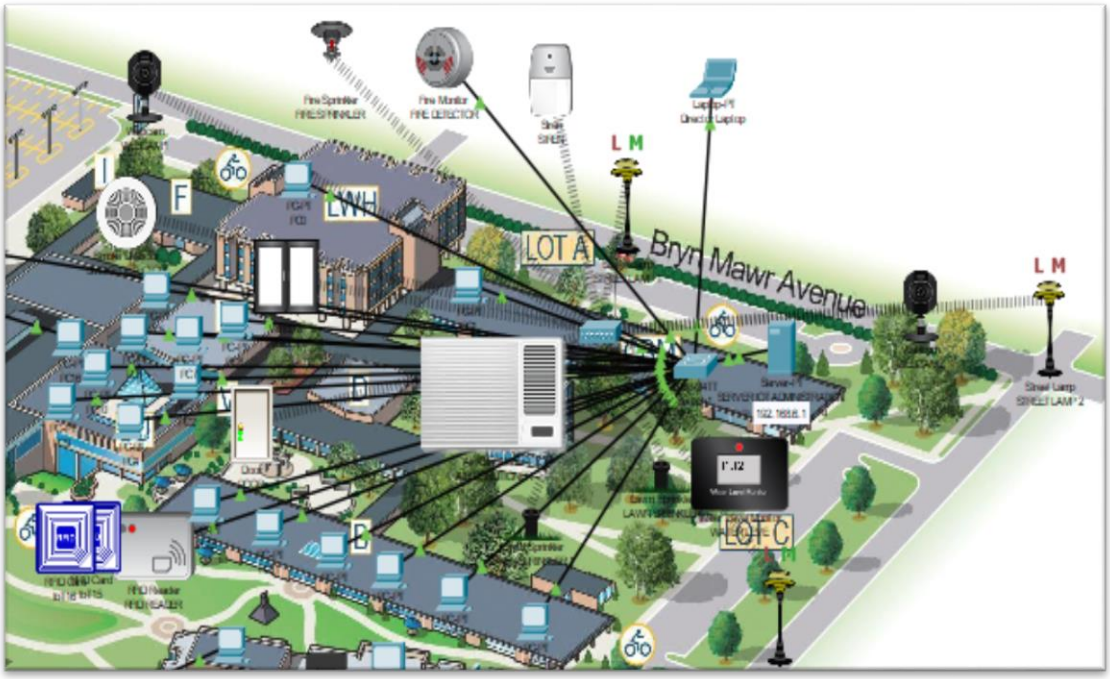


Figure 3.13 : Administration

3.5.1.1 -la Porte intelligente

La porte connectée offre un accès sécurisé au département administratif de l'université.

Elle est équipée de dispositif d'identification telle que **la carte RFID** qui est une technologie d'identification sans contact qui permet de contrôler l'accès sécurisé aux bâtiments administratifs de manière pratique et efficace.

Figure 3.14 : Lecteur RFID

Figure 3.15 : Carte RFID

Figure 3.16 : Porte

3.5.1.2 - Moniteur d'incendie

Le moniteur d'incendie est un équipement essentiel dans le cadre de la sécurité des bâtiments administratifs d'une université intelligente.

Son rôle principal est de détecter rapidement les signes d'incendie et de fournir des alertes précoces pour permettre une intervention rapide et efficace.

Il est associé avec :

- **Une sirène :** qui est un dispositif d'alerte sonore utilisé pour avertir les occupants d'un bâtiment en cas de détection d'incendie.
- **Un gicleur d'incendie :** qui est un dispositif d'extinction automatique qui libère de l'eau ou d'autres agents d'extinction en cas de détection d'incendie pour éteindre les flammes.

Figure 3.17 : Moniteur d'incendie

Figure 3.18 : Gicleur d'incendie

Figure 3.19 : sirène

3.5.2 - PARKING

Ceci est la figure qui montre les équipements du Parking

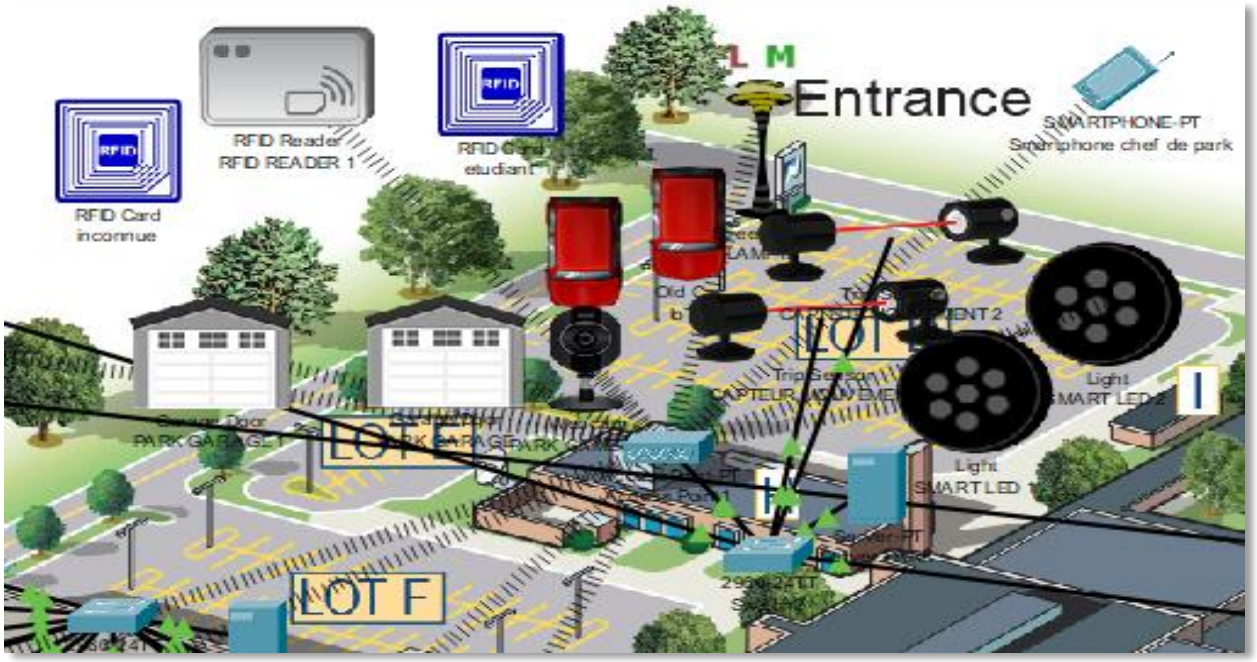


Figure 3.20 : Parking

3.5.2.1 - La Caméra :

Les caméras de surveillance dans le parking sont des dispositifs de sécurité essentiels qui assurent une surveillance visuelle constante des espaces de stationnement.

Figure 3.21 : Camera

3.5.2.2 – Le Garage :

Le garage est équipé de dispositifs tels que la **carte RFID** et **le capteur de déclenchement** qui est installé à l'entrée du garage pour détecter la présence d'un véhicule et envoie un signal pour déclencher l'ouverture automatique du garage.

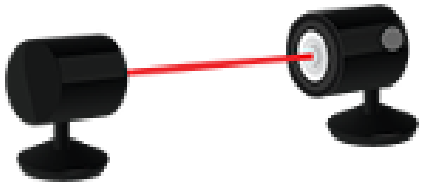


Figure 3.22 : Capteur de déclenchement

Figure 3.23 : Garage

3.5.2.3 - éclairage

Les systèmes d'éclairage intelligents sont équipés de capteurs et de contrôles automatisés qui détectent les mouvements des personnes et des véhicules dans le parking, ce qui permet d'activer ou de désactiver les lumières de manière proactive.

Figure 3.24 : Eclairage intelligent

Figure 3.25 : LED intelligente

3.5.2.4 – LED intelligente

La LED intelligente est équipée d'un **capteur de déclanchement** qui est installé sur toute les positions du parking pour détecter la présence d'un véhicule et envoie un signal pour la LED pour s'allumer automatiquement indiquant que la place du parking est prise déjà.

3.5.3 - BIBLIOTHEQUE

Ceci est la figure qui montre les équipements de bibliothèque

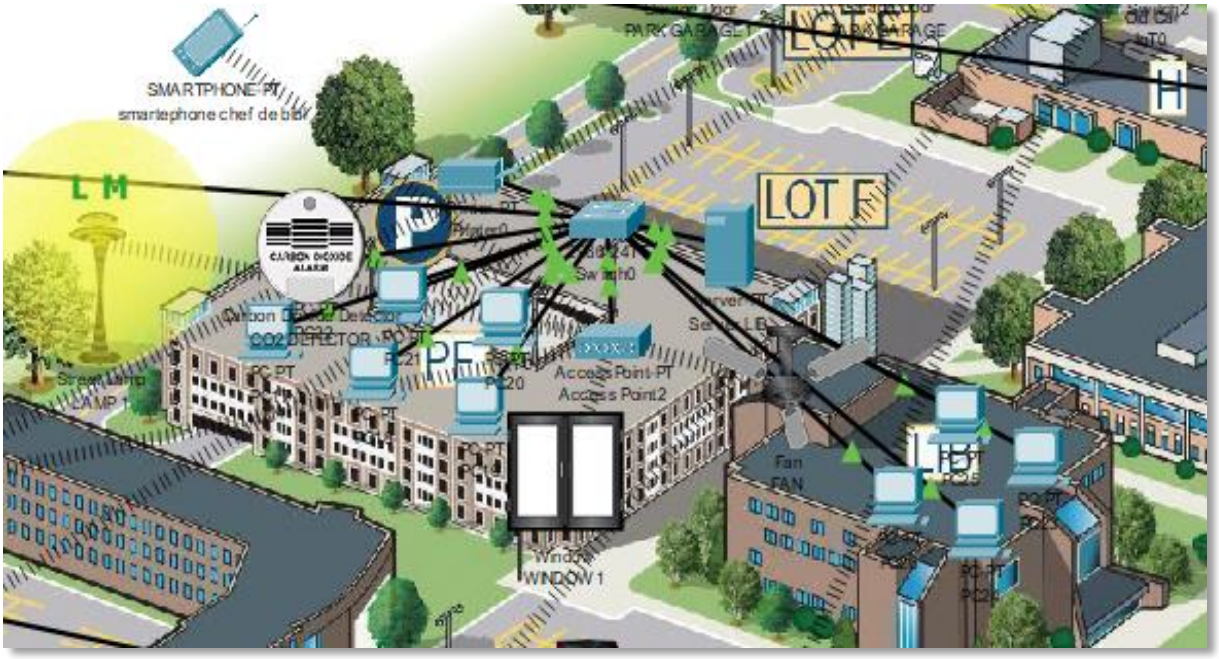


Figure 3.26 : Bibliothèque

3.5.3.1 – Détecteur de fumée :

Il est conçu pour détecter toute augmentation anormale des niveaux de CO2, Ce détecteur peut être associé à **une fenêtre intelligente** pour réguler automatiquement l'ouverture ou la fermeture de cette fenêtre en fonction des niveaux de CO2 détectés.

Figure 3.27 : Détecteur de CO2

Figure 3.28 : Fenêtre intelligente

3.5.4 - LABORATOIRE

Ceci est la figure qui montre les équipements de Laboratoire :

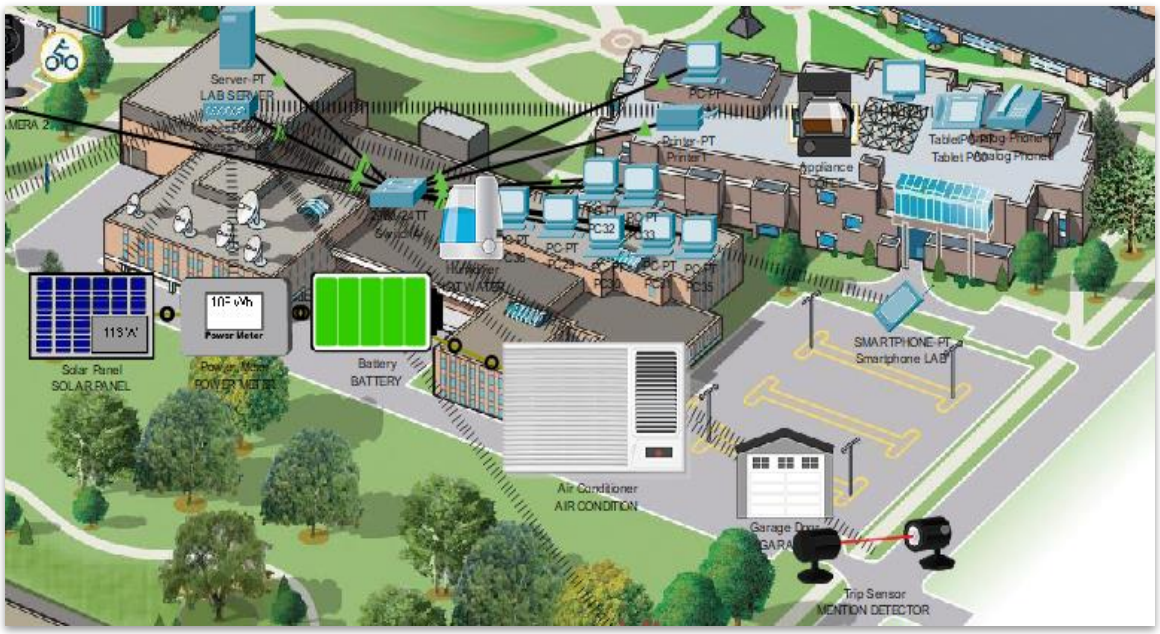


Figure 3.29 : Laboratoire

3.5.4.1 - Panneau solaire

Il produit de l'énergie en fonction de la quantité de SOLEIL dans l'environnement et envoie l'énergie générée à un autre appareil tel que **la batterie.**

Figure 3.30 : Panneau Solaire

3.5.4.2 – Batterie

La batterie est un dispositif de stockage d'énergie qui permet de stocker l'électricité produite par le panneau solaire lorsqu'il y a un excès de production pour une utilisation ultérieure.

Elle peut être associée avec **un wattmètre**

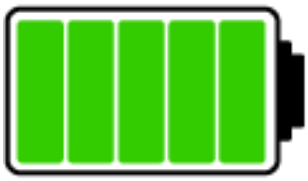


Figure 3.31 : Batterie

3.5.4.3 – Wattmètre

Le wattmètre permet de quantifier la quantité d'énergie électrique consommée ou fournie par un appareil ou un système électrique.

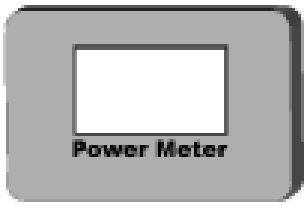


Figure 3.32 : Wattmètre

Lorsqu'on relie cet appareil avec la batterie, Cela nous permet de surveiller la performance de la batterie, de vérifier sa capacité de décharge et de charge, et d'évaluer son rendement énergétique.

3.5.5 - AMPHITHEATRE

Ceci est la figure qui montre les équipements de l'amphithéâtre :

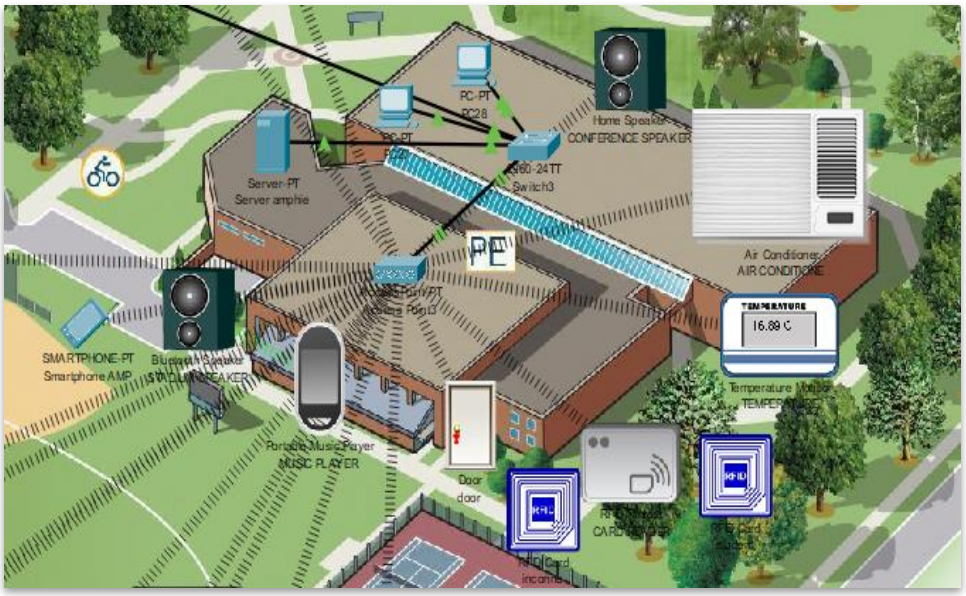


Figure 3.33 : Amphithéâtre

3.5.5.1 - Moniteur de température :

Le moniteur de température est un appareil qui recueille des données concernant la température de l'environnement et les convertit en une forme lisible de données. On peut l'associé avec **un climatiseur**

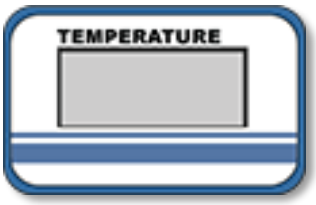


Figure 3.34 : Moniteur de température

3.5.5.2 - Climatiseur

Le climatiseur est un appareil utilisé pour réguler la température, l'humidité et la circulation de l'air dans un espace donné.

Figure 3.35 : Climatiseur

3.5.5.3 - Haut-parleur Bluetooth

Un haut-parleur Bluetooth vous permet de diffuser des fichiers audio à partir de votre smartphone, tablette, ordinateur, **lecteur audio** ou tout autre appareil compatible via une connexion Bluetooth.

Figure 3.36 : Haut-parleur Bluetooth

3.5.5.4 - Lecteur Audio

Le lecteur audio est un dispositif qui permet de stocker, lire, écouter et diffuser des fichiers audio.

Figure 3.37 : Lecteur Audio

3.5.6 - STADE

La figure ci-dessous montre les différents équipements se trouvant dans le Stade :

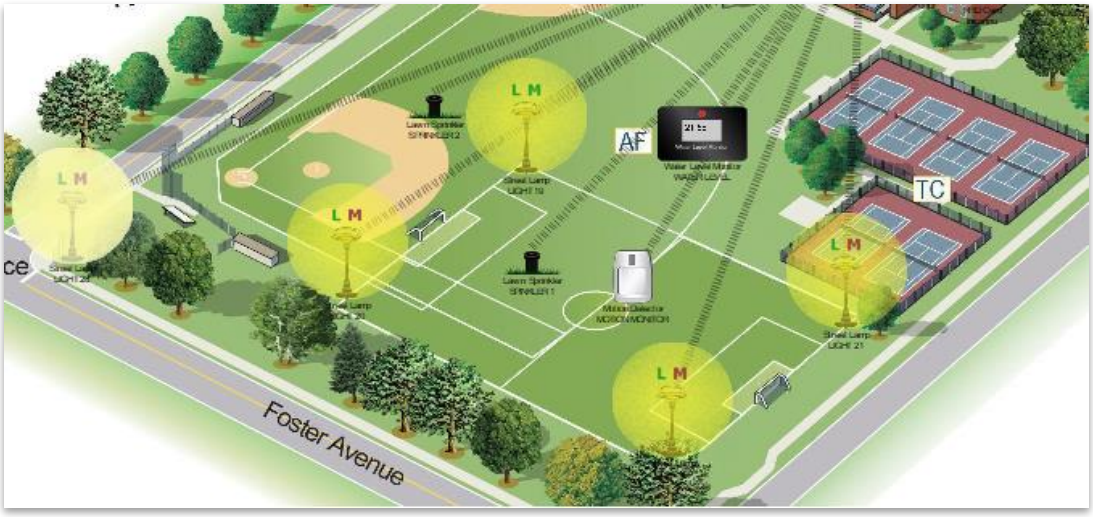


Figure 3.38 : Stade

3.5.6.1 - Arroseur de gazon

Un arroseur de gazon est un dispositif utilisé pour irriguer les pelouses, les jardins et les stades en distribuant de l'eau de manière uniforme sur une grande surface. Il aide à maintenir un gazon sain et bien hydraté.

Figure 3.39 : Arroseur de Gazon

On peut l'associé avec **un moniteur de niveau d'eau** et **le détecteur de mouvement**

3.5.6.2 - Moniteur de niveau d'eau

Un moniteur de niveau d'eau est un dispositif qui mesure et surveille le niveau d'eau dans les terrains du stade, contribuant à maintenir un niveau d'eau optimal.

Figure 3.40 : Moniteur de niveau d'eau

3.5.6.3 - Détecteur de mouvement

Un détecteur de mouvement est un appareil qui utilise des capteurs pour détecter les mouvements dans son environnement,

Dans notre cas, il peut mettre l'arroseur de gazon éteint lorsqu'il y a du mouvement dans le stade.

Figure 3.41 : Détecteur De mouvement

3.6 -CONCLUSION

En conclusion, ce chapitre a exploré les différents équipements et supports de transmission utilisés dans les réseaux informatiques.

Nous avons vu que les équipements tels que les concentrateurs, les commutateurs, les routeurs, les serveurs et les points d'accès sans fil sont indispensables pour établir une connectivité fiable et efficace.

Les médias de transmission jouent un rôle crucial dans le transfert des données entre les différents éléments du réseau.

Nous avons également abordé les équipements requis pour une université intelligente, soulignant l'importance des dispositifs tels que les caméras, les détecteurs, les panneaux solaires et les moniteurs pour créer un environnement connecté et fonctionnel.

En comprenant les différents équipements et supports de transmission, il est possible de concevoir et de mettre en place une infrastructure réseau solide et adaptée aux besoins spécifiques de notre université.

Ces éléments sont essentiels pour assurer une connectivité fluide, sécurisée et efficace, favorisant ainsi l'échange d'informations et la communication au sein des réseaux.

CHAPITRE 4

CONFIGURATIONS, TESTS & RESULTATS

4.1 - INTRODUCTION

Ce projet se concentre sur la conception et la simulation IoT en utilisant Cisco Packet Tracer. Donc nous allons explorer l'utilisation de ce logiciel qui est un outil de simulation réseau largement utilisé, pour configurer les réseaux de l'université et évaluer leur connectivité.

Nous aborderons également des tests manuels et automatiques des appareils IoT (Internet des objets) présents dans ces réseaux. Donc pour simuler cette connectivité et évaluer le bon fonctionnement de notre université nous sommes obligés de structurer notre travail en plusieurs étapes :

- ⇨ Configuration des Réseaux de l'Université
- ⇨ Evaluation de la connectivité des appareils
- ⇨ Test de l'utilisation manuelle des appareils IoT
- ⇨ Test de l'utilisation automatique des appareils IoT

4.2 - APERÇU DE CISCO PACKET TRACER

Cisco Packet Tracer est un programme complet d'enseignement et d'apprentissage des technologies réseau qui offre une combinaison unique d'expériences de simulation et de visualisation réalistes, de capacités d'évaluation et de création d'activités, ainsi que des opportunités de collaboration et de compétition entre plusieurs utilisateurs.

Les fonctionnalités innovantes de Packet Tracer aident les étudiants et les enseignants à collaborer, résoudre des problèmes et apprendre des concepts dans un environnement social captivant et dynamique. **[45]**

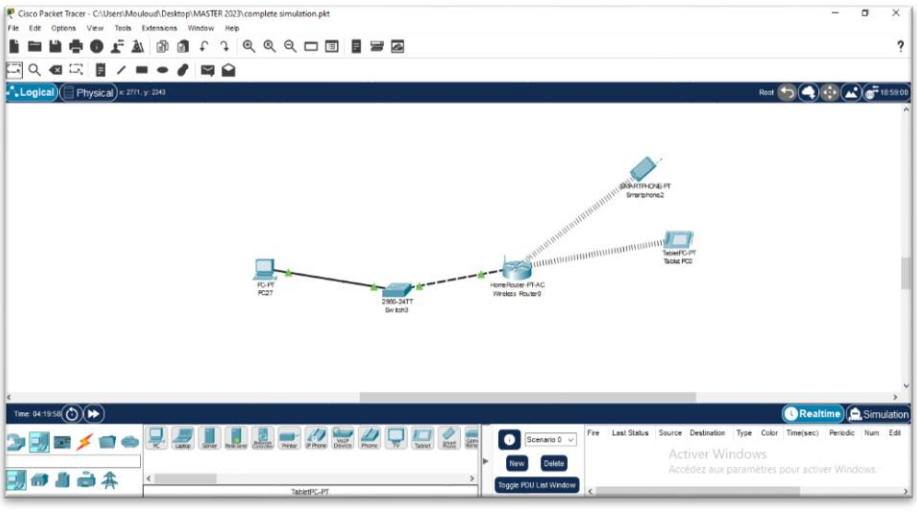


Figure 4.1 : Interface Cisco Packet tracer

L'outil propose un ensemble étendu de matériels et de câblages qui permettent aux étudiants de mettre en place un réseau de base ou très complexe. Il enseigne également comment résoudre les problèmes liés au réseau, car l'outil inclut également des fonctionnalités réalistes de débogage. **[25]**

À partir de la version 7.0, Cisco a également introduit des fonctionnalités IoT dans l'outil, permettant aux étudiants de s'entraîner en configurant des appareils IoT et en utilisant l'automatisation IoT. Pour notre mémoire nous avons utilisé la dernière version disponible, qui est la version 8.2.

4.3 - CONFIGURATION DES RESEAUX DE L'UNIVERSITE

La configuration des réseaux joue un rôle crucial dans le fonctionnement efficace d'une université moderne. Un réseau bien configuré permet une connectivité fluide, une communication transparente et une gestion efficace des appareils et des services connectés. Dans ce chapitre, nous aborderons la configuration des réseaux de notre université, en mettant l'accent sur les réseaux locaux (LAN) et le réseau métropolitain (MAN) qui relie les 6 départements.

Le schéma synoptique ci-dessous illustre les étapes qu'on a suivies pour configurer les réseaux de l'université.

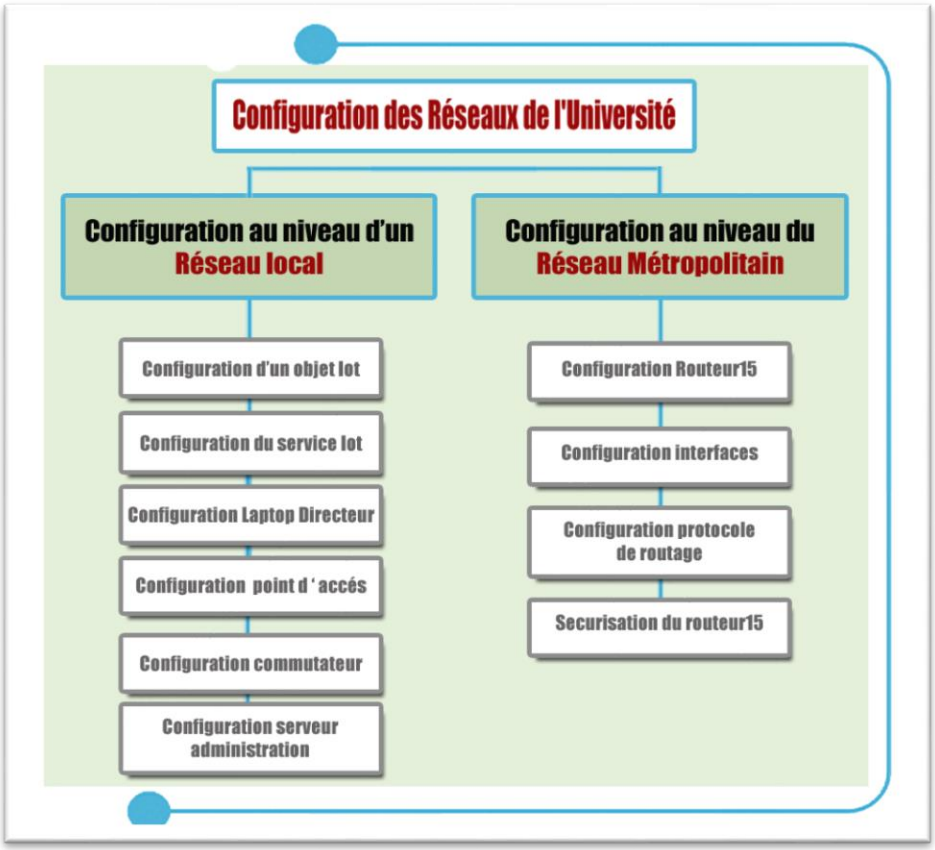


Figure 4.2 : schéma de la configuration du réseau de l'université

4.3.1. CONFIGURATION AU NIVEAU D'UN RESEAU LOCAL

Dans notre université, nous avons opté pour une topologie en étoile pour chaque réseau local (département).

Cette topologie permet une gestion centralisée et facilite l'ajout ou la suppression d'appareils sans perturber le reste du réseau.

Étant donné que nous disposons de cinq réseaux LAN dans notre université, nous allons décrire ici la configuration du réseau LAN de l'administration de l'université.

Les autres départements seront configurés de la même manière.

Avant de procéder à la configuration, il est important de définir la plage d'adresses IPv4 que nous allons utiliser pour chaque département.

Le tableau suivant présente les plages IPv4 pour chaque département :

Remarque : On a utilisé des adresses IPv4 de classe C.

Département	Plage IPv4	
Administration	192.168.6.0	255.255.255.0
Parking & H	192.168.7.0	255.255.255.0
Stade & AM	192.168.1.0	255.255.255.0
Laboratoire	192.168.2.0	255.255.255.0
Bibliothèque	192.168.8.0	255.255.255.0

Tableau 4.1 : plage IPv4 de chaque département

4.3.1.1. Configuration du réseau local de l'administration

La configuration passe par plusieurs étapes :

⇨ **Configuration du serveur de l'administration**

Au début, nous devons configurer l'adresse IP statique du serveur. Étant donné que le serveur se trouve dans la plage d'adresses 192.168.6.0 avec un masque de sous-réseau de 255.255.255.0, nous allons lui attribuer l'adresse IP « 192.168.6.1 » (IPv6 ne sera pas utilisé).

La figure 4.3 montre la configuration.

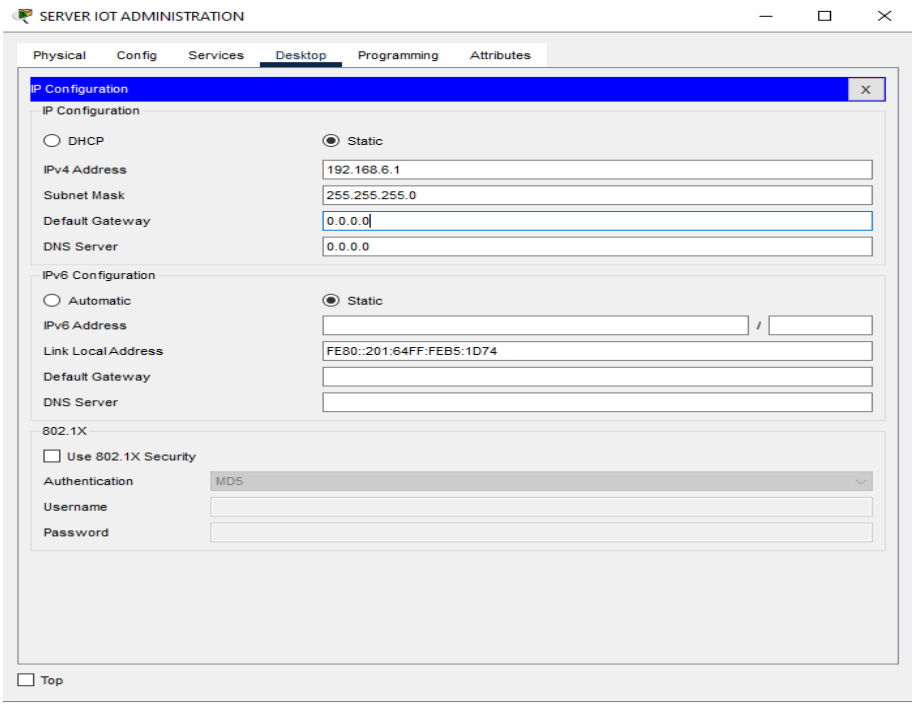


Figure 4.3 : Adresse IP du serveur de l'administration

Voici un tableau qui montre les adresses IP des serveurs de chaque département.

Serveur	Adresse IP
Serveur administration	192.168.6.1
Serveur parking	192.168.7.1
Serveur bibliothèque	192.168.8.1
Serveur amphithéâtre et stade	192.168.1.10
Serveur laboratoire	192.168.2.10

Tableau 4.2 : Adresse IPv4 des serveurs

Après cela, nous allons activer et configurer le service DHCP du serveur. Dans la figure 4.4

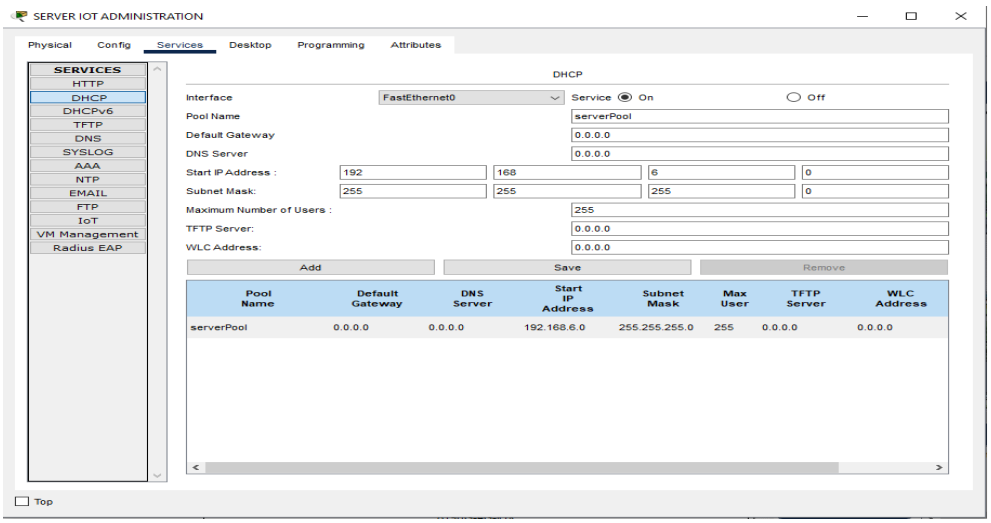


Figure 4.4 : Activation et configuration du service DHCP

Nous avons configuré le service DHCP du serveur en spécifiant la plage IPv4 du réseau local de l'administration dans le champ "Start IP Address", avec un masque de sous-réseau de 255.255.255.0.

Nous avons également défini le nombre maximum d'utilisateurs à 255 (pas plus de 255 utilisateurs).

Pour configurer le service DNS sur le serveur, nous allons dans l'onglet "Services" du serveur, puis dans "DNS", et activons le service DNS.

Ensuite, nous ajoutons le nom de domaine "www.smartuniversity.com" et l'adresse IP du serveur IoT "192.168.6.1", comme illustré dans la figure.

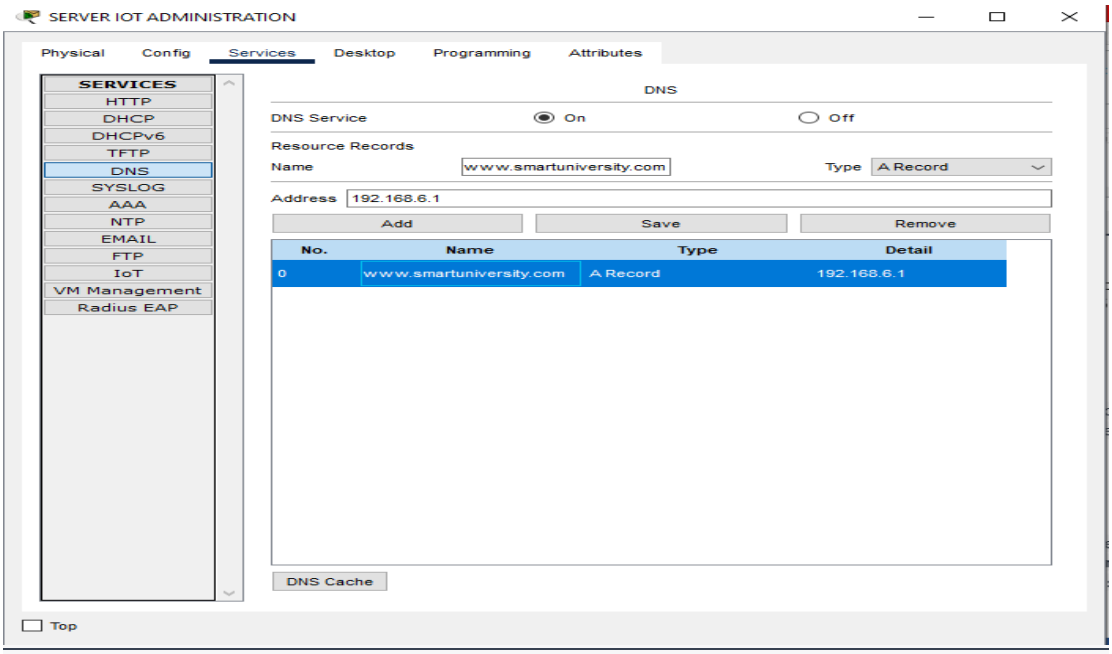


Figure 4.5 : Activation et configuration du service DNS

Voici un tableau qui montre les noms de domaine des serveurs des départements :

Serveur	Nom du Domaine
Serveur administration	www.smartuniversity.com
Serveur parking	www.parkuniversity.com
Serveur bibliothèque	www.libuniversity.com
Serveur amphithéâtre et stade	www.ampuniversity.com
Serveur laboratoire	www.labuniversity.com

Tableau 4.3 : Noms des domaines des serveurs

Ces noms de domaine sont utilisés pour accéder aux serveurs de chaque département à partir du réseau local de l'université.

⇨ Configuration du service IoT

Pour que le serveur fonctionne en tant que serveur IoT, nous devons activer le service IoT à partir de l'onglet "Services". Ensuite, nous devons créer un compte sur le serveur en ouvrant un navigateur Web depuis le bureau du serveur lui-même et en accédant au domaine "www.smartuniversity.com", qui représente l'adresse du serveur IoT "192.168.6.1". Étant donné que nous n'avons pas encore de compte, nous devons cliquer sur "S'inscrire maintenant".

Dans notre cas, pour faciliter les choses, le nom d'utilisateur du compte sera "ADMIN" et le mot de passe sera également "ADMIN".

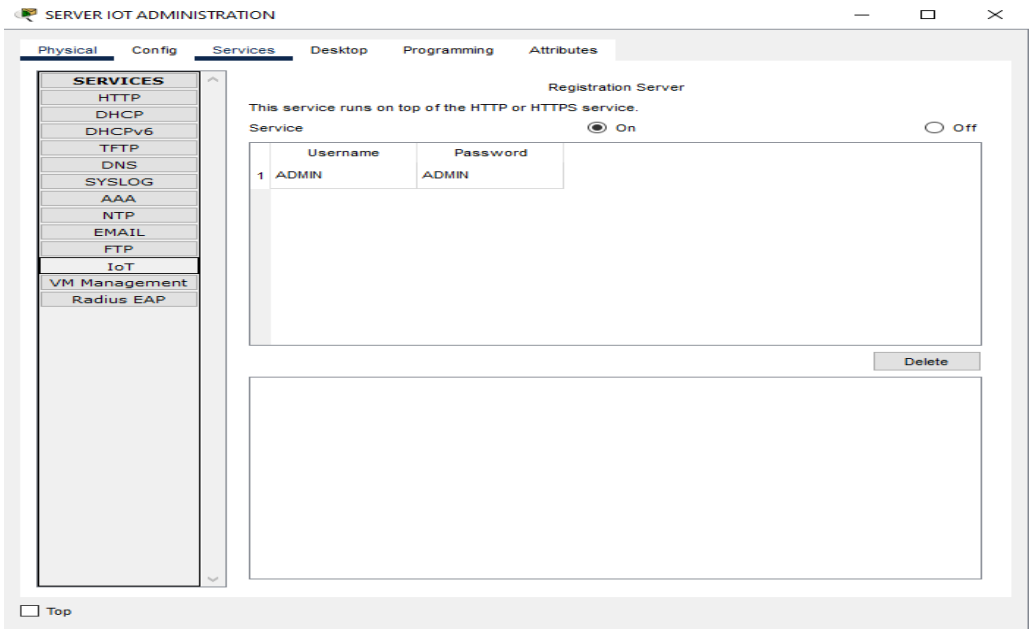


Figure 4.6 : activation du service IoT

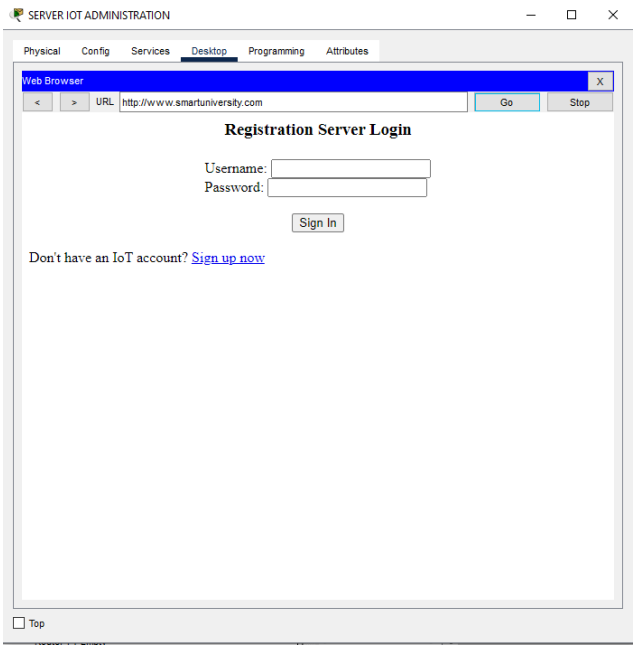


Figure 4.7 : connexion au serveur

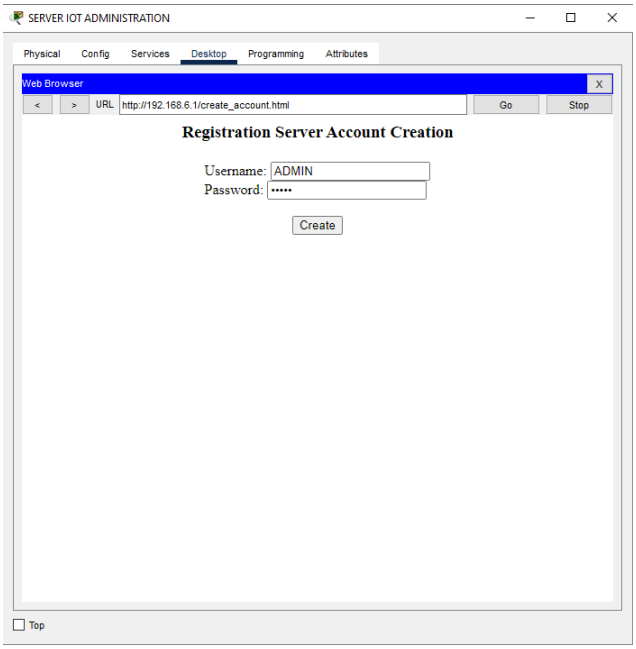


Figure 4.8 : création du compte

Ce tableau révisé montre les noms d'utilisateur et les mots de passe de chaque département :

Serveur	Nom d'utilisateur	Mot de passe
Serveur administration	ADMIN	ADMIN
Server parking	ADMIN	ADMIN
Server bibliothèque	ADMIN	ADMIN
Server amphithéâtre et stade	AMP	AMP
Server laboratoire	LAB	LAB

Tableau 4.4 : informations de connexions des serveurs

Ces informations sont utilisées à titre d'exemple et il est recommandé de choisir des noms d'utilisateur et des mots de passe sécurisés pour assurer la confidentialité et la sécurité des systèmes.

Pour pouvoir accéder à notre compte IoT, il faut suivre cette procédure :

1. Démarrer un navigateur web depuis n'importe quel appareil connecté à Internet.
2. Taper l'adresse IP du serveur ou le nom de domaine.
3. Utiliser le nom d'utilisateur et le mot de passe corrects. On se référant à la table 4.4.
4. Ensuite, il faut cliquer sur "Se connecter" pour accéder à notre compte.

Après la connexion, on sera dirigé vers la fenêtre de la figure 4.8 qui est vide, puisque aucun objet IoT n'est connecté au serveur pour le moment.

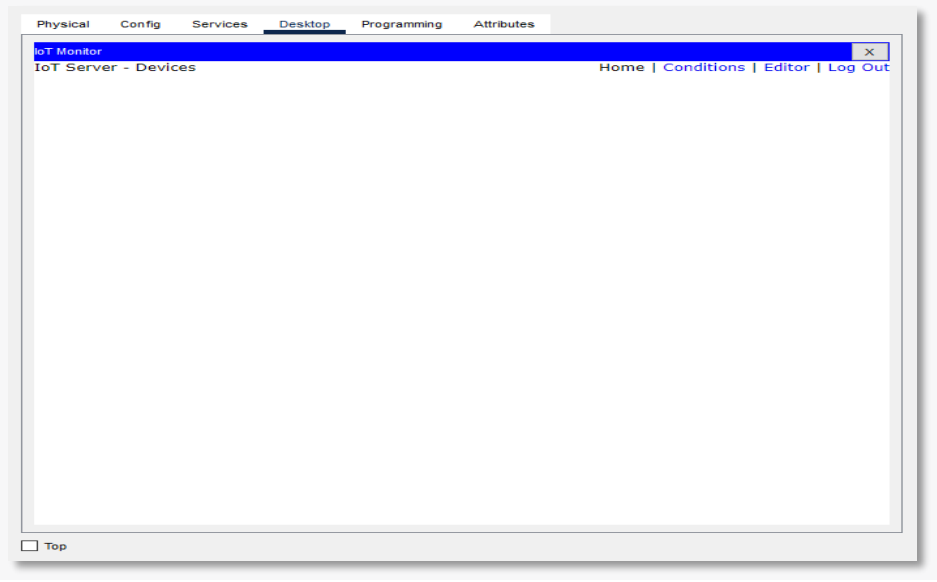


Figure 4.9 : interface du compte IoT

⇨ Configuration du commutateur (switch) :

Le commutateur est auto-configuré ; il est utilisé uniquement pour connecter tous les appareils entre eux et au serveur.

⇨ Configuration du point d'accès :

Dans l'interface du port 1 du point d'accès, il est possible de configurer un SSID personnel et un mot de passe. Dans notre cas, le SSID du routeur domestique a été défini sur "Home Gateway".

Ce SSID sera utilisé par tous les appareils se connectant au réseau.

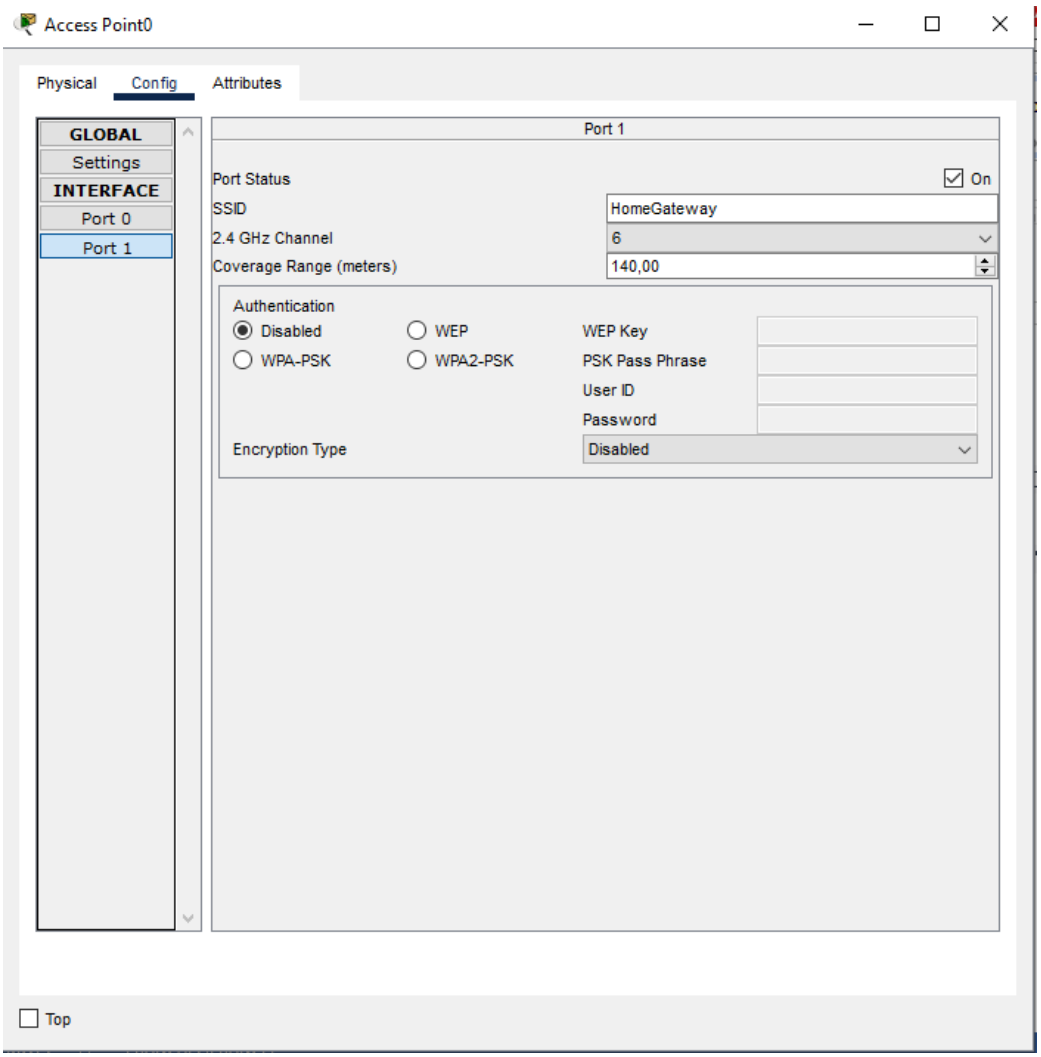


Figure 4.10 : configuration SSID du point d'accès

⇨ Configuration de l'ordinateur portable du directeur :

Cette étape nous montre comment connecter l'ordinateur portable du directeur au serveur IoT de l'administration.

Remarque : Tous les autres appareils réseau seront configurés de la même manière.

D'abord, nous allons connecter l'interface Ethernet (Fa0) de l'ordinateur portable à l'interface du commutateur (Fa0/22) à l'aide d'un câble Ethernet.

Ensuite, nous allons activer le protocole DHCP sur l'ordinateur portable pour lui attribuer une adresse IP automatiquement.

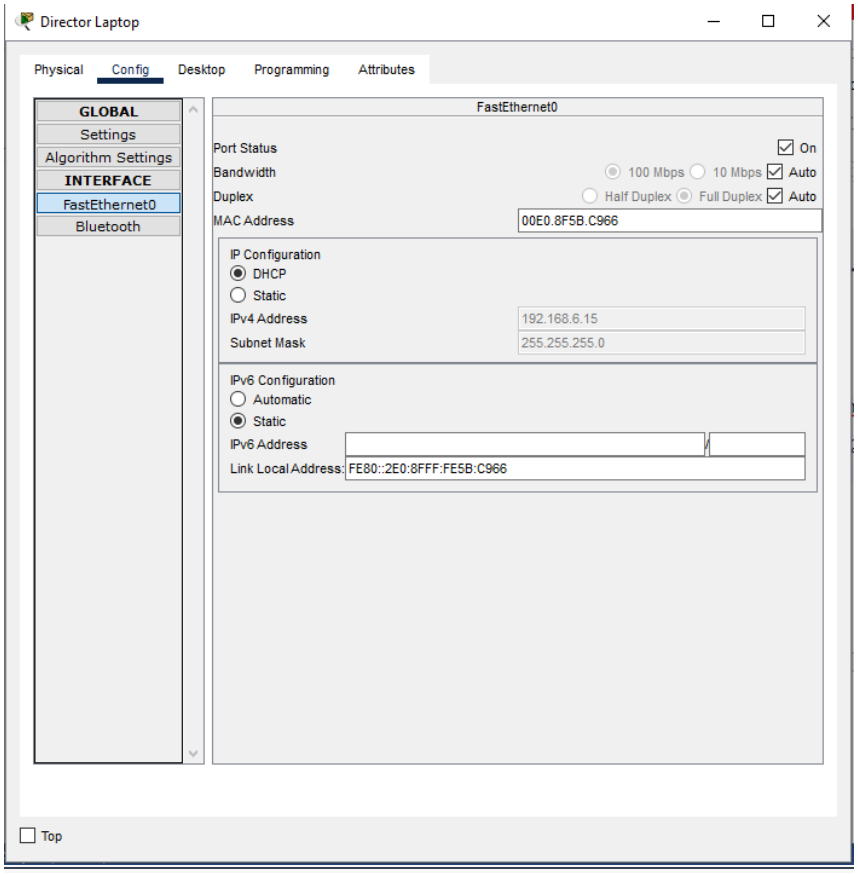


Figure 4.11 : adresse IPv4 de l'ordinateur portable

Selon la figure 4.10 On constate que le DHCP a attribué l'adresse "192.168.6.15" à l'ordinateur portable.

Remarque : Tous les autres appareils filaires du réseau seront configurés de manière similaire.

⇨ Configuration d'un objet IoT :

Par défaut, les périphériques IoT dans Cisco Packet Tracer sont équipés d'une carte réseau sans fil. Nous allons vous montrer comment configurer la Caméra pour la connecter sans fil avec le point d'accès.

1. Sélectionnez la webcam dans Cisco Packet Tracer.
2. Accédez aux paramètres de la webcam et recherchez l'option de configuration sans fil.
3. Dans les paramètres sans fil, recherchez l'option pour configurer le SSID (identifiant du réseau sans fil).
4. Entrez le SSID du point d'accès, qui dans ce cas est "HomeGateway".
5. Enregistrez les modifications et activez la connectivité sans fil de la webcam.

La figure 4.12 montre les étapes

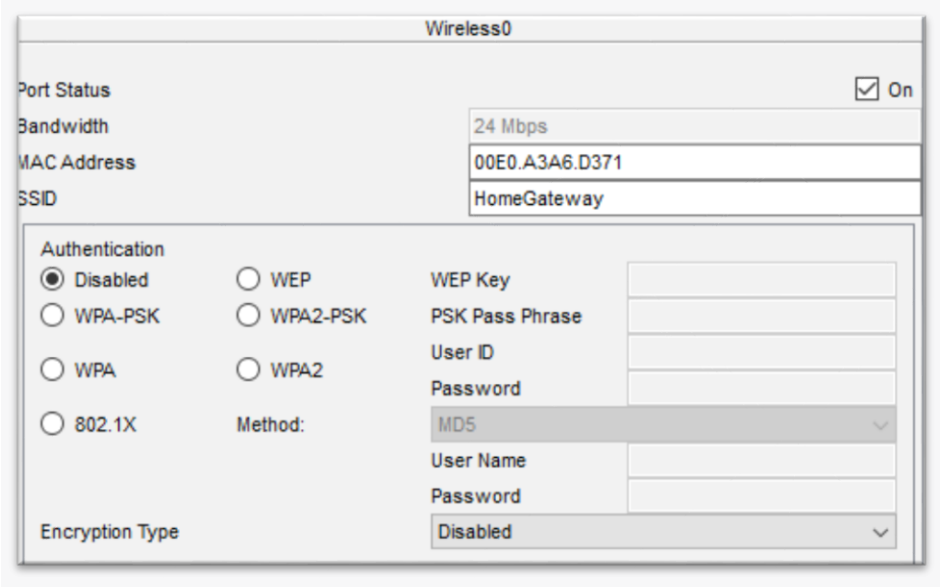


Figure 4.12 : Configuration du SSID de la webcam

Une fois que la Caméra est connectée au point d'accès, il est nécessaire d'activer le DHCP pour attribuer une adresse IP dynamique à la Caméra.

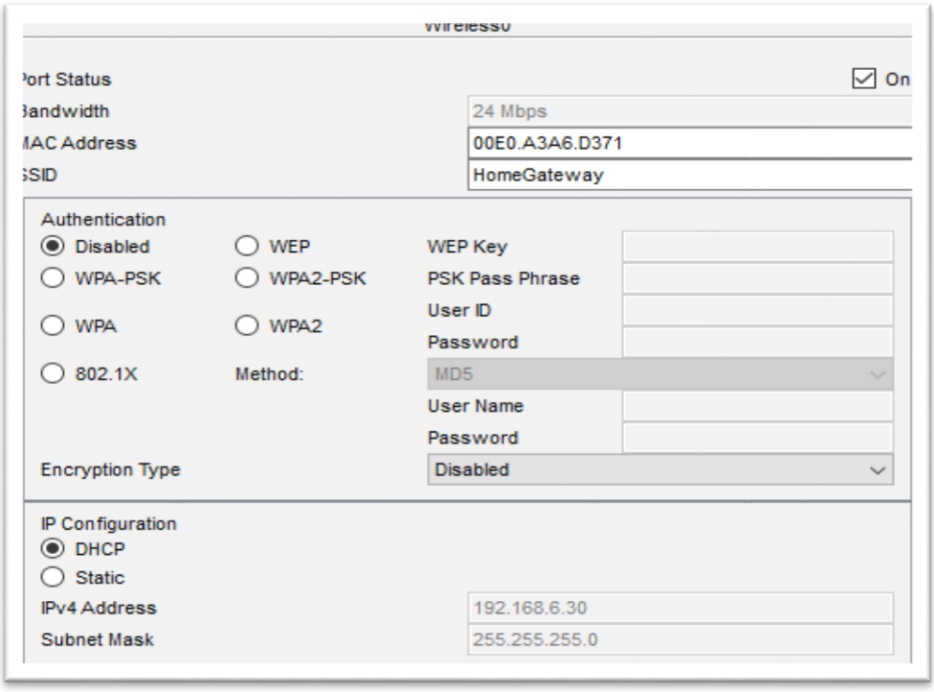


Figure 4.13 : adresse IP de la webcam

Le serveur IoT doit être informé de tous les périphériques IoT installés dans l'université. Pour enregistrer un appareil dans le serveur, les informations suivantes sont nécessaires :

- Adresse du serveur
- Nom d'utilisateur
- Mot de passe du compte

Dans l'onglet de configuration de l'appareil, sélectionnez "Serveur distant" dans le champ "Serveur IoT" (voir la figure 4.14).

Ensuite, saisissez les informations nécessaires et appuyez sur "Connecter" pour établir la connexion.

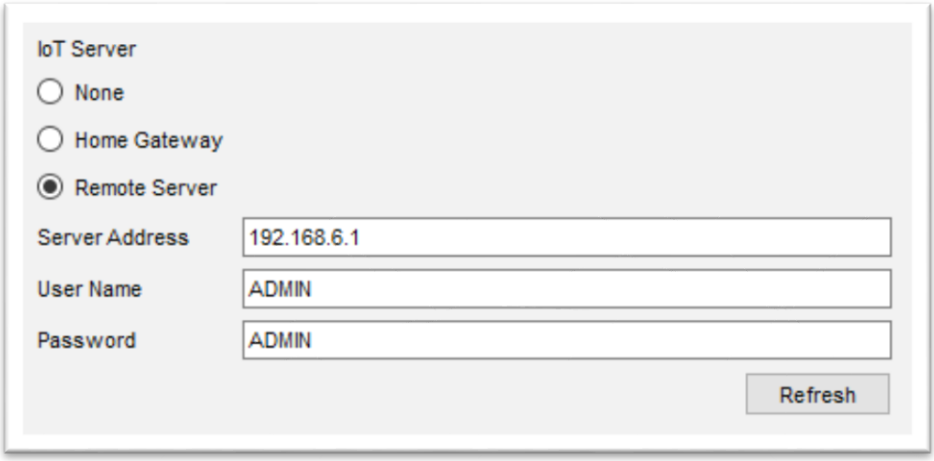


Figure 4.14 : connexion webcam au serveur

Remarque : Tous les autres appareils sans fils de l'université seront configurés de la même manière pour se connecter au point d'accès et au serveur de leur réseau respectif.

Une fois que tous les appareils sont connectés au serveur IoT, ils apparaîtront dans la fenêtre des objets connectés, comme illustré dans la figure 4.15.

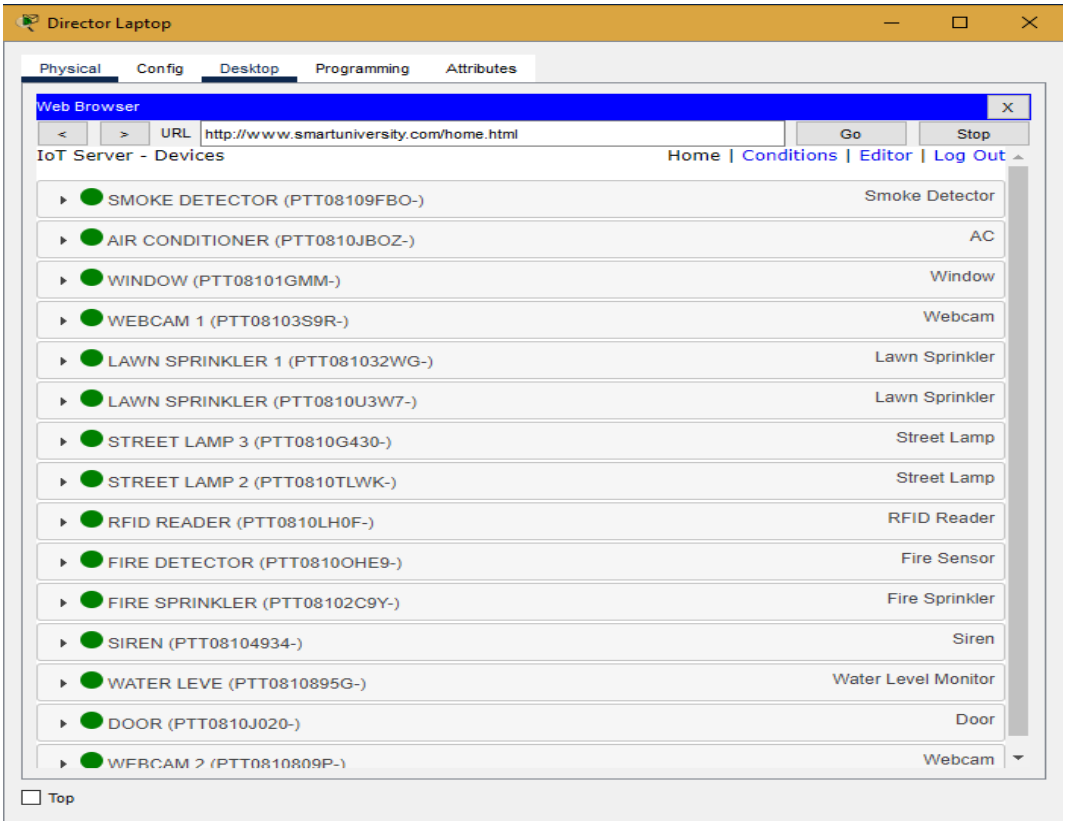


Figure 4.15 : IoT serveur de l'administration

Cet ongle (illustré dans la figure 3.18) permet au chef de chaque département et au directeur de l'université de superviser certains appareils, qu'ils fonctionnent ou non, et de voir certains appareils qui fournissent des informations utiles.

À partir de cet onglet, le personnel peut également interagir directement avec les appareils, si ces derniers disposent de la fonctionnalité d'utilisation directe.

4.3.2. CONFIGURATION AU NIVEAU DU RESEAU METROPOLITAIN

Après avoir configuré les 5 réseaux locaux, nous passerons à la connexion Métropolitain.

Donc dans cette partie nous allons détailler la configuration du réseau MAN (Métropolitain Area Network) qui assure l'interconnexion des 5 réseaux locaux de notre université déjà configuré.

Ce réseau joue un rôle crucial dans la création d'un environnement de communication fiable et efficace, permettant aux différents départements de l'université de partager des ressources, d'accéder aux services centraux et de collaborer de manière transparente.

Nous avons opté pour une topologie en maillage partiel pour l'interconnexion des routeurs. Les routeurs agissent comme des points de liaison entre les différents départements, facilitant ainsi la communication entre eux. Les avantages de cette topologie sont discutés dans le chapitre 1.

Étant donné que nous disposons de cinq routeurs dans notre université, nous allons décrire ici la configuration du routeur15. Les autres routeurs seront configurés de la même manière.

4.3.2.1. Configuration du routeur15

Le routeur15 dispose 2 interfaces :

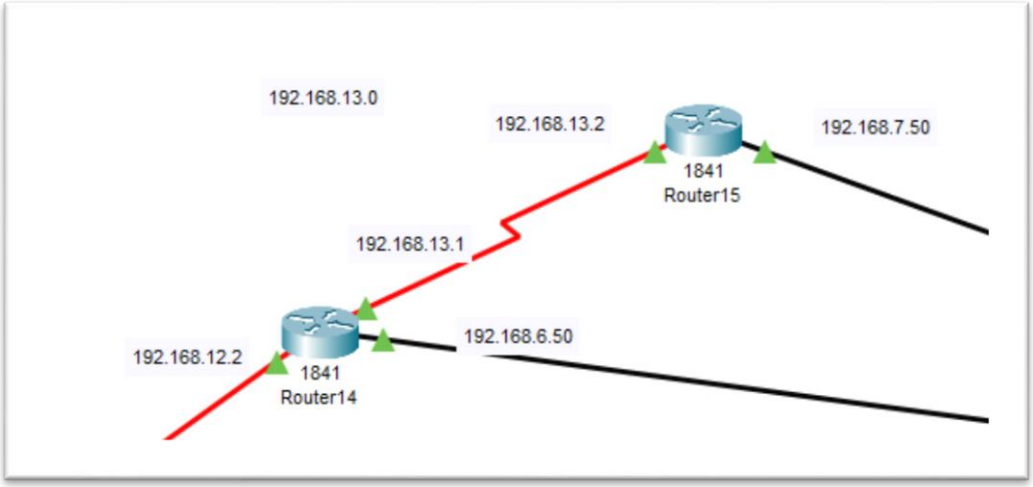


Figure 4.16 : position du Routeur15

- Fa0/0, qui est connectée au switch de l'administration.
- Se0/0/0, qui est connectée au routeur14. (voir figure 4.17)

⇨ Configuration des interfaces

La première chose à faire est de configurer les interfaces du routeur. Pour configurer le router15, nous avons suivi les étapes et les commandes suivantes :

```
<outer>enable
outer#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
outer(config)#hostname ROUTEUR15
OUTEUR15(config)#interface Fa0/0
OUTEUR15(config-if)# ip address 192.168.7.50 255.255.255.0
OUTEUR15(config-if)#no shutdown
OUTEUR15(config-if)#exit
OUTEUR15(config)#interface Se0/0/0
OUTEUR15(config-if)# ip address 192.168.13.2 255.255.255.0
OUTEUR15(config-if)#no shutdown
OUTEUR15(config-if)#end
OUTEUR15#
OUTEUR15#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.17 : commandes de configuration des interfaces du routeur15

Le tableau 4.5 montre les ports Internet utilisés, ainsi que les adresses IP et les masques attribués à chaque routeurs :

Les routeurs	Les ports internet	Les IP adresse	Les masques
ROUTEUR 15	Fa0/0	192.168.7.50	255.255.255.0
	Se0/0/0	192.168.13.2	255.255.255.0
ROUTEUR 14	Fa0/0	192.168.6.50	255.255.255.0
	Se0/1/0	192.168.13.1	255.255.255.0
	Se0/0/0	192.168.12.2	255.255.255.0
ROUTEUR 13	Fa0/0	192.168.8.50	255.255.255.0
	Se0/1/0	192.168.12.1	255.255.255.0
	Se0/0/0	192.168.11.2	255.255.255.0
ROUTEUR 12	Fa0/0	192.168.2.50	255.255.255.0
	Se0/1/0	192.168.11.1	255.255.255.0
	Se0/0/0	192.168.10.2	255.255.255.0
ROUTEUR 11	Fa0/0	192.168.1.50	255.255.255.0
	Se0/0/0	192.168.10.1	255.255.255.0

Tableau 4.5 : adresse IP des ports des routeurs

⇨ Configuration du protocole de routage

Dans cette simulation, nous sommes appuyés sur le routage dynamique, qui est un mécanisme pour lequel les routeurs communiquent entre eux, ce qui est plus simple et pratique que le routage statique, nous avons compté sur le routage RIPv2 qui est un protocole du type vecteur de distance.

Pour l'application du routage dynamique basé sur le RIPv2 du routeur15, nous avons besoin des réseaux qui sont connectés directement avec ce routeur (voir figure 4.15), et pour le configurer nous suivons les étapes et les demandes qui suivent :

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.7.0
Router(config-router)#network 192.168.13.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.18 : Configuration du protocole RIPv2

⇨ La Table de routage du routeur15

Nous affichons la table de routage du routeur15 pour vérifier le bon fonctionnement du routage dynamique (RIPv2), où :

- La lettre C montre les réseaux qui sont directement connectés au routeur15.
- La lettre R indique que nous avons utilisé le protocole RIP

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
R    192.168.2.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
R    192.168.6.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
C    192.168.7.0/24 is directly connected, FastEthernet0/0
R    192.168.8.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
R    192.168.10.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
R    192.168.11.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
R    192.168.12.0/24 is possibly down, routing via 192.168.13.1, Serial0/0/0
C    192.168.13.0/24 is directly connected, Serial0/0/0
```

Figure 4.19 : Table routage du routeur15

⇨ Sécurisation du routeur15

Afin de renforcer la sécurité, nous avons attribué un mot de passe au routeur15, qui est « administration ». Cela permet de restreindre l'accès non autorisé au routeur et de protéger les configurations et les paramètres du réseau. Ainsi, seules les personnes ayant connaissance de ce mot de passe pourront accéder et configurer le routeur15.

Cette mesure de sécurité contribue à maintenir l'intégrité et la confidentialité du réseau.

```
Router#enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password administration
Router(config-line)#login
```

Figure 4.20 : Commande du mot passe

Remarque : Tous les autres routeurs du réseau seront configurés de manière similaire.

4.4 – ÉVALUATION DE LA CONNECTIVITEE DES APPAREILS

Dans cette partie, nous nous concentrerons sur deux méthodes de test de connectivité les plus couramment utilisées :

- **Test de ping** : Le test de ping est un outil simple mais puissant pour évaluer la connectivité entre les appareils réseau. Il mesure le temps nécessaire pour qu'un paquet de données (ping) soit envoyé d'un appareil source à une destination spécifiée et revienne.
- **L'option "Add Simple PDU"** : L'option "Add Simple PDU" est une fonctionnalité disponible dans certains logiciels de simulation de réseaux. Elle permet d'évaluer la connectivité entre les appareils en vérifiant si les paquets de données (PDU) atteignent leur destination prévue et si les appareils peuvent recevoir et traiter correctement ces paquets.

Nous allons effectuer ces tests de connectivité à la fois au niveau des réseaux locaux (LAN) de l'université et au niveau du réseau métropolitain (MAN) qui assure l'interconnexion de ces réseaux locaux. Cela permet de vérifier la connectivité à différents niveaux du réseau.

4.4.1 - TEST AU NIVEAU DES RESEAUX LOCAUX

Pour faciliter la tâche on va tester un exemple de chaque département.

4.4.1.1 - Administration

Ping ordinateur portable du directeur (192.168.6.15) ➔ serveur administration (192.168.6.1)

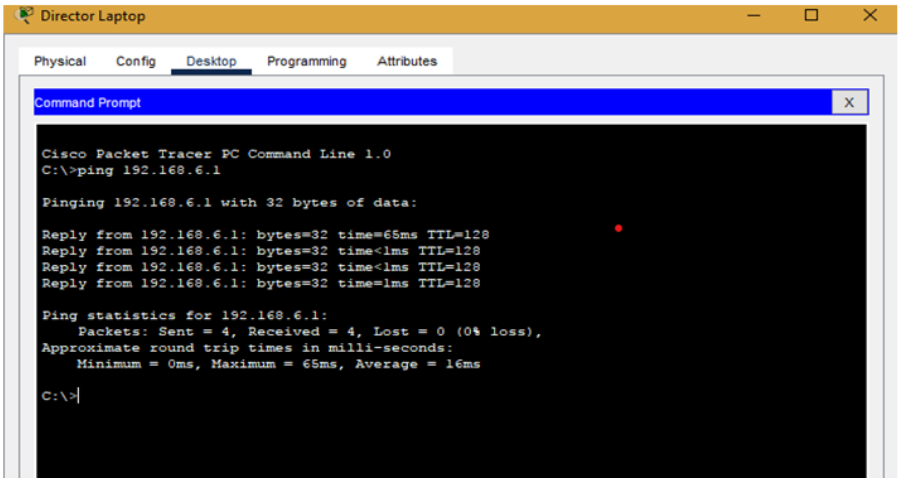


Figure 4.21 : Ping de l'ordinateur portable vers le serveur de l'administration

Test avec PDU :

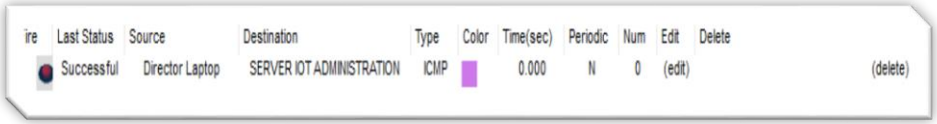


Figure 4.22 : PDU de l'ordinateur portable vers serveur administration

Ping ordinateur portable du directeur ➔ PC0 administration (192.168.6.10)

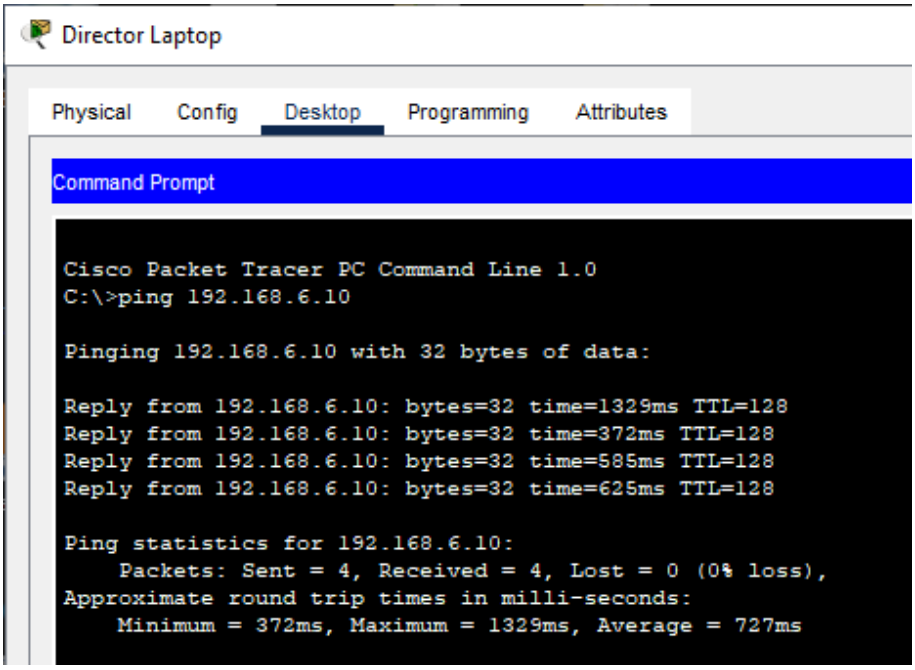


Figure 4.23 : ping de l'ordinateur portable vers PC0 de l'administration

Test avec PDU :

Figure 4.24 : PDU de l'ordinateur portable vers PC0 de l'administration

Ping ordinateur portable du directeur ➔ Camera 1 administration (192.168.6.30)

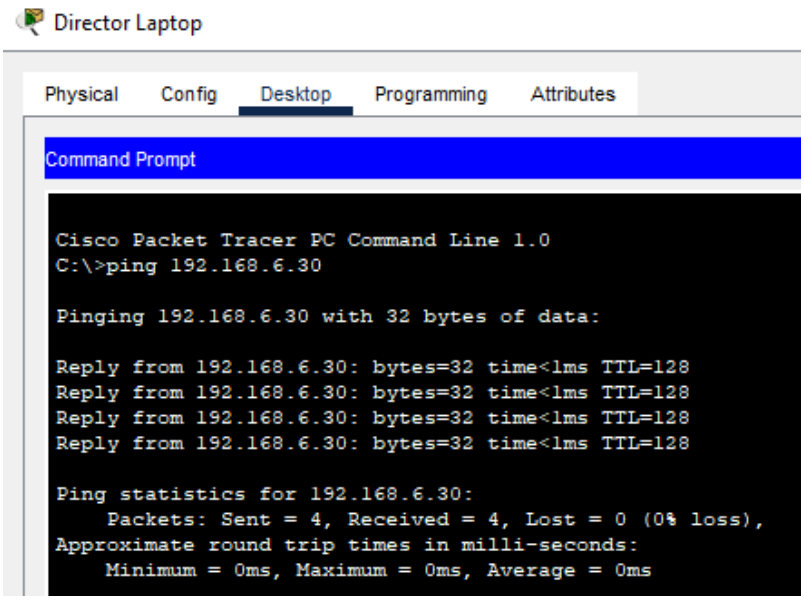


Figure 4.25 : ping de l'ordinateur portable vers Camera 1 administration

Test avec PDU :

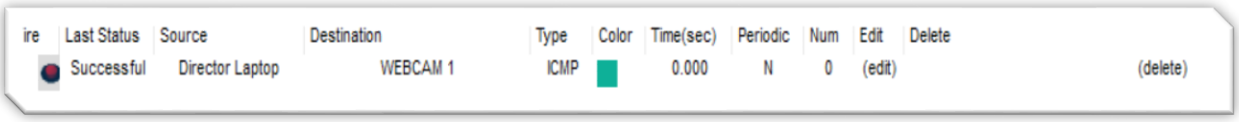


Figure 4.26 : PDU de l'ordinateur portable vers Camera 1 administration

4.4.1.2 - Parking

Ping telephone chef de parking ➔ Garage parking (192.168.7.8)

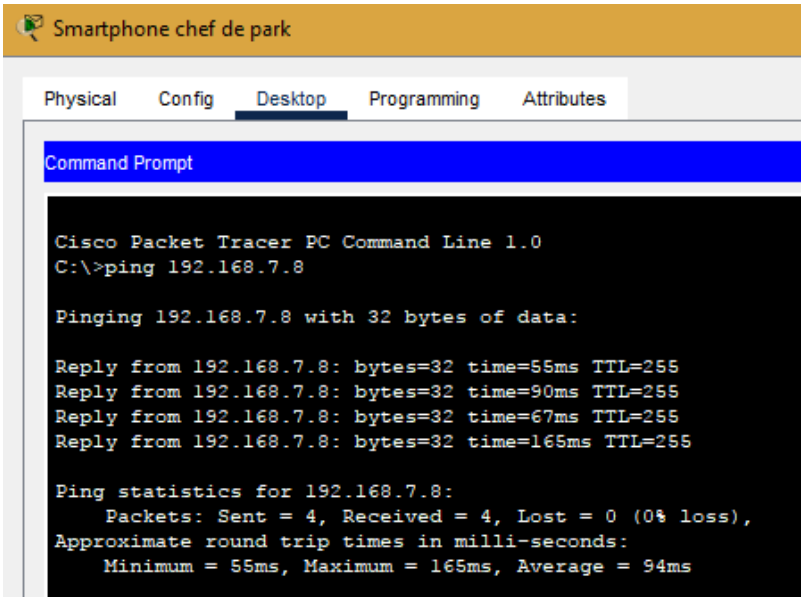


Figure 4.27 : Ping du téléphone chef de parking vers le garage

Test avec PDU :

re	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smartphone chef d...	PARK GARAGE	ICMP		0.000	N	0	(edit)	(delete)

Figure 4.28 : PDU du téléphone chef de parking vers le garage

4.4.1.3 - Laboratoire

Ping téléphone chef du Laboratoire ➔ Climatiseur Laboratoire (192.168.2.50)

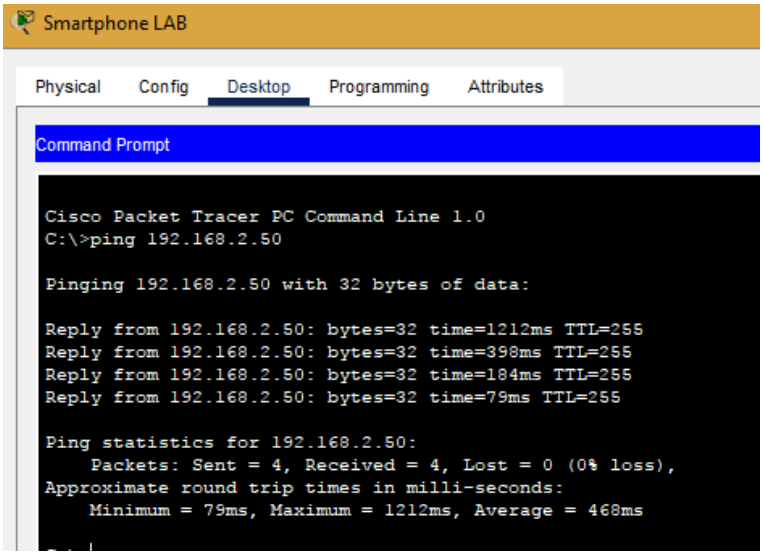


Figure 4.29 : Ping du téléphone chef du Laboratoire vers le climatiseur

Test avec PDU :

re	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smartphone LAB	AIR CONDITION	ICMP		0.000	N	0	(edit)	(delete)

Figure 4.30 : PDU du téléphone chef du Laboratoire vers le climatiseur

4.4.1.4 - Bibliothèque

Ping téléphone chef de la bibliothèque ➔ Ventilateur (192.168.8.3)

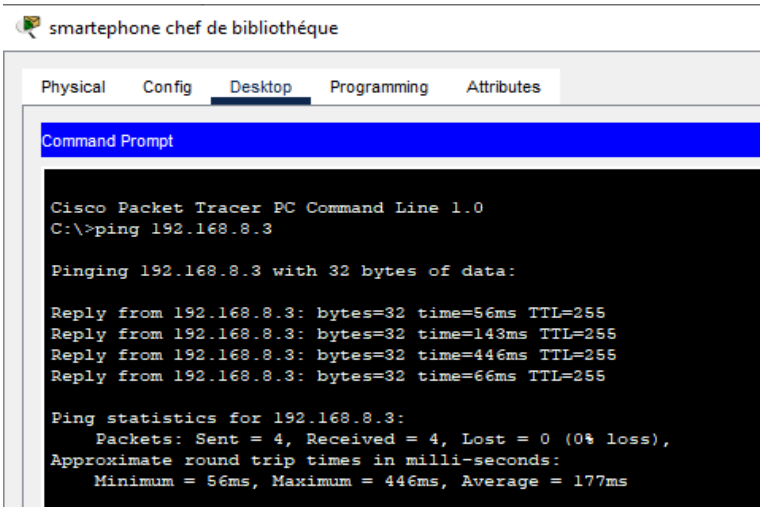


Figure 4.31 : Ping du téléphone chef de bibliothèque vers le ventilateur

Test avec PDU :

ire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	smartephone chef de bibl	FAN	ICMP		0.000	N	0	(edit)	(delete)

Figure 4.32 : PDU du téléphone chef de bibliothèque vers le ventilateur

4.4.1.5 - Amphithéâtre et stade

Ping téléphone chef amphithéâtre et stade ➔ Haut-parleur Bluetooth (192.168.1.7)

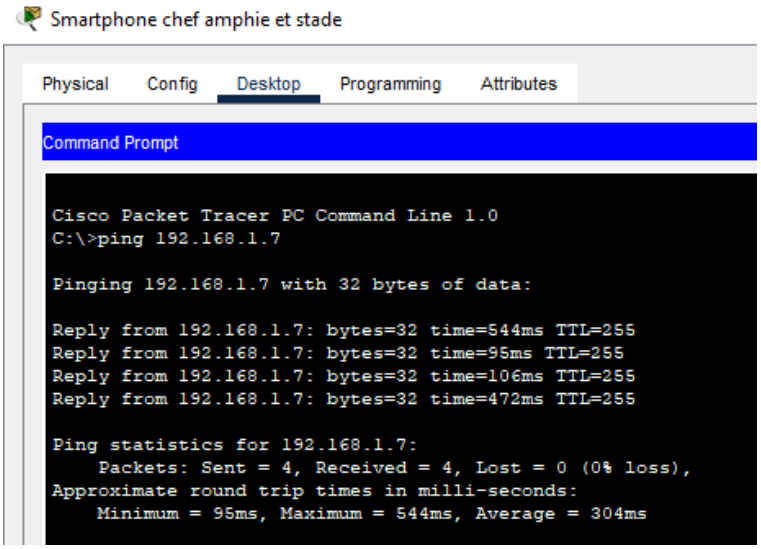


Figure 4.33 : Ping du téléphone chef amphithéâtre et stade vers le Haut-parleur

Test avec PDU :

ire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smartphone chef amphie...	STADIUM SPEAKER	ICMP		0.000	N	0	(edit)	

Figure 4.34 : PDU du téléphone chef amphithéâtre et stade vers le Haut-parleur

4.4.2. TEST AU NIVEAU DU RESEAU METROPOLITAIN

Nous allons d'abord tester la connectivité entre les routeurs, car ce sont eux qui assurent la connexion entre les différents départements.

4.4.2.1. Test entre les routeurs

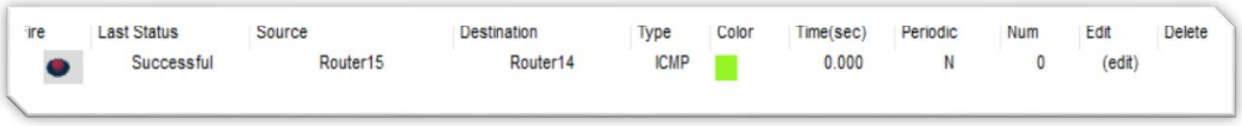
Ping Routeur15 ➔ Routeur14

```
Routeur15#ping 192.168.13.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Figure 4.35 : Ping entre routeur15 et routeur14

Test avec PDU :



ire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router15	Router14	ICMP		0.000	N	0	(edit)	

Figure 4.36 : PDU entre routeur15 et routeur14

Ping Routeur15 ➔ Routeur11

```
Routeur15#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/27/97 ms
```

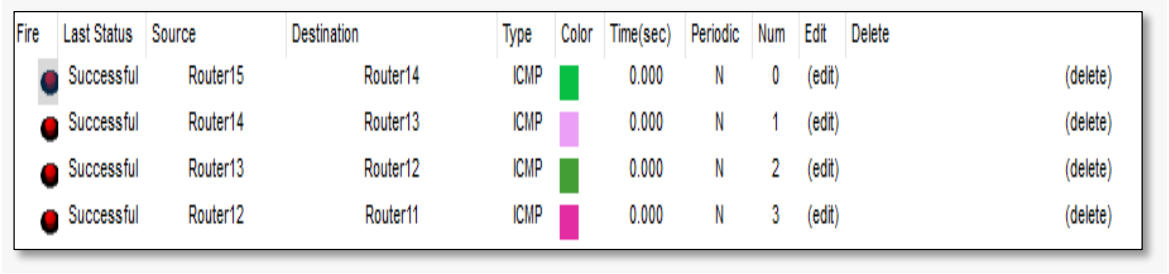
Figure 4.37 : Ping entre routeur 15 et routeur 11

Teste avec PDU :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router15	Router11	ICMP		0.000	N	0	(edit)	

Figure 4.38 : PDU entre routeur15 et routeur11

Test PDU entre tous les Routeurs :



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router15	Router14	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Router14	Router13	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Router13	Router12	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Router12	Router11	ICMP		0.000	N	3	(edit)	(delete)

Figure 4.39 : PDU entre tous les routeurs

4.4.2.2. Test entre les appareils

Vu que tous les routeurs sont connectés entre eux, nous allons maintenant tester la connectivité entre l'ordinateur portable du directeur et un appareil représentatif de chaque département.

Ping ordinateur portable du directeur ➔ Garage du Parking (192.168.7.8)

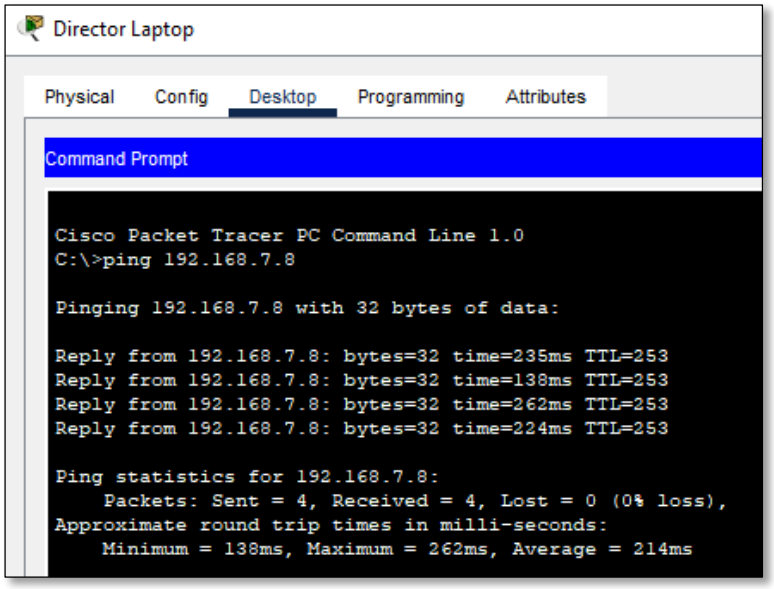


Figure 4.40 : Ping ordinateur portable du directeur vers Garage du Parking

Test avec PDU :

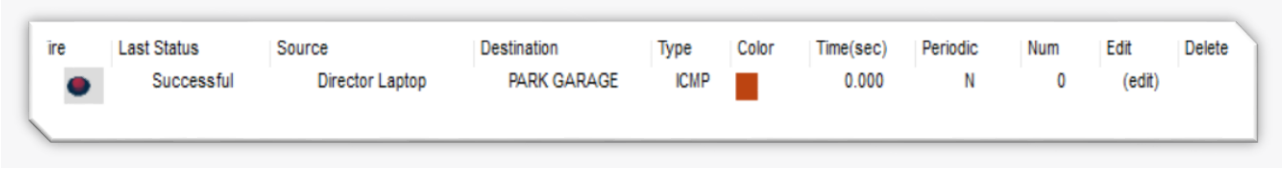


Figure 4.41 : PDU ordinateur portable du directeur vers Garage du Parking

Ping ordinateur portable du directeur ➔ Climatiseur Labo (192.168.2.50)

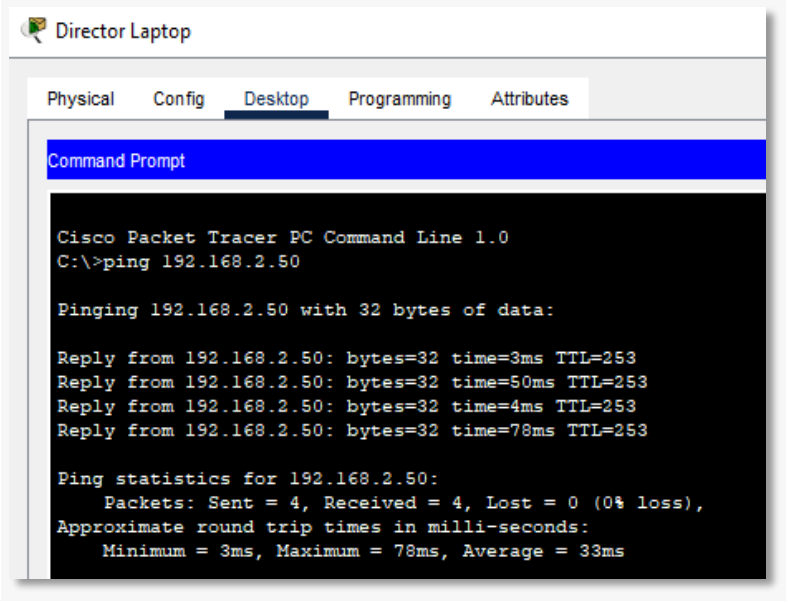


Figure 4.42 : Ping ordinateur portable du directeur vers Climatiseur Laboratoire

Test avec PDU :

Figure 4.43 : PDU ordinateur portable du directeur vers Climatiseur Laboratoire

Ping ordinateur portable du directeur ➔ Ventilateur bibliothèque (192.168.8.3)

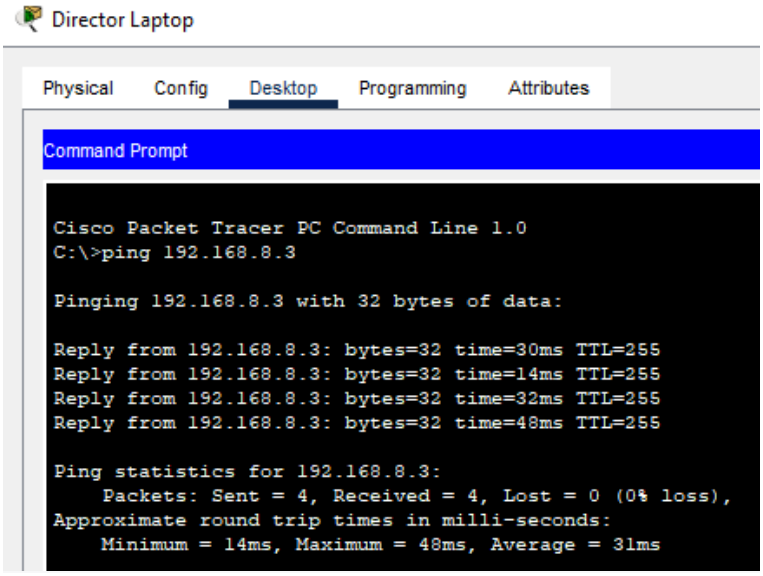


Figure 4.44 : Ping ordinateur portable du directeur vers Ventilateur bibliothèque

Test avec PDU :

Figure 4.45 : PDU ordinateur portable du directeur vers Ventilateur bibliothèque

Ping ordinateur portable du directeur ➔ Haut-parleur Bluetooth (192.168.1.7)

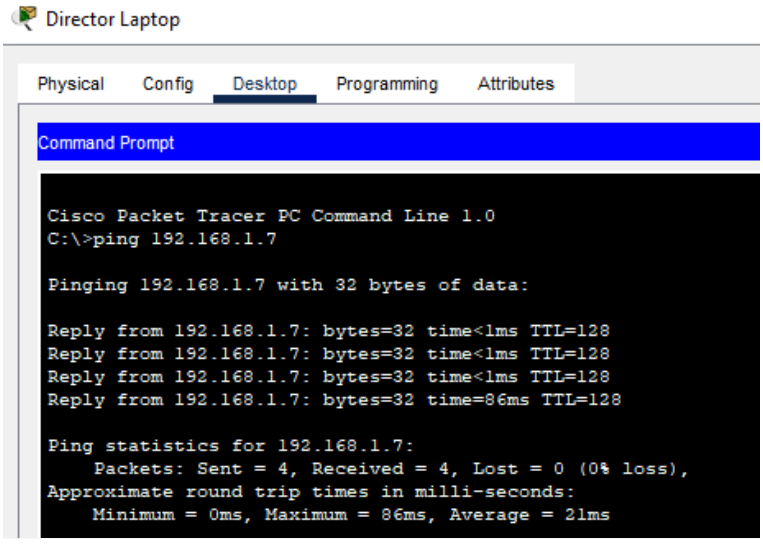


Figure 4.46 : Ping ordinateur portable du directeur vers Haut-parleur Bluetooth

Test avec PDU :

Figure 4.47 : PDU ordinateur portable du directeur vers Haut-parleur Bluetooth

Grâce aux tests de connectivité réalisés, nous avons pu confirmer que tous les appareils des différents départements de l'université étaient connectés et pouvaient échanger des données.

Les résultats des tests ont démontré la robustesse du réseau, permettant ainsi une communication fluide et efficace entre les départements.

4.5 - TEST DE L'UTILISATION MANUELLE DES APPAREILS IOT

Sachant que chaque chef de département a le contrôle du réseau de son département spécifique et le directeur a le contrôle de l'ensemble du réseau de l'université. Cette hiérarchie de contrôle permet une gestion efficace et une responsabilité claire pour chaque département.

Nous allons procéder à une série d'exemples pour évaluer le contrôle manuelle des objets connectées. Plus précisément, nous allons mettre en évidence le contrôle du directeur de l'université sur un appareil situé dans le réseau de l'administration, ainsi que sur deux appareils situés dans d'autres réseaux locaux.

Le test consistera à vérifier la capacité du directeur à accéder et à contrôler ces appareils à distance depuis son poste de travail. Cela permettra de démontrer la fonctionnalité du système de gestion réseau et l'autorité du directeur sur l'ensemble de l'université.

4.5.1. TEST AU NIVEAU DU RESEAU DE L'ADMINISTRATION

Pour chaque scenario nous allons d'abord accéder au compte du serveur IoT du réseau ou se trouve notre Object connecter.

Scénario 1 : Le Directeur contrôle la camera de l'administration avec son ordinateur portable.

L'accès au serveur IoT de l'administration nécessite l'utilisation du domaine du serveur « www.smartuniversity.com » ainsi que d'un nom d'utilisateur et d'un mot de passe. (Voir la figure 4.45).

Figure 4.48 : connexion au serveur de l'administration

Une fois connecté, tous les appareils IoT connecté au serveur de l'administration s'afficheront. Comme illustre la figure 4.49.

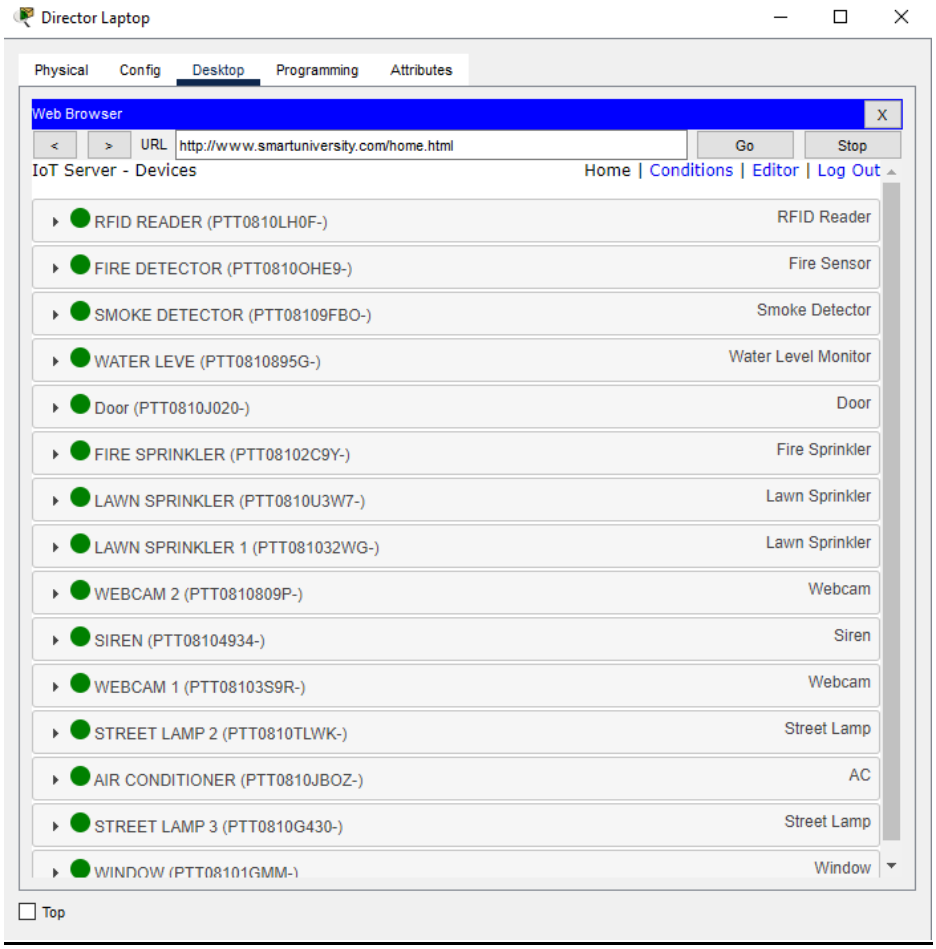


Figure 4.49 : interface du serveur de l'administration

Maintenant, nous avons la possibilité de modifier à distance l'état de la plupart des appareils depuis l'ordinateur portable du directeur.

➪ **La caméra de surveillance**

Le directeur peux surveiller l'administration depuis la camera en juste l'allument.

La camera par default est éteinte

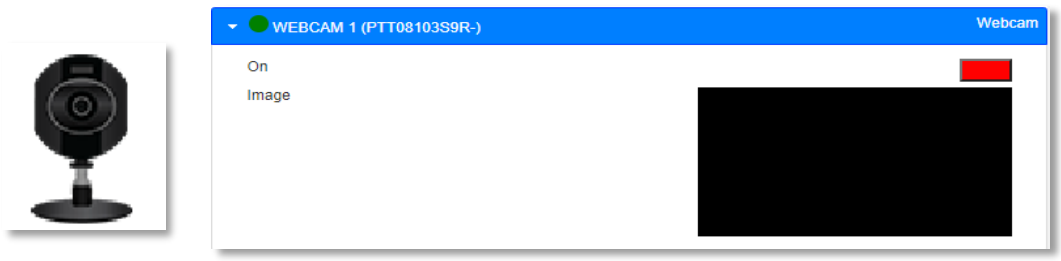


Figure 4.50 : état de la camera éteinte

Après avoir cliqué sur "ON", le camera s'allume et commence à filmer.

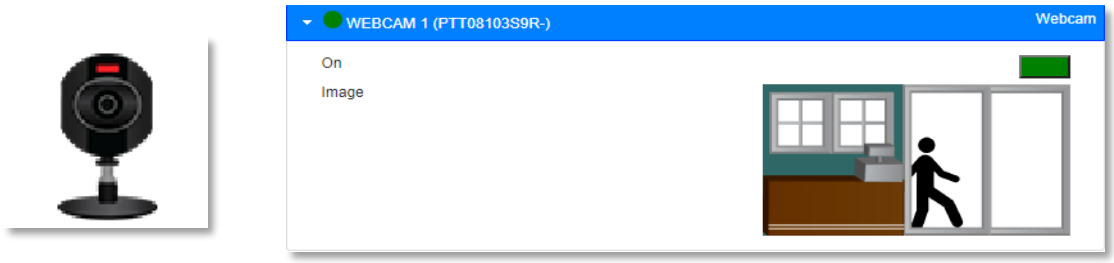


Figure 4.51 : état de la camera allumer

4.5.2. TEST AU NIVEAU DU RESEAU DU LABORATOIRE

Scenario 1 : Le Directeur contrôle le climatiseur du Laboratoire avec son ordinateur portable.

Le Directeur doit d'abord accéder au serveur du Laboratoire avec le nom de domaine « www.labuniversity.com ».ensuite contrôler depuis l'interface du serveur.

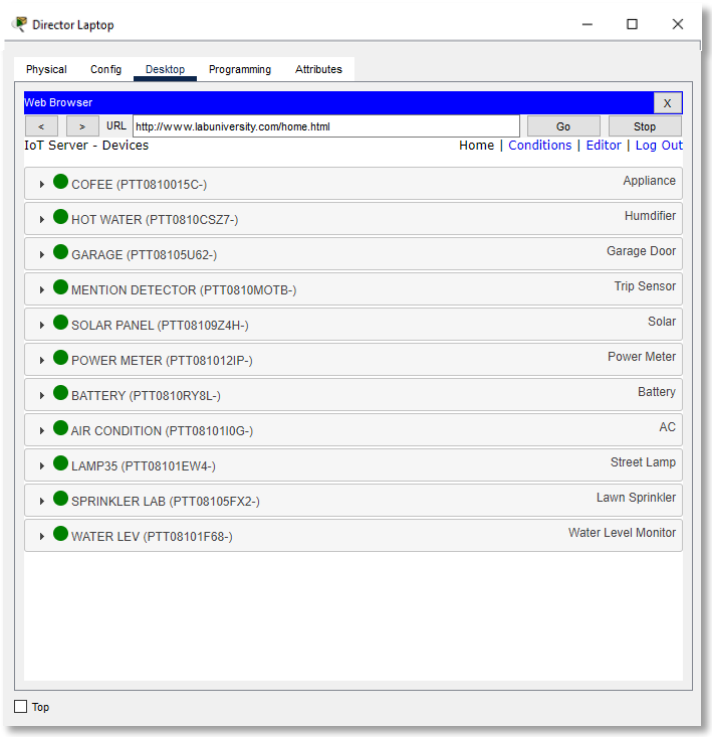


Figure 4.52 : interface du serveur du laboratoire

⇨ **CLIMATISEUR**

Le climatiseur par défaut est éteint comme indiqué sur la figure 4.50

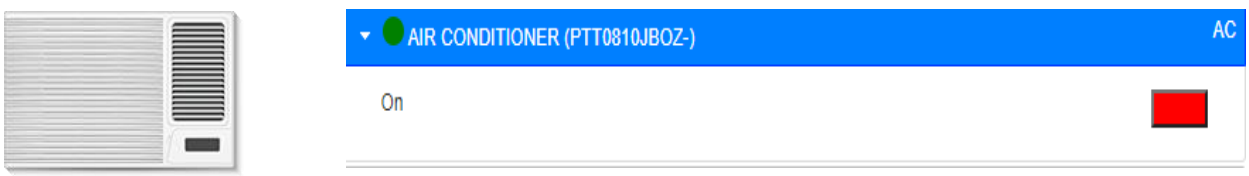


Figure 4.53 : état du climatiseur éteint

Après avoir cliqué sur le rectangle rouge, il devient vert comme illustré à la figure 5 et allume le climatiseur.

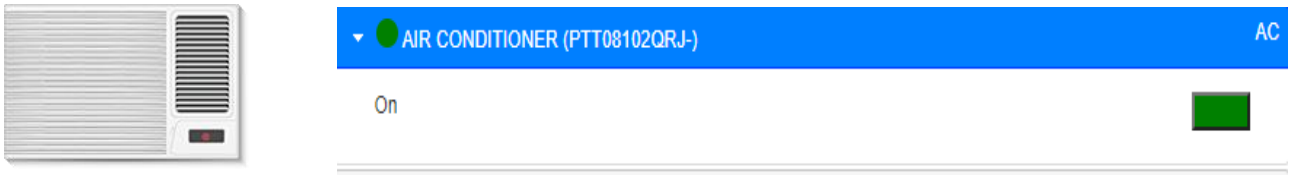


Figure 4.54 : état du climatiseur allumé

4.5.3. TEST AU NIVEAU DU RESEAU DE LA BIBLIOTHEQUE

Scenario 1 : Le Directeur contrôle la fenêtre de la bibliothèque avec son ordinateur portable.

Comme nous l'avons mentionné précédemment, le directeur doit d'abord accéder au serveur de la bibliothèque avec le nom de domaine "www.libuniversity.com » Une fois connecté au serveur, il peut vérifier et contrôler les fonctionnalités depuis son interface.

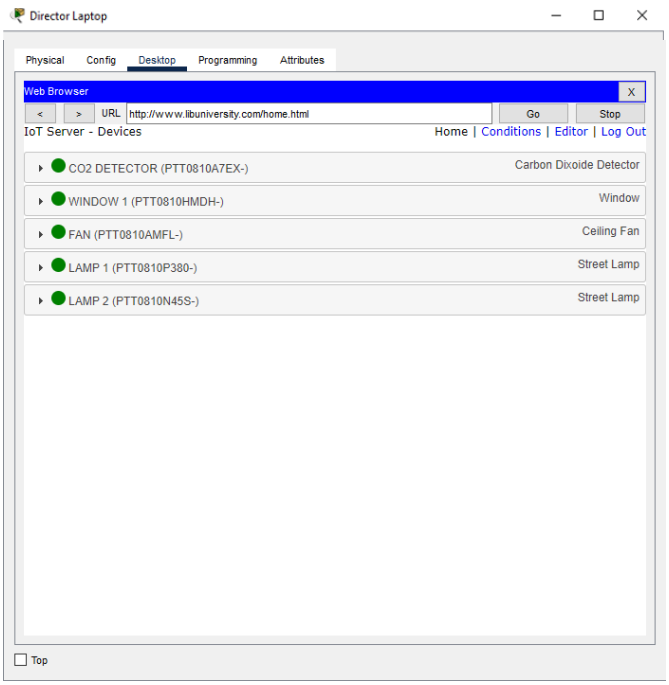


Figure 4.55 : interface du serveur de la bibliothèque

⇨ **<u>La fenêtre</u>**

La fenêtre aussi, par défaut, est fermée

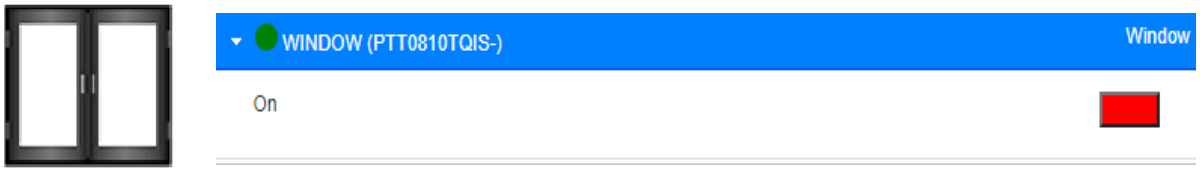


Figure 4.56 : état de la fenêtre fermer

Après avoir cliqué sur le rectangle rouge, il devient vert comme illustré à la figure 4.54 et ouvre la fenêtre.

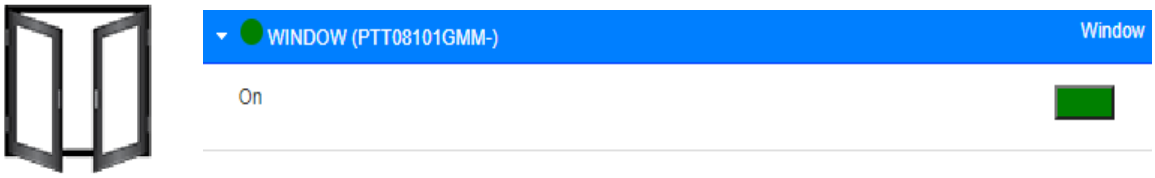


Figure 4.57 : état de la fenêtre ouverte

Nous avons démontré avec succès la capacité de contrôler manuellement les objets IoT de notre université, offrant ainsi des opportunités d'amélioration des opérations et de l'efficacité, tout en tenant compte des aspects de sécurité et de gestion appropriés.

4.6 - TEST DE L'UTILISATION AUTOMATIQUE DES APPAREILS IOT

Dans le chapitre 3, nous avons exploré l'interaction entre les différents objets connectés et les systèmes automatisés que nous avons mis en place au sein de notre université. Dans cette partie, nous allons présenter comment on a pu mettre en place c'est systèmes et on va les tester. Pour permettre aux dispositifs connectés de fonctionner de manière autonome, sans intervention humaine directe.

L'utilisation de l'automatisation dans le contexte des appareils IoT offre de nombreux avantages, tels que l'optimisation des processus, la réduction des tâches manuelles, la gestion énergétique efficace et l'amélioration de l'expérience utilisateur.

4.6.1 - SYSTEME AUTOMATIQUE DE L'ADMINISTRATION :

⇨ **La Porte intelligente :**

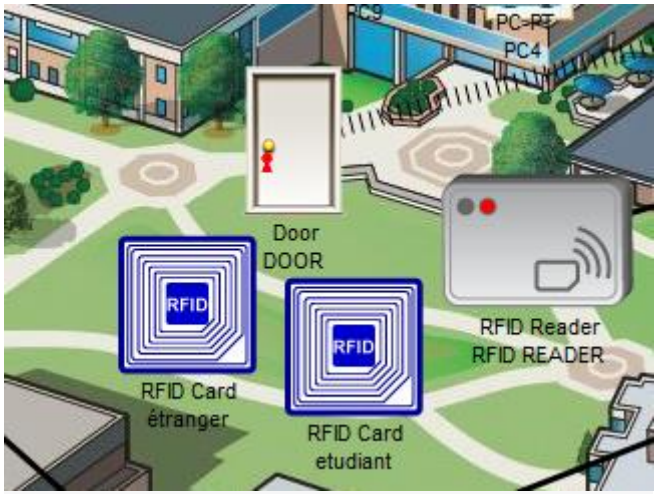


Figure 4.58 : Système automatique de la porte intelligente

Pour cette partie, la sécurité de la porte est testée à l'aide des deux cartes (un étudiant) et (un étranger). Sachant que le code valide pour le lecteur RFID est "1001", ce même code a été attribué à la carte de l'étudiant.

Voici les conditions que nous avons effectuées pour ce système :

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	ENTRE	RFID READER Card ID = 1001	Set RFID READER Status to Valid
Edit Remove	Yes	PAS ENTRE	RFID READER Card ID != 1001	Set RFID READER Status to Invalid
Edit Remove	Yes	OPEN DOOR	RFID READER Status is Valid	Set PTT08107I2R- Lock to 0
Edit Remove	Yes	CLOSE DOOR	RFID READER Status is Waiting	Set PTT08107I2R- Lock to 1

Figure 4.59 : conditions du système de la porte

Scenario 1 : Dans ce scénario, une personne non autorisée ou utilisant une carte invalide approche la porte avec sa carte d'accès. Le lecteur RFID vérifie le code de la carte et constate qu'il ne correspond pas au code valide "1001" ou qu'il est invalide. En conséquence, la porte reste verrouillée et refuse l'accès à cette personne comme montre la figure.

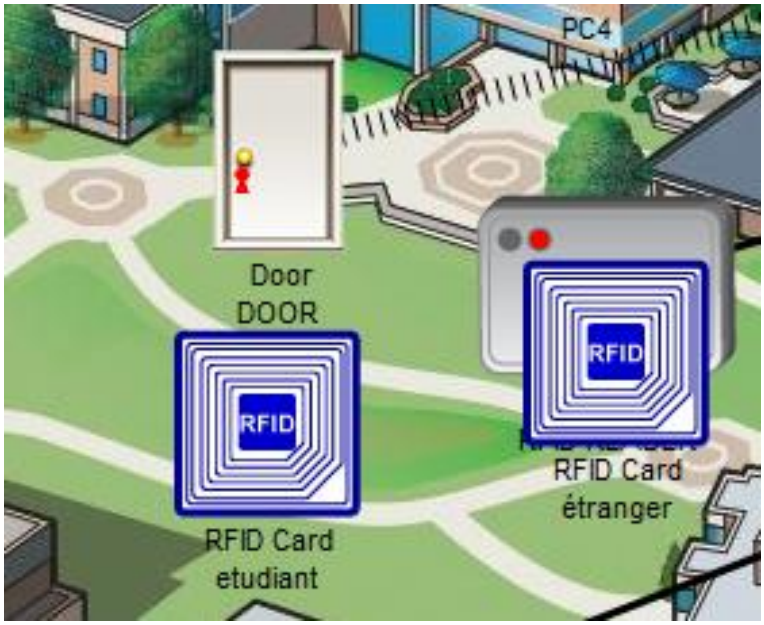


Figure 4.60 : porte intelligente verrouiller

Scenario 2 : Dans ce scénario, l'étudiant approche sa carte d'accès du lecteur RFID de la porte. Le lecteur RFID vérifie le code de la carte et constate qu'il correspond au code valide, c'est-à-dire "1001". En conséquence, la porte se déverrouille et s'ouvre, permettant à l'étudiant autorisé d'accéder à l'intérieur de l'administration. Comme illustre la figure

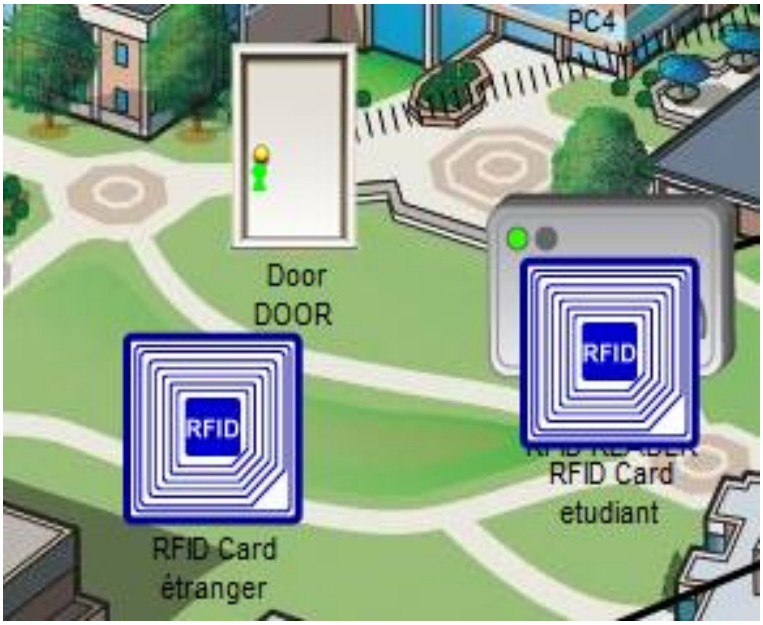


Figure 4.61 : porte intelligente déverrouiller

Ces deux scénarios démontrent comment le système de sécurité de la porte de l'administration fonctionne en accordant l'accès uniquement aux utilisateurs autorisés avec des cartes valides, tandis qu'il refuse l'accès aux personnes non autorisées ou avec des cartes invalides.

- **Le Moniteur d'incendie :**

Figure 4.62 : système automatique du moniteur d'incendie

Dans Cisco Packet Tracer, il n'y a pas d'objet spécifique qui simule directement le feu pour tester notre système. C'est pour ça on va utiliser l'objet « élément chauffant » et on va le programmer avec un programme java script pour simuler le feu.

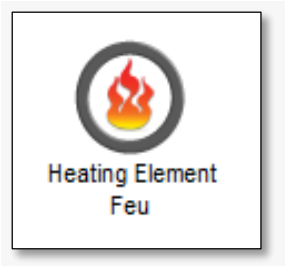


Figure 4.63 : élément chauffant

Voici le programme java script qu'on a utilisés :

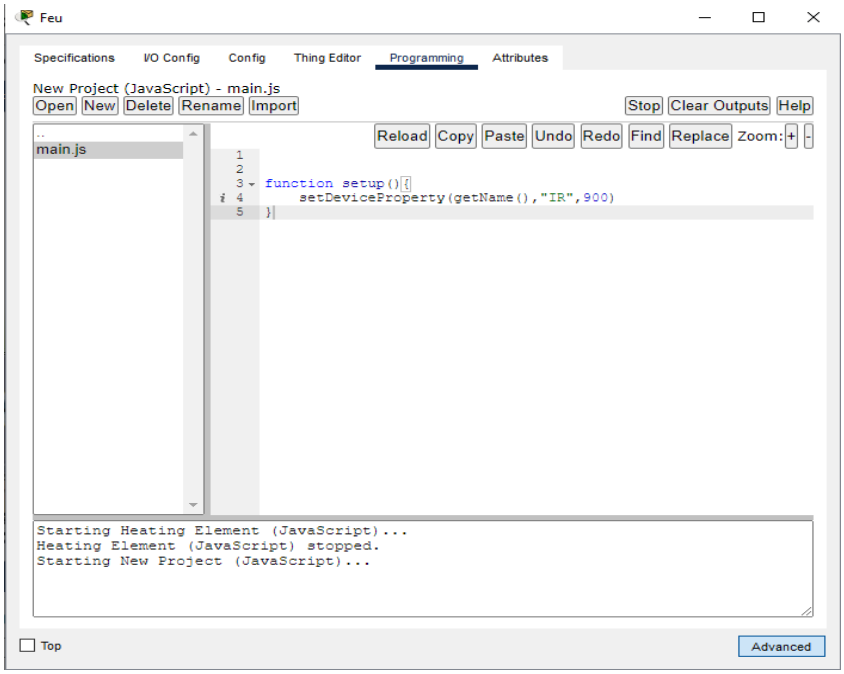


Figure 4.64 : programme JavaScript pour le feu

Voici les conditions que nous avons effectuées pour ce système :

Edit Remove	Yes	FIRE	FIRE DETECTOR Fire Detected is true	Set FIRE SPRINKLER Status to true Set SIREN On to true
Edit Remove	Yes	NO FIRE	FIRE DETECTOR Fire Detected is false	Set FIRE SPRINKLER Status to false Set SIREN On to false

Figure 4.65 : conditions du système du moniteur d'incendie

Scenario 1 : Le moniteur d'incendie dans l'administration est testé en cas d'absence d'incendie(le feu qu'on a programmé est loin). Lorsqu'il n'y a pas d'incendie détecté, le gicleur d'incendie reste inactif, ce qui signifie qu'aucune eau n'est libérée. De plus, la sirène reste silencieuse car il n'y a pas d'alarme à déclencher. Comme illustre la figure

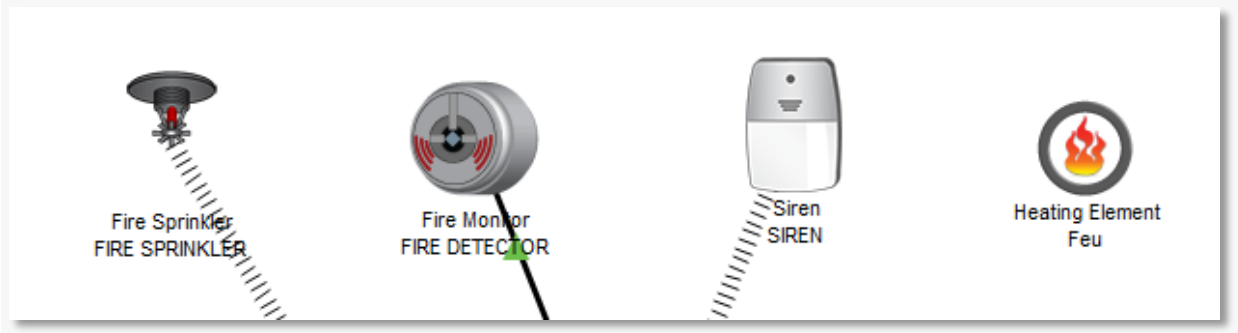


Figure 4.66 : le système d'incendie désactivé

Scenario 2 : Le moniteur d'incendie dans l'administration est testé en cas de détection d'incendie(le feu qu'on a programmé est prêt). Lorsqu'un incendie est détecté, le gicleur d'incendie

est activé, libérant de l'eau pour éteindre le feu. En même temps, le système déclenche la sirène pour alerter les occupants de l'incendie en cours. Comme montre la figure suivante :

Figure 4.67 : le système d'incendie activé

Ces deux scénarios illustrent le fonctionnement du moniteur d'incendie. Le premier scénario montre sa réaction appropriée lors de la détection d'un incendie, en activant les mesures d'extinction et en émettant une alarme sonore. Le deuxième scénario met en évidence sa capacité à rester inactif lorsqu'aucun incendie n'est détecté, évitant ainsi les fausses alarmes.

4.6.2 - SYSTEME AUTOMATIQUE DU PARKING :

➪ **Système de Parking Intelligent :**

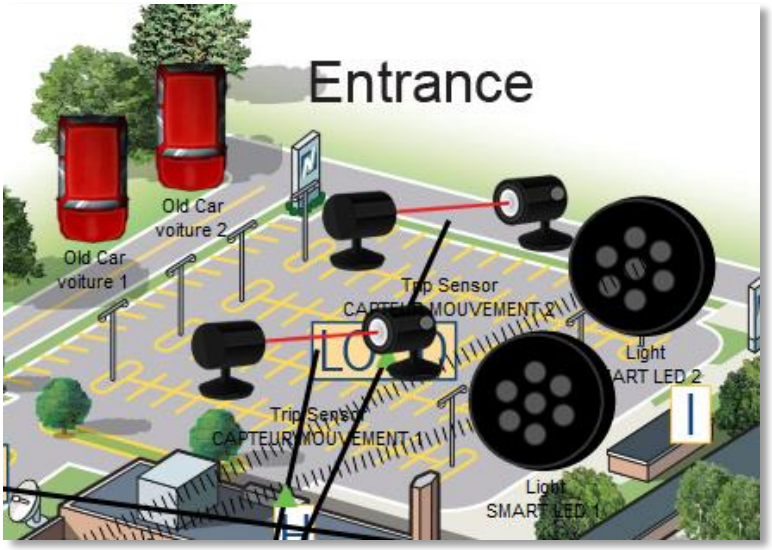


Figure 4.68 : système automatique du parking intelligent

Le système de Parking Intelligent est un système automatisé qui vise à détecter et indiquer la disponibilité des places de stationnement dans un parking. Il utilise des capteurs pour détecter la présence de véhicules dans les emplacements de stationnement et des LED intelligentes pour indiquer visuellement l'état d'occupation de chaque place. Grâce à ce système, les conducteurs peuvent rapidement repérer les places de stationnement libres et optimiser leur recherche, ce qui améliore l'efficacité du stationnement et réduit les temps d'attente.

Voici les conditions que nous avons utilisées pour ce système :

Edit Remove	Yes	VOITURE EN POSITION	CAPTEUR MOUVEMENT 1 On is true	Set SMART LED 1 Status to On
Edit Remove	Yes	AUCUNE VOITURE	CAPTEUR MOUVEMENT 1 On is false	Set SMART LED 1 Status to Off
Edit Remove	Yes	VOITURE EN POSITION 2	CAPTEUR MOUVEMENT 2 On is true	Set SMART LED 2 Status to On
Edit Remove	Yes	AUCUNE VOITURE 2	CAPTEUR MOUVEMENT 2 On is false	Set SMART LED 2 Status to Off

Figure 4.69 : conditions du système du parking intelligent

Scenario 1 : Une voiture arrive et se gare sur la place de parking correspondante. Le capteur 1 détecte la présence de la voiture et envoie un signal au système.

En recevant ce signal, le système active la LED intelligente 1 pour indiquer que la place de parking est occupée. La LED intelligente 2 reste éteinte car la place de parking correspondante est libre.

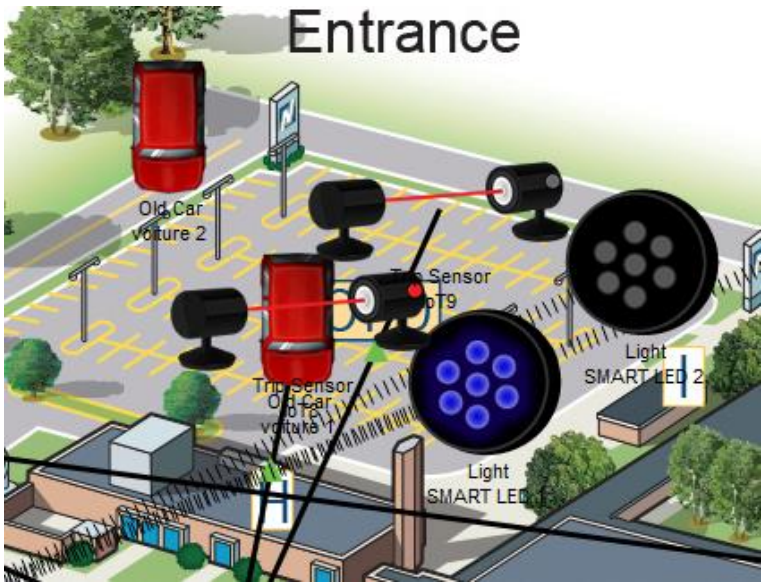


Figure 4.70 : LED 1 allumée et LED 2 éteinte

Scenario 2 : Une deuxième voiture arrive et se gare sur la place de parking correspondante. Le capteur 2 détecte la présence de la voiture et envoie un signal au système.

Le système réagit en activant la LED intelligente 2 pour indiquer que la place de parking est occupée. Dans ce cas, la LED intelligente 1 reste éteinte car la place du parking correspondante est libre.

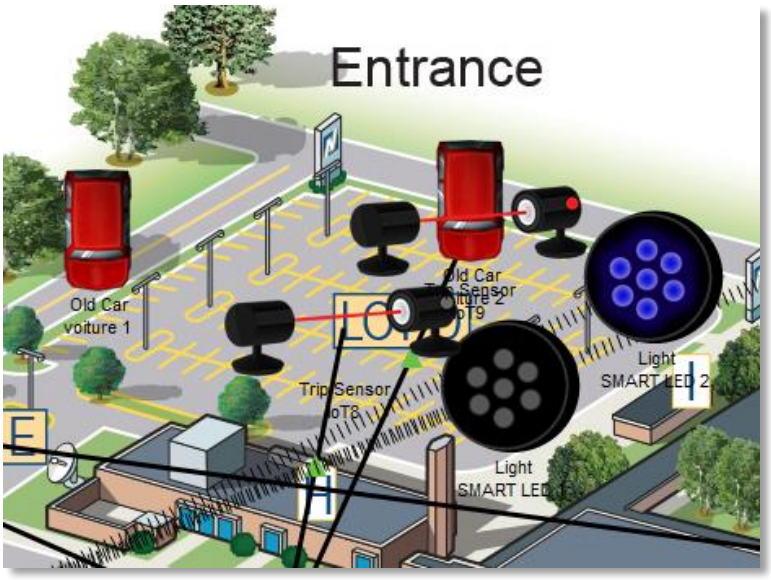


Figure 4.71 : LED 2 allumée et LED 1 éteinte

Scenario 3 : les deux voitures arrivent et se gares sur les deux places du parking correspondantes. Les deux capteurs détectent la présence des voitures et envoient un signal au système.

Le système réagit en activant la LED intelligente 2 et 1 pour indiquer que les places du parking sont occupées.

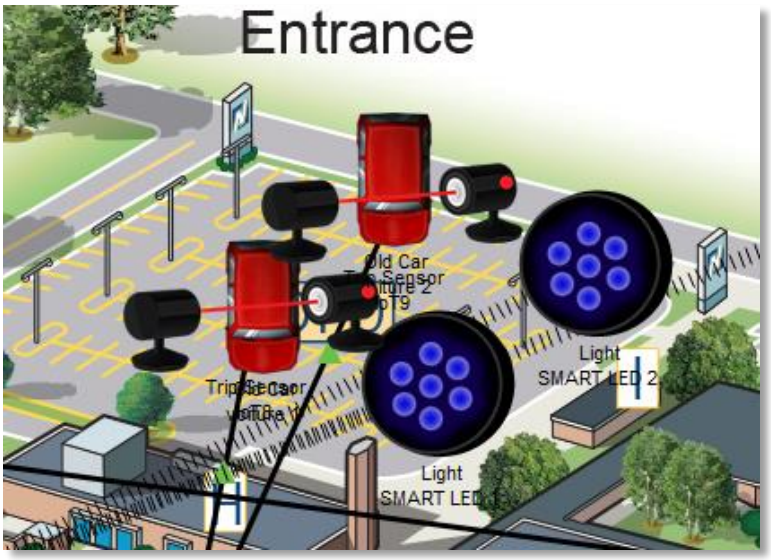


Figure 4.72 : LED 2 allumée et LED 1 allumée

Dans les trois scénarios, le système automatique du parking détecte chaque voiture à l'aide du capteur correspondant et réagit en allumant la LED intelligente appropriée pour indiquer l'occupation de la place de parking.

4.6.3. SYSTEME AUTOMATIQUE DE LA BIBLIOTHEQUE :

➪ **Détecteur de fumée :**

Figure 4.73 : système automatique pour détecter la fumée

Dans Cisco Packet Tracer, il n'y a pas de fonctionnalité native pour simuler directement la fumée pour cela on va utiliser une vieille voiture qui génère de la fumée.

Voici les conditions que nous avons utilisées pour ce système :

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	CO2	CO2 DETECTOR Level > 0.1	Set WINDOW 1 On to true
Edit Remove	Yes	NO CO2	CO2 DETECTOR Level < 0.1	Set WINDOW 1 On to false

Figure 4.74 : conditions du système de détection de fumée

Scenario 1 : Dans ce scénario, nous veillons à ce qu'il n'y ait pas de fumée ou de CO2 générés dans la pièce.

Le détecteur de CO2 doit rester inactif et la fenêtre doit rester fermée tant que le niveau de CO2 reste en dessous du seuil prédéfini (0.1 PM).

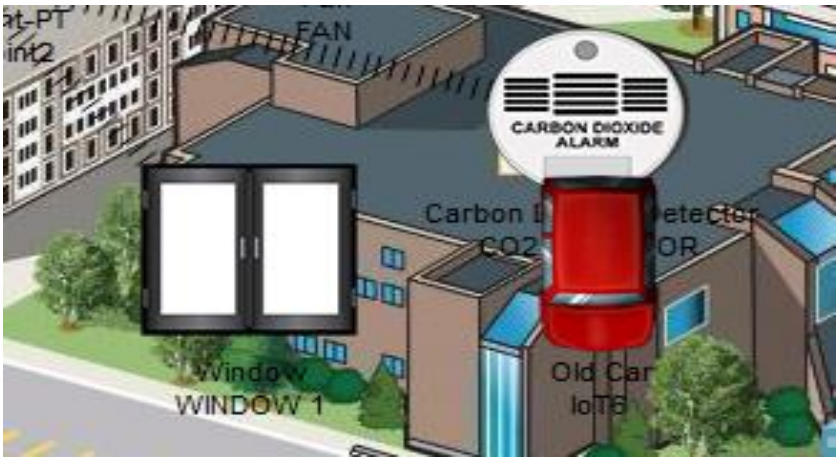


Figure 4.75 : système de détection désactivé

La figure ci-dessus montre la valeur du Co2 détecté par le détecteur

Properties:

	Property	Value
1	PROGRAMMING_EDITING_DIR	
2	level	0
3	state	0

Figure 4.76 : Niveau de fumée détecté

Scenario 2 : Dans ce scénario, nous allons simuler la présence de CO2 en utilisant une vieille voiture qui génère de la fumée. Lorsque le niveau de CO2 atteint une valeur plus grande que 0.1 PM, le détecteur de CO2 doit déclencher une action, en l'occurrence l'ouverture automatique de la fenêtre pour permettre l'évacuation de la fumée et du CO2.

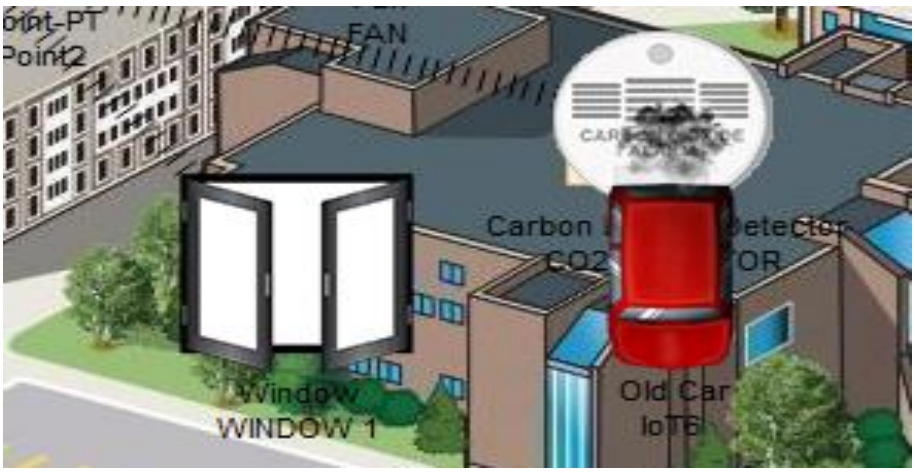


Figure 4.78 : système de détection activé

La figure ci-dessus montre la valeur du Co2 détecté par le détecteur

Properties:

	Property	Value
1	PROGRAMMING_EDITING_DIR	
2	level	0.2785640060901642
3	state	0

Figure 4.79 : niveau de fumée détecté 2

Ces scénarios d'essai du détecteur de CO2 permettent d'évaluer sa réactivité et sa précision dans la détection de la présence de CO2, garantissant ainsi la sécurité des occupants en cas de présence de CO2.

4.6.4. SYSTEME AUTOMATIQUE DU LABORATOIRE :

➪ **Système de climatisation solaire autonome**

Ce système est composé d'un panneau solaire chargé de convertir l'énergie solaire en électricité, d'une batterie pour stocker cette électricité, d'un climatiseur qui est alimenté par la batterie et d'un wattmètre utilisé pour mesurer la consommation électrique du climatiseur.

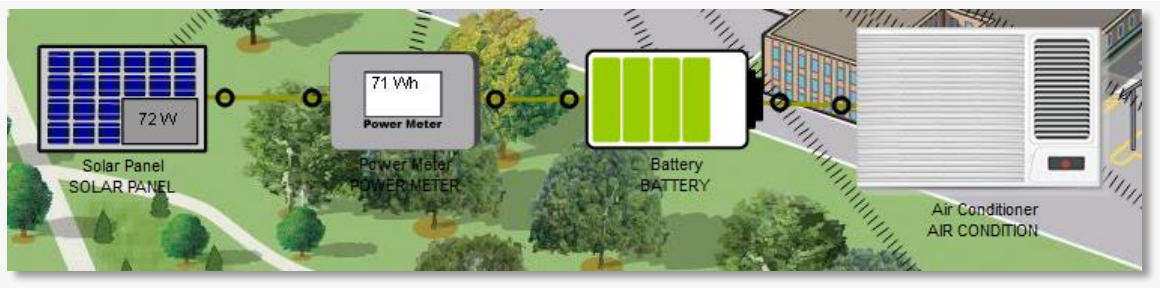


Figure 4.80 : système automatique de climatisation autonome

Scenario 1 : en plein jour. Dans ce scénario, le panneau solaire est exposé à une forte intensité lumineuse et génère une quantité optimale d'énergie solaire. Cette énergie est utilisée pour charger la batterie, qui alimente ensuite le climatiseur.

Environnement logique de Cisco packet tracer montre que l'heure est 11.20 AM

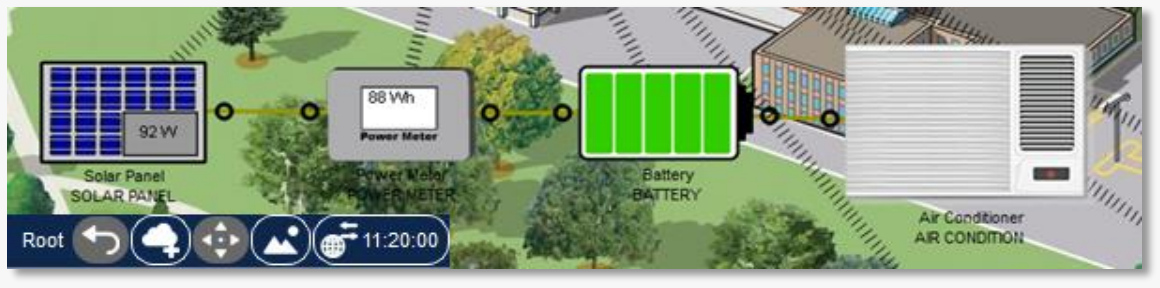


Figure 4.81 : Batterie qui se charge

Scenario 2 : pendant la nuit. Dans ce scénario, le panneau solaire ne reçoit pas de lumière solaire directe et ne génère donc pas d'énergie solaire. La batterie, qui a été chargée pendant la journée, est utilisée comme source d'alimentation pour le climatiseur pendant la nuit.

L'Environnement logique de Cisco packet tracer montre que l'heure est 2.08 PM

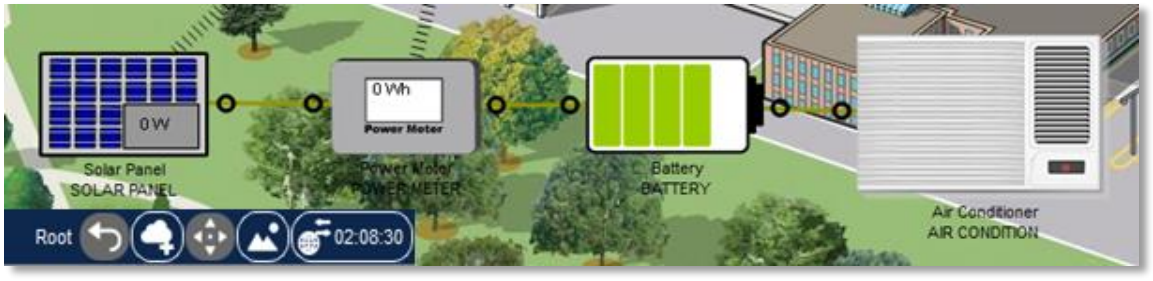


Figure 4.82 : batterie qui se décharge

Les deux scénarios de test, tant pendant la journée que pendant la nuit, ont permis de mettre en évidence les performances et la fiabilité du système.

➪ **Automatisation du garage avec capteur de déclenchement**

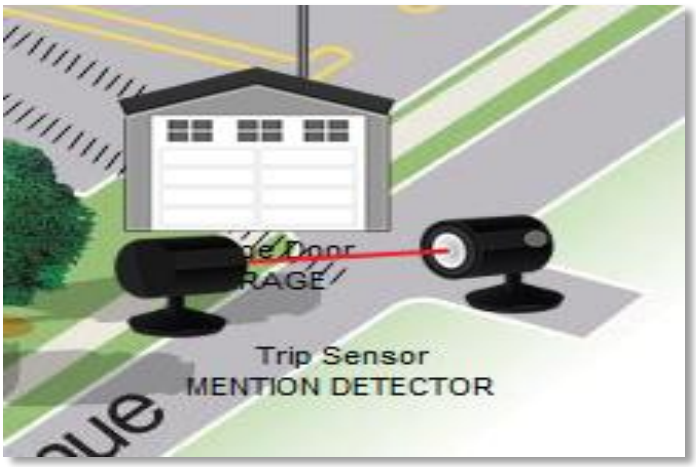


Figure 4.83 : système automatique de détection

Voici les conditions du système :

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	GARAGE OPEN	MENTION DETECTOR On is true	Set GARAGE On to true
Edit Remove	Yes	GARAGE CLOSE	MENTION DETECTOR On is false	Set GARAGE On to false

Figure 4.84 : conditions du système de détection

Scenario 1 : Lorsqu'une voiture est détectée par le capteur de déclenchement du garage, le système se met automatiquement en action.

Les portes du garage s'ouvrent, permettant à la voiture d'entrer. Une fois que la voiture est entièrement à l'intérieur, les portes se referment pour assurer la sécurité du véhicule.

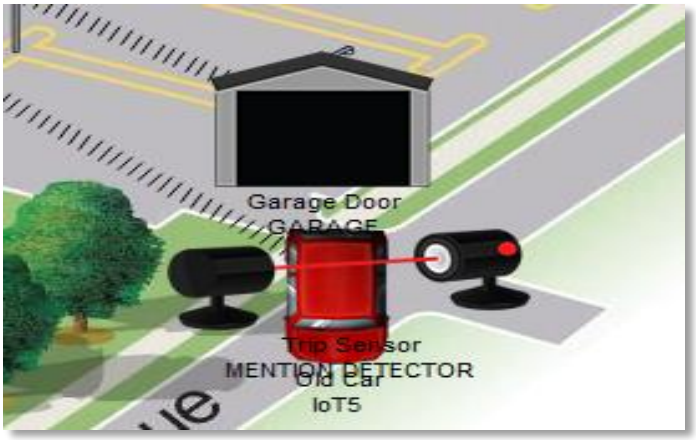


Figure 4.85 : système de détection activé

Scenario 2 : En l'absence de détection de voiture par le capteur, le système reste en état de veille. Les portes du garage restent fermées.

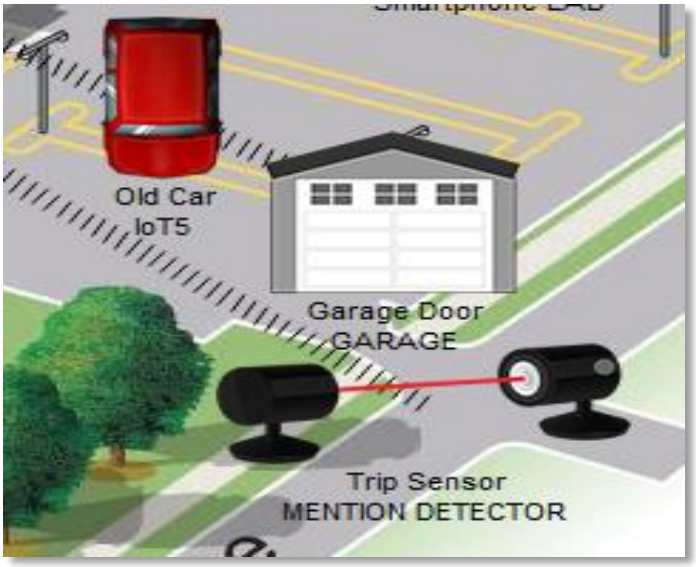


Figure 4.86 : système de détection désactivé

Les scénarios de détection de voiture et d'absence de détection ont démontré son efficacité dans l'ouverture et la fermeture automatique des portes du garage en fonction de la présence d'un véhicule.

4.6.5. SYSTEME AUTOMATIQUE DE L'AMPHITHEATRE :

➪ **Contrôle intelligent de la température :**

Le système est conçu pour assurer un contrôle intelligent de la température dans un environnement donné.

Il utilise des capteurs de température pour surveiller en temps réel les variations de température et ajuste automatiquement le fonctionnement du climatiseur pour maintenir des conditions de confort optimales.

Condition du système :

Edit Remove	Yes	turn on air conditioner	TEMPERATURE Temperature >= 30.0 °C	Set AIR CONDITIONE On to true
Edit Remove	Yes	turn off air conditioner	TEMPERATURE Temperature < 30.0 °C	Set AIR CONDITIONE On to false

Figure 4.87 : conditions du système de contrôle de température

Scenario 1 : Lorsque la température dans l'amphithéâtre est inférieure à 30 degrés Celsius, Le système détecte que la température est dans la plage de confort et aucun besoin supplémentaire de refroidissement n'est nécessaire.

Par conséquent, aucun signal n'est envoyé au climatiseur et celui-ci reste éteint.

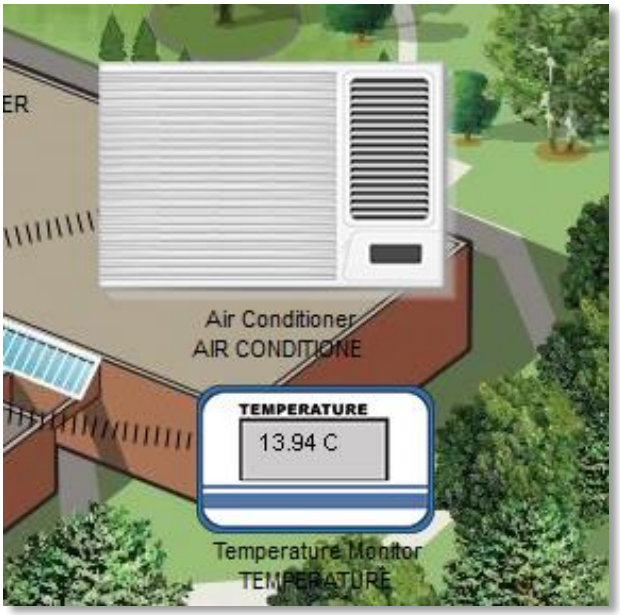


Figure 4.88 : climatiseur éteint

Scenario 2 : Lorsque la température dans l'amphithéâtre atteint ou dépasse les 30 degrés Celsius, Le système détecte la hausse de température et envoie un signal au climatiseur pour le démarrer.

Le climatiseur s'allume et commence à réduire la chaleur ambiante, procurant une sensation de fraîcheur.

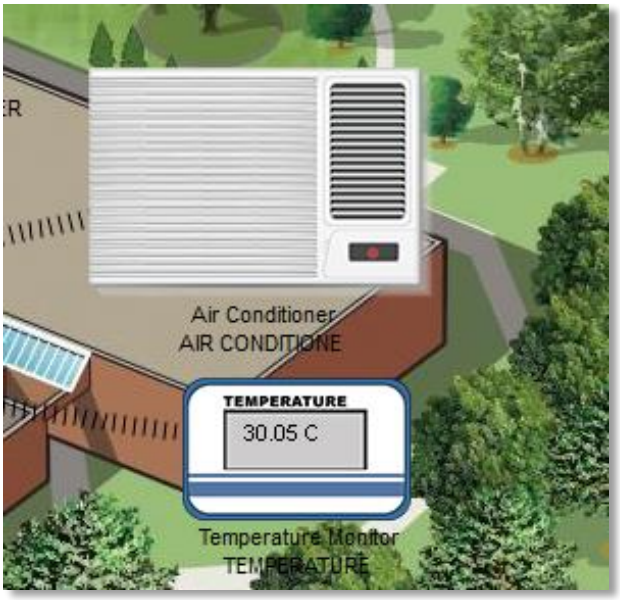


Figure 4.89 : climatiseur allumé

Ces scénarios illustrent l'efficacité du système dans la régulation de la température en fonction des besoins réels, garantissant un confort thermique optimal et une gestion énergétique efficace.

4.6.6 - SYSTEME AUTOMATIQUE DU STADE :

➪ **Système d'arrosage intelligent :**

Le système comprend un moniteur de niveau d'eau, deux arroseurs de gazon et un détecteur de mouvement. Le moniteur de niveau d'eau est responsable de mesurer et de surveiller en continu le niveau d'eau dans le système d'arrosage. L'arroseur 1 est placé dans le stade et l'arroseur 2 est placé au dehors du stade pour fournir un arrosage efficace et uniforme du gazon.

Condition du système :

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	turn on sprinkler 1	WATER LEVEL Water Level <= 5.0 cm	Set SPINKLER 1 Status to true
Edit Remove	Yes	turn off sprinkler	WATER LEVEL Water Level > 5.0 cm	Set SPINKLER 1 Status to false
Edit Remove	Yes	turn on sprinkler 2	WATER LEVEL Water Level <= 5.0 cm	Set SPRINKLER 2 Status to true
Edit Remove	Yes	turn off sprinkler 2	WATER LEVEL Water Level > 5.0 cm	Set SPRINKLER 2 Status to false
Edit Remove	Yes	sprinkler 1 turn off	MOTION MONITOR On is true	Set SPINKLER 1 Status to false

Figure 4.90 : conditions du système d'arrosage

Scenario 1 : Le niveau d'eau dans le système est supérieur à 5 cm, ce qui indique un niveau d'eau adéquat pour l'arrosage du gazon. Dans cette situation,

Les deux arroseurs restent éteints car il n'est pas nécessaire de les activer.

Figure 4.91 : le gazon n'est pas arroser

Scenario 2 : Lorsque le niveau d'eau dans le système est égal ou inférieur à 5 cm et qu'il n'y a aucun joueur dans le stade, les deux arroseurs sont activés. Le système détecte que le niveau d'eau est bas et qu'il est nécessaire d'arroser le gazon.

Figure 4.92 : Arrosage du gazon

Scenario 3 : Lorsque le niveau d'eau dans le système est égal ou inférieur à 5 cm et qu'il y a des joueurs dans le stade, seul l'arroseur 2 est activé. Le système utilise le détecteur de mouvement pour détecter la présence de joueurs dans le stade. Compte tenu de la sécurité des joueurs, l'arroseur 1 reste inactif afin d'éviter tout risque d'accident lié à l'arrosage. Cependant, l'arroseur 2 est activé pour maintenir un niveau d'humidité adéquat dans les zones où les joueurs ne se trouvent pas.

Figure 4.93 : Arrosage du gazon par arroseur 2

4.7 - CONCLUSION

En conclusion, ce chapitre a été consacré à la configuration, à l'évaluation de la connectivité et aux tests de fonctionnement des objets IoT dans le cadre de l'université intelligente.

Nous avons réalisé avec succès la configuration des réseaux de l'université, tous les tests ont été réussis, démontrant ainsi le bon fonctionnement des dispositifs IoT et leur capacité à interagir de manière fiable avec le réseau.

Ces résultats sont encourageants pour la mise en place d'un environnement technologique avancé qui facilite la gestion efficace des ressources et améliore l'expérience des utilisateurs au sein de l'université.

CONCLUSION GENERALE

CONCLUSION GENERALE ET PERSPECTIVES

En conclusion, cette mémoire a abordée la conception d'une université intelligente en mettant l'accent sur le raccordement des objets connectés. Tout au long de ce travail, nous avons exploré les notions de base sur les réseaux informatiques, les concepts clés de l'Internet des objets (IoT) ainsi que les technologies et les protocoles associés.

Nous avons réussi à concevoir et à simuler un réseau IoT pour une université, en utilisant des équipements réseau appropriés tels que les concentrateurs, les commutateurs, les routeurs et les points d'accès sans fil. Les différentes parties de l'université, telles que l'administration, le parking, la bibliothèque, le laboratoire, l'amphithéâtre et le stade, ont été prises en compte pour garantir une connectivité adéquate des objets connectés.

La simulation réalisée à l'aide de l'outil Cisco Packet Tracer a permis de valider la faisabilité du réseau IoT de l'université. Cependant, il est important de souligner que cette simulation reste une représentation simplifiée de la réalité, et que des étapes supplémentaires seront nécessaires pour mettre en œuvre un déploiement réel de l'IoT dans une université.

En résumer, ce projet de conception d'une université intelligente a permis d'explorer les possibilités offertes par l'IoT pour améliorer les environnements éducatifs. Il ouvre la voie à des recherches et à des mises en œuvre plus approfondies dans le domaine de l'IoT pour les institutions d'enseignement supérieur.

L'évolution rapide des technologies IoT offre des opportunités passionnantes pour transformer les campus universitaires en des environnements connectés, sécurisés et efficaces, propices à l'apprentissage et à l'innovation.

Cependant, ce travail ouvre la voie à de nombreuses perspectives et opportunités pour l'amélioration et l'expansion du réseau IoT de l'université intelligente. Voici quelques-unes des perspectives envisagées :

1. Mettre en place une connexion à Internet pour l'université intelligente : En mettant en place une connexion à Internet pour l'université intelligente, vous permettrez l'accès à distance, la collecte de données en temps réel, la gestion centralisée des objets connectés et l'intégration avec des services en ligne. Cela ouvrira de nouvelles possibilités pour l'innovation, la recherche et l'amélioration des services au sein de l'université.

2. Améliorer la sécurité de l'université : en utilisant des méthodes de protection des réseaux, telles que la configuration de pare-feu, de VPN (Virtual Private Network) ou d'autres mécanismes de sécurité pour renforcer la protection du réseau IoT de l'université contre les menaces potentielles.
3. Conception d'un VLAN pour les départements de l'université : Mettez en place des VLAN (Virtual Local Area Networks) pour séparer et sécuriser les différents départements de l'université. Cela permettra de mieux gérer le trafic réseau, de contrôler l'accès aux ressources spécifiques à chaque département et d'améliorer la confidentialité des données.
4. Conception des systèmes IoT automatisés plus avancés : En adoptant cette perspective, vous pourrez explorer les possibilités de conception de systèmes IoT plus avancés et réaliser des expérimentations intéressantes en utilisant des microcontrôleurs dans Cisco Packet Tracer. Cela permettra de simuler et de tester des scénarios réalistes pour l'université intelligente, ouvrant ainsi la voie à des solutions IoT plus sophistiquées et automatisées.

Ces perspectives offrent des opportunités passionnantes pour l'évolution et l'amélioration continue de l'université intelligente. L'application de ces idées permettra d'élargir les fonctionnalités du réseau IoT, d'augmenter la sécurité et l'efficacité, et d'optimiser les environnements d'apprentissage et d'innovation au sein de l'université.

BIBLIOGRAHPE

[1] Andrew S. Tanenbaum, David J. Wetherall. COMPUTER NETWORKS. *5th edition. Pearson. Janvier 2010.*

[2] Claude Servin, RESEAUX ET TELECOMS, *Dunod 2003*

[3] Yekini Nureni. DATA COMMUNICATION & NETWORKING. *November 2015. Yaba College of Technology.*

[4] Odom, W. (2003). CCNA Intro Exam Certification Guide. Cisco Press

[5] Yaibuates, M., & Chaisricharoen, R. ICMP BASED MALICIOUS ATTACK IDENTIFICATION METHOD FOR DHCP. *Présenté à Chiang Rai. 2014*

[6] Chao, H.-C., Wn, T. Y., Chang, S. W., & Wang, R.-C. THE NETWORK TOPOLOGY -based domain name service. *Présenté à Aizu-Wakamatsu, Japan. 1999*

[7] Pujolle, S. (2008). Les réseaux : concepts, administration et mise en œuvre. Eyrolles.

[8] Dromard, D., & Seret, D. ARCHITECTURE DES RESEAUX. Paris : Eyrolles. 2009

[9] Modèle TCP-IP Le modèle TCP-IP et les raisons de son succès – Wikiversité URL.

[10] Lohier, S., & Quideller, A. LE RESEAU INTERNET. *(3rd ed.). Dunod. 2010*

[11] Pacôme Massol, INITIATION AU ROUTAGE, *2ème partie.*

[12] Jean Robert HOUNTOMEY, le routage statique, *AFNOG 2006 -NAIROBI- KENYA*

[13] Kemmoe .R, COURS DE LICENCE PROFESSIONNELLE EN RESEAUX INFORMATIQUES *à l'IPES et à l'IUT de Bandjoun*.

[14] Doug LOWE, NETWORKING ALL-IN-ONE FOR DUMMIES.

[15] Behrouz A. Forouzan, DATA COMMUNICATIONS AND NETWORKING.

[16] Bruse, E. Internet of Things: Definition, applications and comparison of wifibased communication protocols for implementation of an irrigation system. 2015

[17] Firouzi, F., Chakrabarty, K., & Nassif, S. R. (Eds.). Intelligent Internet of Things: From Device to Fog and Cloud. CRC Press. 2019

[18] Madakam, S., Lake, V., Lake, V. et Lake, V. INTERNET DES OBJETS (IOT) : *une revue de la littérature. Journal d'informatique et des communications, 2015*

[19] Sethi, P. et Sarangi, SR (2017). INTERNET DES OBJETS : *architectures, protocoles et applications. Journal of Electrical and Computer Engineering, 2017*

[20] Tanwar, S., Tyagi, S., & Kumar, N. (Eds.). MULTIMEDIA BIG DATA COMPUTING FOR IOT APPLICATIONS: *Concepts, Paradigms and Solutions (Vol. 163). Springer. 2019*

[21] Urso, O., Chiacchio, F., Compagno, L., et D'Urso, D. UNE APPLICATION RFID POUR L'AUTOMATISATION DE LA CARTOGRAPHIE DES PROCESSUS. *Procedia Manufacturing, 2020*

[22] Porkodi, R. et Bhuvaneswari, V. LES APPLICATIONS DE L'INTERNET DES OBJETS (IOT) ET LES NORMES DE TECHNOLOGIE DE COMMUNICATION : *un aperçu. En 2014 Conférence internationale sur les applications informatiques intelligentes (pp. 324-329). IEEE.*

[23] Principles of Internet of Things (IoT) Ecosystème : Insight Paradigm | SpringerLink

[24] Stephen McQuerry. CCNA Self-Study: NETWORK MEDIA (THE PHYSICAL LAYER). *Cisco Press. Apr 9, 2004*

[25] Sayed M. and Ali. G. PERFORMANCE EVALUATION OF A NETWORK USING SIMULATION TOOLS OR PACKET TRACER. *IOSR Journal of Computer Engineering (IOSR-JCE), 19:1–5, 2017*

WEBOGRAPHIE

[26] https://www.it-connect.fr
[27] https://networkel.com/subnet-mask-explained/
[28] https://www.cloudflare.com/fr-fr
[29] https://www.gliffy.com/blog/network-topology-diagram
[30] http://ilyse.e-monsite.com
[31] Statista - The Statistics Portal for Market Data, Market Research and Market Studies
[32] https://apacheIoT.org
[33] https://www.matooma.com/fr
[34] https://cdn.freebiesupply.com/logos/
[35] NFC technology - EndlessID.
[36] http://en.dpc.com.cn/products/index.html.
[37] https://i0.wp.com
[38] https://www.konectcity.com
[39] https://content.instructables.com
[40] https://www.lesnumeriques.com
[41] Free CCNA Tutorials. Study CCNA for free ! (study-ccna.com)
[42] Digitalguide | Compétences informatiques pour tous - IONOS
[43] www.cisco.com
[44] https://www.neiu.edu
[45] https://www.netacad.com