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

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

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

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

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

Présenté par
Juba NAIT KACI
Aimed KHEMIS

Thème

Etude et mise en place d'un système de vidéosurveillance IP à l'ENIEM

Mémoire soutenu publiquement le 19/06/ 2017 devant le jury composé de :

M Prénom NOM
Grade, Lieu d'exercice, Président

M Mourad LAHDIR
Maitre de conférence A, UMMTO, Encadreur

M Prénom NOM
Grade, Lieu d'exercice, Co-Encadreur

M Prénom NOM
Grade, Lieu d'exercice, Examinateur

M Prénom NOM
Grade, Lieu d'exercice, Examinateur

Année universitaire 2016-2017

Remerciements

Nous remercions ALLAH de nous avoir donné le courage, la volonté et la patience pour la réalisation de ce modeste travail.

Sincèrement, c'est un grand honneur pour nous d'avoir eu la chance de travailler avec Mr LAHDIR Mourad, notre promoteur. Aussi, nous tenons à lui exprimer notre profonde gratitude et nos remerciements les plus chaleureux, pour son aide la plus précieuse, son apport constructif, ses encouragements, ses conseils, sa grande disponibilité et surtout sa modestie qui est aussi grande que son mérite.

Nous tenons à remercier l'ensemble des membres du jury de nous avoir fait l'honneur d'assister à notre soutenance, d'examiner et d'évaluer notre travail.

Nous tenons à remercier également l'entreprise ENIEM qui nous a ouvert les portes de son usine, et plus particulièrement Mr TALEB Farhath , notre encadreur au sein de l'ENIEM , qui nous a faciliter l'accès et surtout d'avoir mis a notre disposition tout le nécessaire pour réaliser notre étude , sans oublier l'ensemble de l'unité .

Enfin, nous remercions toute personne qui a participé de prés ou de loin dans la réalisation de ce travail.

Aimed et Juba

Dédicace

Je dédie ce travail à ma grand-mère

A mon oncle Hand et toute sa famille

A mon père Lounis et à ma mère Malika

Mes grands parents

Mes frères Said, Tarik et Toufik

Mes sœurs Ouardia, Lynda et Naima

Mes oncles Madjid et Sadek

Mes neveux Aimed, Khaled et Hakim

Mes cousins Karim et Anis

Mes tantes

A toute la famille KHEMIS et TABLAT

Aimed

Dédicace

Je dédie ce travail à ma famille

Mes parents qui ont été toujours présents pour me guider et m'encourager, que Dieu les bénissent.

Mon frère Elyas et à ma sœur Cylia pour leurs soutiens sans failles tout au long de ma vie.

A Ouissam qui m'a tant motivé, et à mes amis qui m'ont apporté leurs supports moraux et intellectuels.

Juba

Glossaire

ACL = Access Control List

AVC = Advanced Vidéo Coding

CCD = Charge Coupled Device

CMOS = complementary metal-oxide-semiconductor

CPU = Central Processing Unit

DHCP = Dynamic Host Configuration Protocol

DRAM = Dynamic Random Acces Memory

DTP = Data Transfer Process

FTP = File Transfer Protocol

HTML = HyperText Markup Language

HTTP = HyperText Trasport Protocole

IEEE = Institute of Electrical and Electronics Engineers

IETF = Internet Engineering Task Force

IP = Internet Protocol

JPEG = Joint Photographic Experts Group

LAN = Local Area Network

MAC = Media Access Control

MAN = Métropolitain Area Network

M-JPEG = Motion Joint Photographic Experts Group

MPEG = Moving Picture Experts Group

NTP = Network Time Protocol

PABX = Private Automatic Branch Exchange

PAL = Phase Alternating Line

PC = Personal Computer

PI = Protocol Interpreter

PoE = Power over Ethernet

QoS = Quality of Service

RJ45 = Registered Jack 45

RTCP = Real time Transport Protocol

RTP = Real time Transport Protocol

SD = Secure Digital

SDHC = Secure Digital eXtended Capacity

SSL = Secure Sockets Layer

SSH = Secure Shell

TCP = Transmission Control Protocol

TDM = time-division multiplexing

To = Téra Octet

UDP = User Datagram Protocol

URL = Uniform Resource Locator

UPT = Unité de Prestation Technique

VLAN = Virtual Local Area Network

WAN = Wide Area Network

WDM = Wavelength Division Multiplexing

WLAN = Wireless Local Area Network

WIFI = Wireless Fidelity

WWW = World Wide Web

Liste des figures :

Liste des tableaux :

SOMMAIRE

INTRODUCTION

La vidéosurveillance IP consiste à placer des caméras de surveillance dans un lieu public ou privé et de recevoir le flux vidéo sur un PC localement ou à distance, c'est une technologie émergeante et encore peu connue dans notre pays. Pourtant, Elle représente l'une des plus importantes évolutions dans le domaine de la sécurité, et elle offre de nombreux avantages que la vidéosurveillance traditionnelle et ouvre de nouvelles possibilités.

Le développement récent des réseaux IP dans les entreprises et dans les différents organismes professionnels les a persuadés de migrer vers ce genre de technologies, dans l'optique de minimiser les coûts d'installation et d'entretien. En effet, utiliser un seul réseau pour les données, la voix et la vidéo est moins couteux.

L ' ENIEM (Entreprise National des Industries de l'Electroménager) faisant parti des plus grandes entreprises du pays et qui détient une part importante du marché de l'électroménager à travers le monde, attire les convoitises de certaines personnes malveillantes qui œuvrent dans le but de vol de matériaux, de sabotage ou d'espionnage industriel. L'ENIEM doit faire face aussi aux problèmes des accidents. En employant des milliers de personnes dans ses unités, il est nécessaire de veiller à leur sécurité et d'intervenir rapidement et efficacement en cas de blessure de l'une d'entre elles. Des incendies pourraient aussi provoquer des pertes considérables s'ils ne sont pas détectés à temps.

Pour ces raisons, l'entreprise ENIEM a engagé un certain nombre d'opérations pour améliorer la sécurité de son infrastructure, parmi elles, la mise en place d'un système de vidéosurveillance. En effet, la présence de caméras dans l'infrastructure permettra de mieux détecter les personnes qui nuiraient à l'organisme et d'agir en conséquence. Elles sont aussi très efficaces en cas de problèmes majeurs tel qu'un incendie, défaillance de l'usine, blessure d'un employé…etc.

Ce travail a pour objectif d'étudier la vidéosurveillance IP, les protocoles et les technologies qui permettent son fonctionnement, étudier l'architecture du réseau informatique de l'ENIEM, ainsi que les éléments qui le composent, et la mise en place d'une solution de vidéosurveillance IP basée sur un serveur CamTrace. L'entreprise ENIEM, pourra utiliser notre solution afin de mettre en place un système de vidéosurveillance IP performant et peu couteux.

Ce mémoire se compose de quatre chapitres :

Le premier chapitre est une présentation du groupe industriel ENIEM, il décrit son emplacement géographique, son historique, ses objectifs futurs et le matériel du réseau informatique de l'entreprise.

Le deuxième chapitre a introduit la vidéosurveillance IP et les éléments qui la constituent, nous détaillerons son principe de fonctionnement, les protocoles qui y contribuent, et nous présenterons quelques technologies qu'elle utilise.

Le troisième chapitre s'est intéressé au réseau informatique de l'entreprise ENIEM et des éléments qui le constituent, nous avons fait la critique de ce dernier et nous avons définis les points à améliorer pour lui permettre de recevoir un système de vidéosurveillance IP. Nous avons finis par des propositions d'amélioration du réseau local.

Le dernier chapitre s'est intéressé à la mise en place du système de vidéosurveillance IP sur le réseau local basé sur une solution CamTrace. Les différentes étapes d'installations et de configuration, nous avons procédé à une simulation afin de définir le nombre et l'emplacement des caméras et à un calcul afin de nous assurer du bon fonctionnement du système.

Nous avons terminé notre travail par une conclusion tout en donnant les perspectives.

I. Préambule :

Notre étude s'effectue au sein d'une entité précise qu'il est important avant tout de présenter globalement. Il s'agira donc pour nous dans ce chapitre de présenter l'ENIEM et son historique, ainsi que son organisation interne et son environnement.

L'ENIEM qui a une place parmi les géants de l'électroménager à travers le monde et disposant de moyens financiers importants, a engagé un certain nombre d'opérations afin de renforcer la sécurité de son infrastructure, vu son importance ainsi que son activité intense, nous avons donc choisi d'effectuer notre stage au sein de celle ci et de participer à ce projet.

Dans ce chapitre, nous allons voir de plus près les détails de l'entreprise concernée. C'est à dire présenter le groupe industriel ENIEM.

II. Présentation de l'entreprise ENIEM :

1- Situation Géographique :

L'Entreprise ENIEM (Entreprise Nationale des Industries de L'Electroménager) se trouve au sein de la zone industrielle AISSAT- IDIR OUED - AISSI à 10 Km de TIZI - OUZOU, elle s'étale sur une surface totale de 55 Hectares, comme indiqué sur la figure 1.1 :

Sa direction générale se trouve au Chef lieu de TIZI - OUZOU à proximité de la gare ferroviaire.

Figure 1.1: Image satellite du complexe industriel ENIEM

2- Historique de l'entreprise ENIEM :

ENIEM résulte d'un contrat "produit en main" établi dans le cadre du premier plan quadriennal, et signé le 21 Août 1971 avec un groupe d'Entreprises allemandes représentées par le chef de file D.I.A.G (Société allemande) pour une valeur de 400 millions de dinars les travaux de Génie Civil ont été entamés en 1972 et la réception des bâtiments avec tous les équipements nécessaires a eu lieu en juin 1977.

En 1983, l'ENIEM issue la restructuration de SONELEC en 1983, elle est donc une entreprise au statut de la société nationale.
En 1989, l'ENIEM est passée à l'autonomie, les premières réformes ont été engagées et dans ce cadre l'ENIEM fut dotée de tous les organes de gestion légaux:

- Une assemblée Générale.
- Un Conseil d'Administration
- Un Capital Social.

Ainsi que le redéploiement des activités à l'intérieur de l'unité ces plans d'extension et de redéploiement de l'ENIEM se conjuguent directement avec ses autres programmes relatifs à la formation et à l'amélioration de la gestion, de la maintenance et de la qualité.

3- La gamme de production :

- Réfrigérateurs 160 l, 200 l, 240 l – 1 porte (2 étoiles)
- Réfrigérateurs 300 D, 290C - 2 porte (3 étoiles)
- Congélateur vertical 220 F - 1 porte, (4 étoiles)
- Réfrigérateur vertical 350 S - 1 porte, 2 étoiles.
- Congélateurs Bahut 350 l, 480l (4 étoiles)
- Réfrigérateurs 520l - 2 portes, (3 étoiles)
- Cuisinières tout Gaz 6400, 6000, 6100 (4 feux)
- Cuisinières tout gaz 8200 (5 feux)
- Climatiseurs Type fenêtre - 9000, 12000, et 15000 BTU/h
- Climatiseurs Split système S320 - 11250 BTU/h
- Climatiseurs Split système S430 - 14950 BTU/h
- Climatiseurs Split système S530 - 18000 BTU/h

4- Activités de l'entreprise :

L'activité de l'ENIEM est concentrée sur la fabrication de réfrigérateurs, cuisinières, et climatiseurs. Cette activité sera assurée par 3 unités de production :

a) Unité Froid

Elle est composée de 3 lignes de production.

1. Une Ligne de réfrigérateurs petits modèles :

Les capacités installées sont de 110.000 réfrigérateurs / an, dont les modèles fabriqués sous licence BOSCH –Allemagne - 1977. Sont :

- 160 l - 1 porte 2 étoiles
- 200 l - 1 porte 2 étoiles
- 240 l - 1 porte 2 étoiles

2. Une Ligne de réfrigérateurs grands modèles :

Les capacités installées sont de 390.000 Réfrigérateurs / an dont les modèles fabriqués sous licence TOSHIBA JAPON - 1987. sont :

- Réfrigérateurs 300 D - 2 portes, 3 étoiles
- Réfrigérateurs congélateurs 290C - 2 portes, 3 étoiles
- Congélateur vertical 220 F - 1 porte, 4 étoiles
- Réfrigérateur vertical 350 S - 1 porte, 2 étoiles.

3. Une Ligne de congélateurs bahut et réfrigérateurs de 520 L

Les capacités installées sont de 60.000 appareils / an. Dont les modèles sous licence Lematic /Liban 1993 sont:

- Congélateurs Bahut 350 l, 4 étoiles
- Congélateurs bahut 480 l, 4 étoiles
- Réfrigérateurs 520l - 2 portes, 3 étoiles.

b) Unité Cuisson :

Les capacités installées sont de 150.000 cuisinières / an fabriquées sous Licence TECHNO GAZ - Italie - 1991. Dont les modèles sont :

- Cuisinières tout Gaz 6400 4 feux

- Cuisinières tout gaz 6000 4 feux
- Cuisinières tout gaz 6100 4 feux
- Cuisinières tout gaz 8200 5 feux

c) Unité Climatisation

Les capacités existantes sont de 60.000 climatiseurs sous Licence Airwell - France 1977 dont les modèles sont :

- Type fenêtre - 9000 BTU/h
- Type fenêtre - 12000 BTU/h
- Type fenêtre - 15000 BTU/h
- SplIt système S320 - 11250 BTU/H
- SplIt système S430 - 14950 BTU/H
- SplIt système S530 - 18000 BTU/H

En plus de ces trois unités, nous trouvons aussi autres unités :

d) Unité Commerciale

Ses activités sont :

- la distribution et l'exportation des produits ENIEM,
- Le service après-vente (à travers ses moyens propres et un réseau d'agents agréés).

e) Unité Prestations Techniques

Cette unité assure les fonctions de soutien aux unités de production dans les domaines de :

- Réparation des outils et moules,
- Fabrication de pièces de rechange mécanique,
- Conception et réalisation d'outillages,
- Gestion des énergies et fluides.

- Gardiennage et sécurité,
- Travaux d'imprimerie,
- Travaux de menuiserie.
- Travaux de nettoyage.

5- Objectifs de l'entreprise

Parmi les principaux objectifs que le complexe s'est assigné, nous pouvons citer:

- L'amélioration de la qualité des produits.
- La maîtrise des coûts de production.
- L'augmentation des capacités d'études et de développement.
- L'amélioration de la maintenance de l'outil de production des installations.
- La valorisation des ressources humaines.
- L'augmentation des taux d'intégration (Interne et Externe).
- L'augmentation du volume de production.
- Demande (marché et externe).

6- Missions de l'Entreprise:

La mission de l'ENIEM est d'assurer la production, le montage, la commercialisation, le développement et la recherche dans les différentes branches de l'électroménager notamment :

- Les appareils de réfrigération et de congélation par l'unité froide
- Les appareils de cuisson par unité cuisson
- Les appareils de climatisation par l'unité climatisation
- Les produits sanitaires par unité d'AIN DEFLA

7- Le règlement intérieur qui englobe :

L'organisation générale de travail (horaires de travail, et de sortie, la tenue de travail, le contrôle de présence, etc.……) l'hygiène, sécurité et médecine du travail.

Ce présent règlement intérieur a pour but :

- De contribuer à l'amélioration de la production et de la productivité.
- De fixer les principes et les règles relatifs à l'organisation technique de travail, ainsi que celles relatives à l'hygiène, la sécurité, la discipline et la médecine du travail.

8- Système informatique de l'ENIEM :

Au début des années 80, ENIEM, a commencé à s'organiser dans le but d'informatiser certains services, jugés prioritaires telles les ressources humaines et la comptabilité ; en optant d'abord à un recrutement du personnel qui aura la charge d'asseoir un projet informatique.

Vers 1985, les prémices d'une solution intégrant la comptabilité et la paie a vu le jour et sera finalisé vers 1986 par l'achat d'un mini ordinateur Hp3000 modèle 52 dont la configuration était de 1 MO de mémoire centrale et de 800 MO de disque. Quatorze terminaux et quatre imprimantes desservant les structures de gestion comptabilité et paie forment le réseau informatique de l'époque.

Vers 1990, après une organisation tournée vers la gestion de production assistée par ordinateur (GPAO) et un système « achats », l'ENIEM s'est équipée d'un nouveau mini ordinateur Hp3000/70 modèle 70 dont la configuration est de 8 MO de mémoire RAM et de 4 disques de 571 MO, muni d'une solution réseau LAN intégrant une interface réseau vers le Hp3000/52 déjà en place. Si ajoutent 96 terminaux et 14 imprimantes installés soit aux ateliers aux fins de gestions de production et de stocks, soit dans les structures de gestion des achats et autres transits.

Vers 1997, l'obsolescence de la solution informatique commence à se ressentir sérieusement. En effet, le constructeur Hewlett - Packard ayant délaissé les systèmes sous OS MPE (Multi – Programming - Equipment), générant ainsi une maintenance trop cher payée, et un suivi sous label Remarkete (vente de cartes électroniques sous maintenance). De plus, le problème du passage à l'an 2000 et les très fortes indisponibilités de la pièce de rechange auront fortement agi sur la décision d'acquérir de nouvelles machines capables à la fois de la prise en charge de l'existant et de permettre une ouverture vers les systèmes dits ouverts.

- **Solution préconisée et mise en œuvre actuelle**

Plusieurs axes sont mis au point. Le schéma directeur final sera matérialisé par une solution de continuité, à savoir :

- Une machine Hp3000 série A500 pouvant immédiatement prendre en charge l'existant tout en ayant la possibilité de devenir Serveur Hp9000, moyennant un kit agissant sur le hardware et le software ;
- Un serveur Hp9000 servant de plate forme de base pour une solution future.

Les deux systèmes, une fois l'intégration du passif terminée, formeront un couple de serveurs, qui, grâce au memoring (sauvegardes à chaud durant les périodes de travail), permettra à ENIEM de bénéficier de la sécurité de ses données.

Le nombre d'utilisateurs, actuellement porté à 90 ports de terminaux départagés entre les ateliers et l'administration, se verra augmenté suffisamment pour arriver à connecter le complexe dans un cadre de réseau Internet en utilisant toutes les solutions et moyens adéquats.

Grâce à la solution préconisée, ENIEM gagnera à acquérir toutes les solutions existantes sur le marché et pouvant améliorer ses modes de gestion.

- **Configurations :**

Matériel et Description du Hp3000 Série A500	**Quantité**
HP 3000 A500, 1 processeur, 200MHz, 512MB, MPE, IMAGE	1
CPU HP e3000 A500 200MHz	1
Module mémoire 512MB Haute densité SyncDRAM	3
Disque 36GB 10K HotPlug Ultra160	2
MPE/ix Release 7.5	
HP3000 A-Class to rp24X0 Srvr Conversion	1
A500 200 MHz to HP svr rp2470 650MHZ	
Module pour baie HP SureStore DAT40	1
Module pour baie HP SureStore DVD - ROM	1
Module pour baie HP SureStore DLT 80	1
DTC 16MX Serveur de communication	3
Remplacement de 8 ports Directs par Modem	6
RS-232 avec connecteurs DB25,	
DTC 16MX Serveur de communication	3
Solution HP serveur rp2470	**1**
CPU HP serveur rp24X0 PA8700 750MHz	2
Module mémoire 1024MB HD SyncDRAM	2
Disque 36GB 10K HotPlug Ultra160	2
Adaptateur réseau PCI 10/100Base-T	2
PCI Ultra160 SCSI Adapter	1
HP-UX version 11i	1
Terminal console for HP3000/9000 systems	1
CD-ROM (support seulement)	1

Intégration en usine	1
Licence d'utilisation HP-UX OE pour 1 CPU	2
Licence MirrorDisk/UX pour serveurs HP 9000	1
Licence Système pour HP 9000 tiers 1	2
Baie de bande HP SureStore 5300 (usine)	1
Module pour baie HP SureStore DVD-ROM	1
Intégration en usine	1
Module pour baie HP SureStore DLT 80	1
Imprimante Printronix 1500 LPM et interface réseau	1
Imprimante Printronix 500 LPM et interface réseau	3
Imprimante LQ-208 N&B - 406 x 559 mm - 360 pppx360ppp	5
EVO D310m, PIV, 2 Ghz, 40GB DD, C.D., WXP	50
Oracle 9i Database Edition Entreprise 1 NU	50
Support produit et mises à jour, 1 année, 1 NU	50
Support sur C.D.	1
Note : Pour Oracle 9i, le minimum de NU est de	
25 utilisateurs par processeur	
Suite Oracle Developpeur Internet, 1 Utilisateur	6
Support produit et mises à jour, 1 année, 1 NU	6
Licence Openview NNM 250 utilisateurs pour HP-UX	1

Tableau 1.1 : Les équipements informatiques de l'ENIEM

III. Discussion :

Tout au long de ce chapitre, nous avons montré l'étendu géographique ainsi que les ressources matérielles et logicielles de l'entreprise ENIEM. Nous avons décidé d'effectuer notre étude dans cette entreprise car elle est réputée par son excellent niveau, et sa qualité de formation et d'encadrement.

I. Préambule :

La vidéosurveillance occupe une place prépondérante dans le monde industriel, elle permet de garantir une sécurité maximale que ce soit pour la protection de ces salariés, mais aussi la lutte contre le vol et le sabotage.

Ces dernières années, la prolifération des réseaux IP a facilité et réduit considérablement les coûts d'installation et d'entretien de ce système. En effet, il est désormais possible d'installer les caméras directement sur un réseau déjà existant sans avoir besoin d'ajouter des équipements supplémentaires. De ce fait, elle ne se limite plus aux grands groupes industriels, de plus en plus de particuliers investissent dans cette technologie que ce soit pour sécuriser un foyer, ou bien dans les boutiques pour lutter contre les vols.

L'objectif de ce chapitre est l'étude des systèmes de vidéosurveillance IP ainsi que des éléments nécessaires à sa conception, tel que, les réseaux informatiques et la fibre optique qui serviront de support de transmission. Nous allons détailler aussi son principe de fonctionnement, en commençant par l'acquisition de l'image jusqu'à son visionnage.

II. La vidéosurveillance :

1) Définition :

La vidéosurveillance est une technologie permettant de surveiller un lieu quelconque grâce à un flux constant d'images vidéos captées à l'aide de caméras (analogique ou numérique) et transmise par un support physique à un équipement de lecture (moniteur ou PC).

La vidéosurveillance permet notamment :

- L'augmentation de l'efficacité des sites de production.
- Le contrôle des stocks, et l'amélioration de la sécurité dans le cadre des chaînes de fabrication.
- La prévention d'éventuels menaces physiques et la dissuasion des personnes malveillantes.
- Sécurisation d'un lieu public ou privé.

2) L'évolution de la vidéosurveillance [2] :

La vidéosurveillance est une technologie vieille de plusieurs dizaines d'années. A ces débuts, elle était entièrement analogique mais comme toutes autres technologies, elle a eu sa part d'évolution et de développement qui a permis aujourd'hui de la rendre accessible au grand publique. L'évolution a connue 3 principales périodes :

- **<u>Système de Vidéosurveillance analogique avec magnétoscope :</u>**

Dans un système de vidéosurveillance analogique on utilise des caméras vidéos analogiques avec des sorties coaxiales. Des magnétoscopes sont reliés à cette sortie pour enregistrer la vidéo et un moniteur pour visionner les images tel que ce schéma nous le décrit :

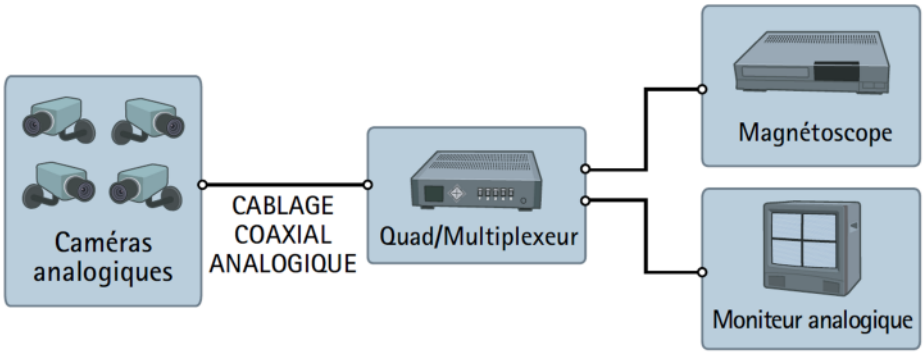

Figure 2.1 : Système de vidéosurveillance analogique

Autrefois les images n'étaient pas numérisées, elles étaient sous forme de signaux électriques et leurs transmissions se faisaient avec des câbles coaxiaux comme celles de la télévision.

La qualité de la vidéo était très basse, et la capacité de stockage était limitée du fait que la bande magnétique avait une capacité réduite en plus d'être couteuse, et en cas de détérioration de cette bande, cela entrainera des pertes de données.

- **Système de Vidéosurveillance analogique avec enregistreur numérique** :

Un système de vidéosurveillance analogique avec enregistreur numérique est un système qui utilise des caméras analogiques et un enregistreur numérique tel que cette image nous le montre :

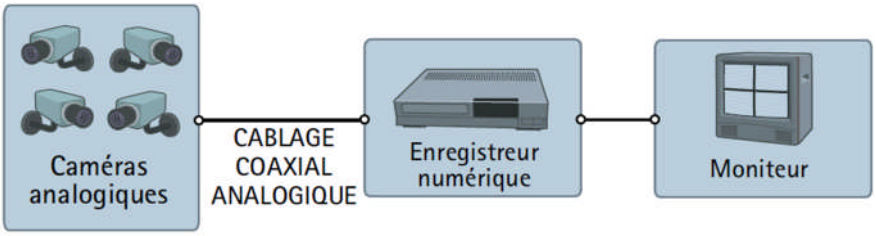

Figure 2.2 : Système de vidéosurveillance analogique avec enregistreur numérique

Ce système fonctionne de la même façon que le précédent, à la différence près qu'une fois les signaux électriques arrivés à l'enregistreur, ils sont convertis en une séquence binaire (signal numérique). Cette nouvelle technologie a notamment permis d'enregistrer les images sur des supports numériques (CD-ROM, disque dur) et donc d'augmenter considérablement la capacité de stockage.

Certains enregistreurs numériques possèdent un port RG45, ce qui lui permet de transmettre les images directement sur un réseau informatique et de les visualiser sur un ordinateur.

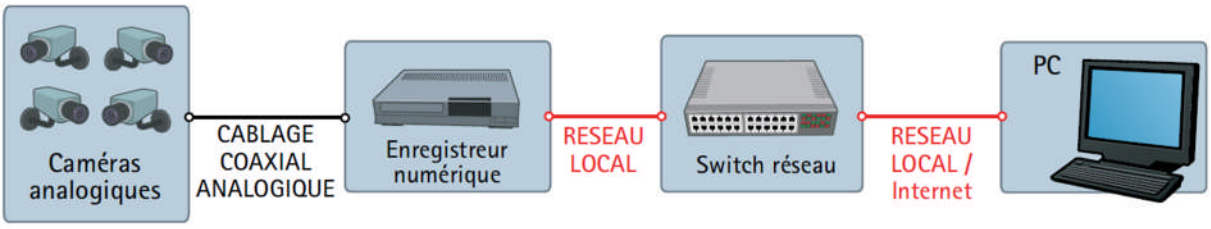

Figure 2.3 : Système de vidéosurveillance analogique avec enregistreur numérique réseau

- **Système de Vidéosurveillance IP** :

C'est le système de vidéosurveillance de nos jours. Entièrement numérique, à la différence des systèmes de vidéosurveillance analogique, la vidéosurveillance IP utilise des caméras réseaux qui ont la capacité de convertir les signaux électriques en une séquence binaire et de la transmettre sur le réseau informatique grâce au protocole TCP/IP.

Les caméras réseaux (cameras IP) peuvent êtres définies comme étant l'association d'une caméra avec un ordinateur, possédant une adresse IP, elle est considérée comme un équipement informatique à part entière, elle capte et elle transmet les images en direct sur le réseau IP, les images vidéos seront acheminées au poste de gestion vidéos où elles seront enregistrées.

La vidéosurveillance IP permet aux utilisateurs d'obtenir à tout instant et en tout lieu des informations sur une opération en cours, et de la suivre en temps réel.

Un système de vidéosurveillance IP se compose de plusieurs éléments qui assurent son fonctionnement depuis l'acquisition des images jusqu'à son visionnage. Ces éléments sont :

III. La vidéosurveillance IP :

La vidéosurveillance IP fonctionne notamment grâce aux caméras IP, les images sont captées par ces dernières puis retransmise par un réseau IP jusqu'au moniteur, nous allons détailler chacun des éléments qui permettent sont fonctionnement :

1) Les caméras réseaux (caméras IP) :

C'est l'élément le plus important dans les systèmes de vidéosurveillance IP, son rôle est de capter les photons et de les convertir en un signal électrique, ces derniers seront à leur tour converti en une suite binaire (signal numérique) et seront transmis à travers le réseau IP.

Ces caméras numériques sont considérées comme des équipements informatiques dans le réseau, c'est-à-dire qu'elles possèdent leur propre adresse IP et peuvent être installées sur n'importe quel lieu possédant un réseau IP.

a) Présentation de la caméra réseau :

L'image ci-dessous montre les composants d'une caméra réseau :

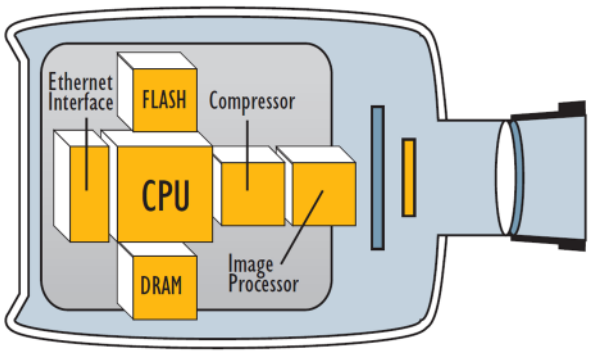

Figure 1.4 : Composants d'une caméra réseau [9]

Chacun des ces éléments à un rôle important qu'on résumera comme suit :

Image processor :

Autrement dit un processeur d'image, c'est un appareil qui permet de créer l'image numérique grâce à un capteur qui peut être soit un capteur CCD ou un capteur CMOS, la variation de la lumière à l'entrée de ces capteurs est convertie en une variation du signal électrique à leur sortie. Ce principe permet de générer des pixels qui représentent l'image captée, ainsi elle peut être retransmise.

Compressor :

Comme son nom l'indique, le compresseur permet de compresser les images vidéos afin de réduire leur taille et de les transmettre plus rapidement.

CPU :

En anglais Central Processing Unit .C'est un microprocesseur, son rôle est prédominant dans le fonctionnement de la caméra, en effet il s'occupe de la gestion de tous les autres composants de la caméra, et de garantir une bonne transmission de l'image. Il permet aussi la configuration de plusieurs paramètres de la caméra réseau tel que l'adresse IP et le protocole utilisé.

DRAM :

La mémoire dynamique à accès aléatoire (DRAM) Dynamic Random Acess Memory, c'est un type de mémoire vive dynamique à accès aléatoire.

Flash :

C'est une mémoire flash intégrée. Associé avec la DRAM, elles sont spécialisées dans les applications réseaux.

Ethernet Interface :

C'est un composant qui permet à un équipement tel qu'une caméra de pouvoir se connecter à un réseau local (LAN), en utilisant Ethernet comme mécanisme de transmission.

b) Les types de caméras :

Il existe plusieurs types de caméras dont :

Les cameras Infrarouges : [17]

Une caméra infrarouge (ou caméra thermique) est une caméra qui enregistre les différents rayonnements infrarouges (ondes de chaleurs) émis par le corps et qui varient en fonction de leur température.

Un corps vivant émet des radiations sous formes de lumière infrarouge, cette lumière est captée par le détecteur infrarouge, elle sera numérisée et transmise vers l'afficheur.

C'est un procédé qui est de plus en plus utilisé dans l'industrie car ces caméras permettent d'effectuer des contrôles au niveau d'une ligne de production et ceci sans aucun contact avec le produit contrôlé.

Les caméras motorisées :

Une caméra motorisée est une caméra équipée d'un moteur électrique qui lui permet de faire des mouvements verticaux, horizontaux et des rotations, cette particularité lui permet d'avoir un choix de déplacement du champ de vision, et de surveiller un espace plus important que les caméras ordinaires.

Caméras Dôme: [13]

Il existe plusieurs avantages pour les caméras dôme. Les caméras dôme rotatives montées au plafond offrent une vue à 360 degrés d'une zone. Pour empêcher le vol dans un magasin ou empêcher le vandalisme à l'extérieur, une caméra dôme plus sombre cache l'objectif afin que la personne ne sache pas si la caméra s'adresse à eux. Les caméras Dôme ne possèdent pas non plus de fils exposés offrant un certain degré de sabotage.
Il existe de nombreux types de caméras dôme: faible éclairage, infrarouge, intérieure / extérieure.

Caméra extérieure: [13]

A moins que la caméra soit spécialement conçue pour une utilisation à l'extérieur il ne faut jamais utiliser une caméra à l'extérieur. Certaines caméras sont conçues pour résister et fonctionner sous la pluie, une forte humidité et des températures extrêmes et basses. D'autres caméras peuvent gérer l'humidité et les températures extrêmes, mais doivent être placées dans un boîtier métallique pour se protéger des éléments. Placer une caméra d'intérieure à l'extérieur provoquera une panne.

2) Les lignes de transmission des images vidéo :

Dans la vidéosurveillance IP, les images vidéo sont transmises dans un réseau informatique, elles passent à travers un support physique qui peut être soit de la fibre optique, un câble à paires torsadées, ou par des ondes électromagnétiques. Nous allons vous présenter quelques généralités sur les différents supports que nous utiliserons dans notre étude :

- **Les câbles à paires torsadées :**

Un câble à paires torsadées est composé de 4 paires de fils enroulés en hélice, cette caractéristique permet d'atténuer les interférences et d'augmenter la distance de transmission des informations.

Le réseau local de l'ENIEM utilise des câbles à paires torsadées de catégorie 5, avec un débit de 100Mbps sur une distance de 100 mètres.

- **La fibre optique :**

La fibre optique est un fil en verre très fin qui a la propriété de conduction de lumière, c'est un support de transmission utilisé dans le domaine de la télécommunication, très performant grâce à sa vitesse de transmission et sa grande largeur de bande. Elle permet l'acheminement des informations sur de longues distances (entre 500m à 100km).

Dans notre étude on va utiliser la fibre optique multimodale à gradient d'indice, c'est-à-dire que l'indice de réfraction du cœur diminue en s'éloignant de son axe. La lumière est donc constamment déviée vers l'axe jusqu'à atteindre l'extrémité de la fibre elle permet une vitesse de transmission de 1Gbps sur une distance de 500m.

- **LE WIFI : [3]**

La norme WIFI (Wireless Fidelity) est le nom commercial donné a la norme 802.11, c'est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN), elle offre des débits allant jusqu'à 54 Mbps sur une distance de plusieurs centaines de mètres tout dépend du milieu et de la norme utilisée.

Le WIFI présente plusieurs normes IEEE802.11, selon la bande passante, la distance d'émission ainsi que le débit qu'elles offrent, nous avons choisis d'utiliser la norme 802.11g.

La norme 802.11 g :

Elle étend la norme 802.11b, en augmentant le débit jusqu'à 54Mbps théorique (30 Mbps réels). Elle fonctionne aussi à 2,4GHz, ce qui rend les deux normes parfaitement compatibles.

3) Equipements de visionnage :

Afin de visionner, traiter et enregistrer les images captées par les caméras IP, le système possède un ensemble d'équipements matériels et logiciels :

a) Logiciel de lecture vidéo :

Dans le cas de la vidéosurveillance IP, un pc muni d'un logiciel de lecture sert d'équipement de lecture des images vidéo. En introduisant l'adresse IP d'une caméra réseau dans un navigateur web, on pourra alors configurer la caméra et ensuite utiliser un logiciel pour visionner les images en temps réel. Dans notre étude ,nous utiliserons le logiciel Camtrace ,en plus du visionnage, il offre aussi la possibilité aux utilisateurs :

- Le contrôle des alarmes.
- L'enregistrement des images vidéo avec plusieurs modes (cas d'activation d'une alarme)
- Le contrôle des caméras motorisées.

b) Serveur Vidéo :

C'est un système de conversion, il transforme les signaux vidéos PAL et les signaux vidéos numériques d'une caméra en un flux numérique sous un format MPEG 2 ou MPEG 4 via le port RG45. Ce serveur vidéo est très utilisé dans le domaine de la vidéosurveillance. Un serveur vidéo permet de faire :

- L'acquisition des vidéos à partir des caméras.
- Le stockage de vidéos enregistrées.

- La transmission des vidéos vers d'autres serveurs via le réseau IP.

c) Serveur FTP (File Transfert Protocol) :

Comme son nom l'indique, c'est un serveur qui sert à transférer les fichiers soit par le réseau Internet soit par le biais d'un réseau informatique local.

4) Les technologies utilisées dans la vidéosurveillance IP :

a) L'adressage :

L'adressage permet d'identifier de façon unique un équipement dans un réseau, chaque équipement se voit attribué une adresse IP unique, qui contient des informations sur le réseau ainsi que sur la machine.

On utilise aussi les adresses proxy comme substituant aux adresses IP (semblable à une adresse mail) pour identifier les utilisateurs dans le réseau.

b) VLAN :

Les réseaux virtuel (VLAN) permettent de réaliser des réseaux d'accès sur une organisation de l'entreprise on s'affranchissant certaines limites de certaines contraintes techniques comme la localisation géographique.

On peut ainsi définir les domaines de diffusion, du broadcast indépendamment de l'endroit où se situent les systèmes.

Les VLAN introduisent la notion de segmentation virtuelle qui permet de constituer des sous réseaux logiques en fonction des critères prédéfinis comme les adresses MAC et les numéros de ports de façon statique ou dynamique .Les échanges à l'intérieur d'un domaine sont automatiquement sécurisés et les communications inter domaines peuvent être contrôlées.

Il existe plusieurs niveaux de VLANS :

- **VLAN de niveau 1 :** appelé VLAN par port qui regroupe les stations connectées à un même port des commutateurs.

- **VLAN de niveau 2 :** appelé VLAN par adresse MAC qui associe des stations par leurs adresses MAC selon des tables d'adresses introduite par l'administrateur.

- **VLAN de niveau 3 :** appelé VLAN adresse réseau qui associe des sous réseaux IP par un masque ou par adresse, les utilisateurs sont affectés à un ou plusieurs VLAN.

c) PoE (power over Ethernet) : [18]

Power over Ethernet est une technologie qui permet d'alimenter via le réseau local des équipements réseau tel que des téléphones IP ou des caméras réseaux. Ces derniers ne seront alors branchés qu'à un seul câble (câble à paires torsadées) qui aura la double fonction d'alimenter l'équipement et de transmettre les informations.

PoE est conçu de manière à ne pas perturber les signaux, ni à réduire la distance de transmission, il assure une alimentation pouvant aller jusqu'à 15W. Associé à un système d'alimentation sans coupure, les équipements pourront fonctionner constamment sans interruption.

L'énergie est directement transmise à travers les ports de transmission, la plupart des commutateurs et des équipements récents offre cette technologie. Dans le cas contraire, il suffit de brancher un injecteur au commutateur et un diviseur actif à l'équipement pour bénéficier du service du PoE.

d) Compression vidéo [4] :

Les technologies de compression vidéo ont pour but de réduire et de supprimer les données vidéos redondantes, améliorant ainsi l'efficacité de la transmission sur le réseau et du stockage d'un fichier vidéo numérique sur des disques d'ordinateurs, il existe plusieurs normes, les plus répondues sont :

M-JPEG :

M-JPEG est la norme la plus utilisée parmi les systèmes de vidéosurveillance sur IP. Une caméra réseau, tout comme un appareil numérique permettant la capture d'images immobiles, saisie des images individuelles, et les compressent au format JPEG. Une caméra réseau peut ainsi capturer et compresser, par exemple, 30 images individuelles par seconde puis les envoyer sur réseau sous forme de flux continu pouvant être lu sur un poste de visualisation. À une fréquence de l'ordre de 16 images par seconde ou plus, l'utilisateur perçoit une vidéo en mouvement. C'est cette méthode que l'on appelle Motion JPEG ou M-JPEG. Chaque image individuelle étant totalement compressée en JPEG, une qualité identique est assurée pour toutes les images, en fonction du taux de compression sélectionné pour la caméra réseau ou le serveur vidéo.

MPEG :

La norme MPEG (fondée par le *Motion Picture Experts Group* à la fin des années 1980) est la plus connue des techniques de transmission directe audio et vidéo. Dans cette section, nous nous limiterons à la partie vidéo de la norme MPEG.
Le principe de base du MPEG consiste à comparer deux images compressées destinées à être transmises sur le réseau. La première des deux images servira de trame de référence. Sur les images suivantes, seules les zones qui diffèrent de la référence seront envoyées. L'encodeur réseau reconstruit alors toutes les images en fonction de l'image de référence et de la "plage de différence".
Bien que plus complexe que la technique Motion JPEG, la compression vidéo MPEG produit de plus petits volumes de données à transmettre via le réseau.

H.264 :
La norme H.264, également connue sous le nom de MPEG-4 Part 10/AVC (pour Advanced Vidéo-Coding), est la norme de codage vidéo MPEG la plus couramment choisie a l'heure actuelle. En effet, un encodeur H.264 peut réduire la taille d'un fichier vidéo numérique de plus de 80 % par rapport a la norme Motion JPEG et de 50 % par rapport a la norme MPEG-4 Part 2, sans affecter la qualité d'image. Le fichier vidéo occupe alors nettement moins d'espace de stockage et de bande passante réseau.

e) Protocoles :

Dans un réseau informatique les données sont acheminées grâce à des différents protocoles, chacun d'entre eux assure une fonction particulière qui garantie le fonctionnement du réseau et sa protection.

Les systèmes de vidéosurveillance et notamment la vidéosurveillance IP utilise certains de ces protocoles afin d'assurer les fonctions d'acheminement des images vidéos et leurs sécurisations. Nous allons présenter les protocoles nécessaires au fonctionnement de ce système :

i. Internet Protocole (IP) : [19]

C'est le protocole le plus utilisé dans le monde pour les communications distantes. L'information est segmentée, et chaque segment est envoyé dans des trames (datagramme), ces trames sont ensuite envoyées dans internet. Le paquet contient des informations sur le

destinataire et peut donc être routé jusqu'à arriver à destination, ce dernier aura qu'à réassembler les trames pour reconstituer l'information.

L'IP étant un protocole orienté non connexion, les paquets IP peuvent prendre des chemins différents selon la disponibilité des lignes de transmission.

ii. Protocoles http et https : [19]

HyperText transport protocole, autrement dit protocole d'échange d'HyperText est un protocole de type client/serveur développé spécialement pour le WWW. Et depuis sa création en 1990, il est le plus utilisé dans internet.

Il permet de lancer une requête http à un serveur web dans le but d'accéder à des documents écrit en HTML (HyperText). Les documents écrits avec ce langage peuvent être repérés grâce à une chaine de caractère appelée URL qui contient notamment des informations sur le nom du serveur, le protocole utilisé ainsi que chemin nécessaire à son acheminement.

Une fois avoir que la requête a été acceptée de la part du serveur web, le protocole http utilise le protocole TCP/IP comme couche de transport afin de transmettre les informations du serveur vers le destinataire et vice versa.

Afin de palier les défauts de l'http, une version sécurisée a été développée en l'associant à un protocole de chiffrement appelé protocole SSL. Ce dernier permet une authentification et une création d'un tunnel sécurisé où circulent les informations et permet de garantir la confidentialité et l'intégrité des données.

iii. Protocole TCP/IP : [20]

1) Définition :

Le protocole TCP/IP représente l'ensemble des protocoles utilisés pour le transfert de données dans les réseaux informatiques, son nom provient des deux principaux protocoles qui le constituent, le protocole de transmission (TCP) et le protocole internet (IP).

Il répond à de nombreux critères parmi eux :

- L'encapsulation des données dans des paquets.
- L'utilisation de l'adressage qui permet l'acheminement des paquets grâce au routage.
- Le contrôle des erreurs de transmission.

2) Modèle TCP/IP :

Le modèle TCP/IP est constitué de 4 couches comme ce schéma ci-dessous l'indique :

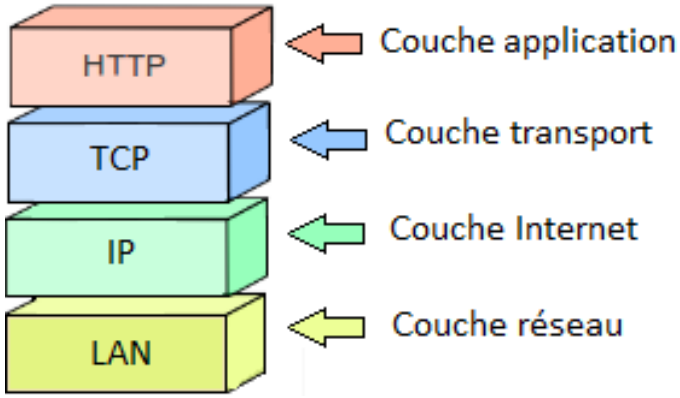

Figure 2.5 : Les couches TCP/IP.

3) Principe de fonctionnement :

Lors de la transmission d'un flux de données, il est dans un premier temps encapsulé en paquets, ensuite chacun d'entre eux passe à travers les couches de la machine émettrice afin qu'il soit enrichi en information en lui ajoutant des en-têtes qui indiqueront :

- L'adresse IP de la source.
- L'adresse IP du destinataire.
- La version du protocole IP (version 4 ou 6)
- La longueur de l'entête IP (généralement elle est de 20 octets)
- Le niveau de priorité du paquet.
- La longueur totale du paquet (elle est toujours inférieure à 64 ko)
- Le numéro du paquet.
- La possibilité de fragmenter les paquets et indiquer l'ordre des fragments si c'est le cas.
- Le type de protocole utilisé.
- La présence d'une erreur dans la constitution de l'erreur, cet en-tête permet aussi de détruire entièrement le paquet en cas de présence d'erreurs.

Une fois que le paquet est entièrement constitué, il est envoyé à travers le réseau et il est acheminé jusqu'à la machine réceptrice où le paquet passera par toutes les couches où les en-têtes seront lus et supprimés pour retrouver le message initial.

iv. Protocole FTP : [14]

En français « protocole de transfert de fichier », C'est un protocole de type client/serveur qui est conçu pour les réseaux utilisant la technologie TCP/IP et permet un transfert de données de manière efficace entre des machines distantes.

Le client envoie une requête qui sera traitée par le serveur FTP. Une fois la requête acceptée, deux canaux sont ouverts entre la machine et le serveur, un pour les données et un autre pour le contrôler. Afin de gérer ces canaux, le client ainsi que le serveur possèdent deux processus :

- **DTP** : c'est le processus qui est chargé de la création et de la gestion du canal de transmission de données.
- **PI** : c'est le processus qui est chargé de contrôler le DTP suivant les instructions venant du canal de contrôle.

v. Protocole SSH : [22]

Secure Shell, c'est un protocole de communication sécurisé, a chaque début de connexion ce protocole de communication impose au utilisateur une clé de chiffrement. Alors tous les segments TCP sont authentifiés et chiffrés. Ce principe nous permet de configurer à distance les Switch de façon sécurisée.

vi. Les Protocoles de transport (RTP et RTCP) : [21]

a) Description du RTP :

Le protocole RTP (Real time Transport Protocol) est un protocole créé et standardisé par l'IETF en 1996 dans le but d'améliorer les transport des paquets audio et vidéo en temps réel dans les réseaux IP. Pour ce faire, le protocole RTP fonctionne au dessus de la couche UDP mais ce concept ne permet pas une qualité de service optimal en raison de son fonctionnement qui est au niveau applicatif.

b) Fonctionnement du RTP :

Le but du protocole RTP est d'organiser les paquets afin de pouvoir les assembler correctement à la réception, cela se fait de la façon suivante :

- Identification de l'expéditeur des paquets.
- Numérotation des paquets afin de détecter les paquets perdus et de pallier les pertes.

- Identification du contenu des paquets afin d'assurer une communication sécurisée.
- Inclusion des trames dans les paquets afin de faciliter leur récupération et ainsi rendre le décodage plus rapide.

c) Description du RTCP :

Le Protocol RTCP est utilisé par le protocole RTP afin de transporter les informations nécessaires à la gestion d'une session.

Le récepteur envoie à l'émetteur par le billet de protocole RTCP des informations sur l'état de la qualité de la session en cour comme, par exemple, le nombre de paquets perdus, le délai de réception, et la variance de distribution. Ces différents paramètres permettront à l'émetteur de s'adapter afin de garantir une bonne qualité de service.

Le protocole RTCP assure les fonctions suivantes :

- L'identification des participants en intégrant directement l'adresse et toutes les informations dans les paquets RTCP.
- Synchronisation entre les médias, c'est-à-dire que les images, le son et les données sont envoyés séparément et la synchronisation permet de les récupérer avec le bon timing.
- L'indication des participants du comportement, par exemple, le paquet Bye de RTCP indique que le participant quitte la session.

d) Fonctionnement du protocole de transport :

Le protocole de transport fonctionne grâce à l'utilisation des deux protocoles RTP et RTCP simultanément, en effet, le protocole RTP se charge de transporter en temps réel uniquement les données, tandis que le protocole RTCP demande régulièrement aux utilisateurs des informations afin de superviser la session en cour.

5) Le fonctionnement de la vidéosurveillance IP: [18]

Le principe de la vidéosurveillance est l'acquisition des images et leurs numérisation, c'est-à-dire le passage d'un signal électrique au niveau des capteurs à un signal numérique, ensuite ce signal numérique sera compressé afin de réduire sa taille et de faciliter sa transmission à travers le réseau.

Le signal numérisé et compressé sera enfin découpé en trames selon le protocole utilisé, à chacune des trames seront ensuite rajoutés des en-têtes qui contiennent des informations nécessaires à l'acheminement et au réassemblage des trames pour ainsi former l'image initiale.

La figure suivante montre le chemin qu'empruntent les données vidéos et les équipements nécessaires à son acheminement et au bon fonctionnement du système :

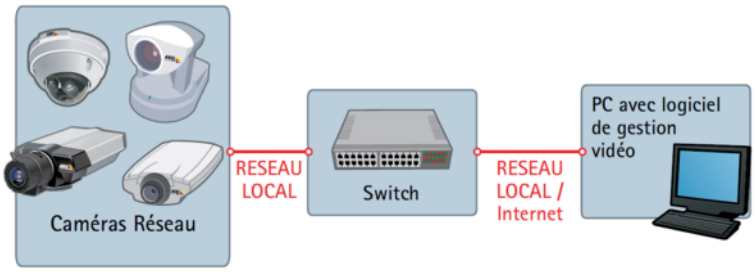

Figure 2.6 : Système de vidéosurveillance IP avec caméras réseaux.

Afin de mieux comprendre ce principe, nous allons suivre les différentes étapes qui consistent à transmettre les images :

1- Acquisition de l'image :

L'acquisition des images se fait au niveau de la caméra réseau, plus précisément dans le processeur d'image. Grâce à un capteur sensible aux variations lumineuses CCD ou CMOS, les photons pourront être convertis en un signal électrique qui sera envoyé vers le compresseur.

2- Numérisation et compression :

La numérisation et la compression se fait aussi au niveau des caméras réseaux, dans un composant qui porte le nom de compresseur.

La numérisation consiste à échantillonner le signal électrique en plusieurs petits échantillons et de quantifier chacun d'entre eux, c'est-à-dire donner une valeur numérique (binaire) pour chaque échantillon et ainsi pouvoir transmettre notre signal sous forme numérique.

Ce signal sera ensuite compressé grâce à des algorithmes dans le but de réduire sa taille au maximum et ainsi faciliter son acheminement et améliorer les performances du système.

3- Acheminement de l'image :

Afin de transporter le signal dans le réseau local, il doit être adapté au protocole TCP/IP qu'utilise le réseau, c'est-à-dire que le flux est encapsulé dans des paquets auxquels on rajoute des différents en-têtes qui contiennent :

- L'adresse IP de la caméra (l'expéditeur).
- L'adresse IP du destinataire.

- Les types de protocoles utilisés.
- Le support de transmission.
- Le numéro de port de la caméra.
- Le numéro de port du moniteur.
- La durée de vie du paquet.
- L'ordre de réassemblage des paquets.

Après sa formation, le paquet est injecté vers le réseau et se déplace à travers les câble à paires torsadées et la fibre optique, les différents Switch se chargeront d'orienter le paquet grâce au protocole IP jusqu'à arriver au destinataire (moniteur).

Le numéro de port du destinataire servira à indiquer par où les données transitent jusqu'au PC. Une fois les paquets arrivés à destination, ils seront réassemblés afin de reconstituer l'image initiale qui sera visionnée puis enregistrée selon les besoin du client.

6) Sécurisation des données : [18]

La vidéosurveillance est un moyen de sécurisation qui permet de surveiller nos locaux et nos maisons, il ouvre directement une fenêtre sur nos biens. Il est donc indispensable d'empêcher qu'il soit piraté et qu'il soit utilisé à notre insu.

Plusieurs solutions existent afin de prévenir le piratage et d'empêcher une intrusion dans le système :

1- Le cryptage vidéo :

Afin d'éviter que les images vidéos soient visionnées en cas d'interception sur la ligne de transmission, les caméras réseau permettent un cryptage des images de manière qu'elles ne peuvent être ni visualisées ou bien manipulées par d'autres utilisateurs , que celui qui possède la clé de décryptage.

2- Création d'un journal de vérification :

C'est un journal qui enregistre toutes les personnes ayant visionné ou modifié les images vidéos, il permet notamment de nous mettre au courant en cas de piratage et d'agir en conséquence.

3- L’estampillage :

Ce procédé permet aux caméras d’ajouter une information numérique indiquant l’endroit, l’heure ainsi que les données pouvant identifier l’utilisateur, associé au journal de vérification, il permettra notamment de connaitre l’identité du pirate.

IV. Discussion :

Tout au long de ce chapitre, nous avons présenté des généralités nécessaires à la compréhension et à la conception d’un système de vidéosurveillance IP, ainsi que son évolution qui à permis de nos jours aux entreprises et aux particuliers de sécuriser leurs biens de façon efficace, et à de très longues distances.

C’est dans cette logique que les grands groupes industriels tel que ENIEM se tournent vers cette technologie qui ne cesse de s’améliorer.

I. Préambule :

Afin de mettre en place un système de vidéosurveillance IP, il est primordial d'avoir une idée précise du réseau existant ainsi que des différents problèmes qui peuvent survenir.

Dans ce chapitre, nous allons étudier de plus près les détails de l'entreprise concernée. C'est-à-dire présenter le groupe industriel ENIEM, étudier le réseau informatique existant, détecter les éventuels problèmes qui pourraient empêcher la mise en place du système, puis nous allons finir par des propositions de solutions à ces contraintes.

II. Etude du réseau informatique de l'ENIEM :

1. Définition d'un réseau informatique:

Un réseau informatique est un ensemble de plusieurs équipements informatiques. Tel que, des PC, des téléphones IP et des imprimantes interconnectés entre eux grâce à un support physique, le but de cette interconnexion est de capter et faire circuler des informations plus rapidement à travers le réseau.

L'apparition des réseaux a permis :

- Une amélioration de la rapidité de transmission, et un accès plus facile et rapide aux informations, cela se fait de manière quasi instantanée, permettant un gain de temps non négligeable par rapport aux anciens supports tel que, les CD-ROM.
- Une possibilité de communication instantanée entre les terminaux, permettant ainsi de se passer des lignes téléphoniques couteuses et encombrantes.
- Le partage de ressources entre les membres du réseau.
- Une structuration et une hiérarchisation des machines, avec la possibilité de limiter l'accès des machines à certaines ressources ou informations.
- Les créations de banque de données collectives, ce qui augmente les capacités de stockage et leur structuration sur le réseau.

Afin d'installer dans les meilleurs conditions un système dans un réseau LAN, il est primordial de faire l'étude de ce dernier afin d'anticiper les éventuels problèmes qui peuvent survenir pendant ou après l'installation, et de trouver les meilleures solutions à ces problèmes, c'est-à-dire des solutions durables et économiques à la fois.

1. Architecture du réseau informatique de l'ENIEM :

Le schéma suivant montre la disposition des éléments du réseau et les interconnexions qui les relient entre eux :

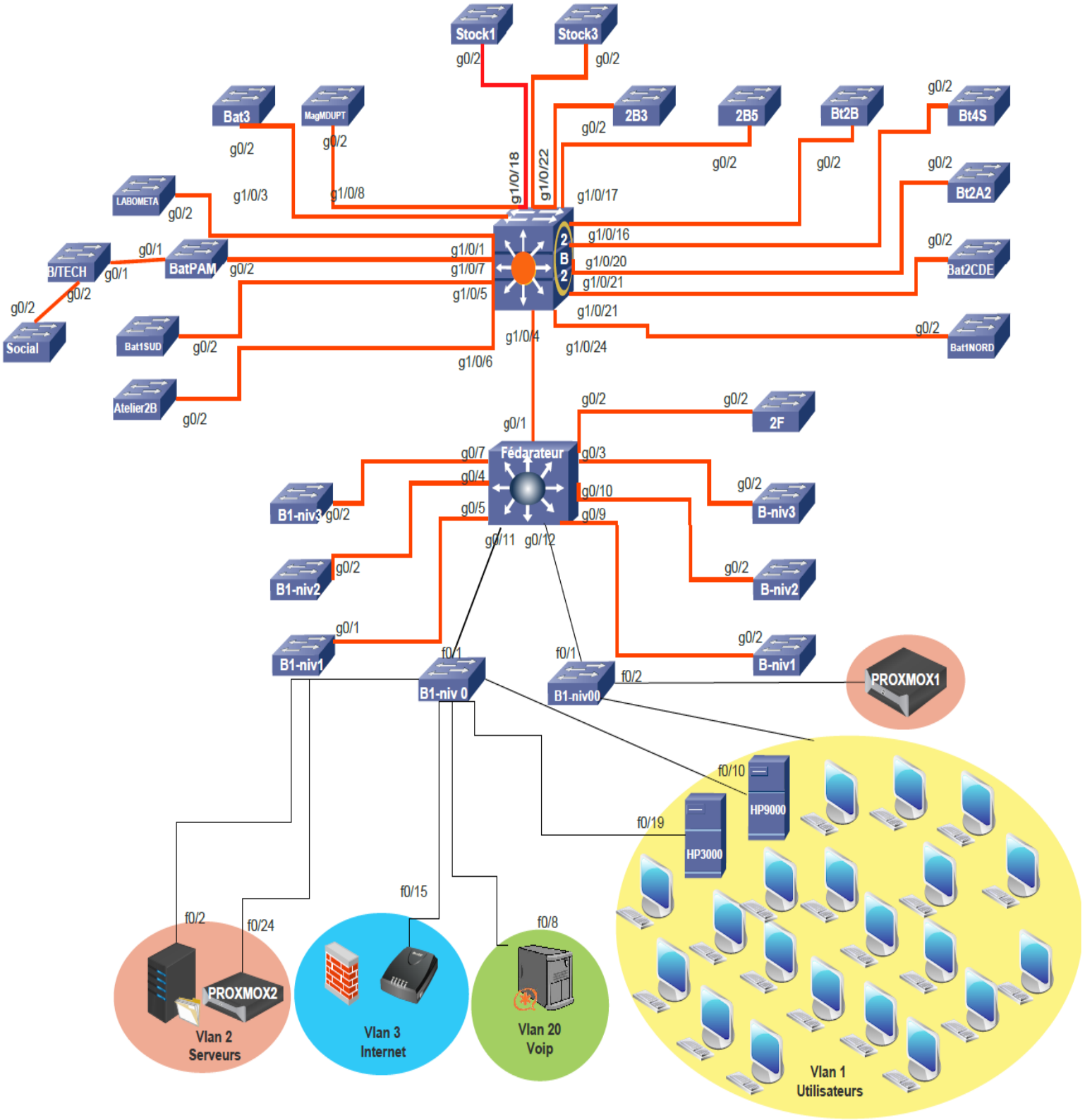

Figure 3.1 : Architecture du réseau informatique de l'ENIEM

Le réseau local de l'entreprise ENIEM est un réseau qui se compose de centaines d'éléments (serveurs et équipements informatiques) interconnectés par des câbles à paires torsadées et de la fibre optique et s'étend sur plus d'un kilomètre, les serveurs se trouvent tous dans une zone appellée l'UPT qui a les fonctions de gestion et maintenance du réseau informatique, et les équipements sont répartis dans toute l'infrastructure de l'usine et dans tous les blocs.

2. Les éléments du réseau :

Comme nous avons pu le voir précédemment, le réseau se compose de plusieurs éléments, chacun de ces éléments assure une fonction particulière dans le réseau, ils se résument comme suit :

- **Le pare-feu :**

Le pare-feu est un ensemble de différents composants matériels et logiciels qui contrôlent le trafic de données interne et externe selon la politique prédéfinie. Il permet d'analyser et de gérer les paquets entrants et sortants grâce à leur adresse IP, et refuse la circulation de ceux qui sont jugés malveillants par le pare-feu.

- **Les serveurs : [23]**

Le réseau local de l'ENIEM est un réseau étendu qui offre plusieurs applications, et chaque application est gérée grâce à un serveur. Nous allons donc énumérer chaque serveur et donner ses caractéristiques :

- **Serveur de fichier :**

C'est un serveur qui permet le partage de fichiers dans le réseau local, c'est-à-dire qu'un équipement pourra avoir accès aux données d'un autre par l'intermédiaire du serveur grâce au protocole FTP.

Le serveur de fichier possède une base de données puissante afin de stocker les fichiers destinés au partage, les autres utilisateurs n'auront qu'à envoyer une requête au serveur afin d'accéder aux données, une fois la requête acceptée, un tunnel sera créé par le protocole FTP pour acheminer jusqu'au client les fichiers préalablement enregistrés.

- **Le serveur HP 3000 :**

C'est un serveur de gestion possédant une base de données puissante et permet l'authentification et l'identification. Au sein de l'ENIEM, on lui a attribué la tache de gérer les stockes et la production, la gestion des soldes et les couts de production. Ainsi, grâce au serveur HP3000, il est possible de prévoir les besoins futurs en matériaux et garantir un fonctionnement permanant.

- **Le serveur HP 9000 :**

Comme son prédécesseur le HP3000, le HP9000 est un serveur de gestion auquel on a alloué la tâche de gestion de la comptabilité au sein de l'entreprise ENIEM, il permet aux responsables de la comptabilité de se connecter à ce serveur et de gérer les revenus et les dépenses de l'entreprise, les investissements, ainsi que les paies des salariés.

- **Le serveur Asterisk : [21]**

Le serveur asterisk est un serveur auquel on installe le logiciel asterisk qui offre les services de voix sur IP, il transforme les ordinateurs en autocommutateurs PABX et leur permet de lancer des appels entre eux grâce au logiciel ZOIPIER ou avec les téléphones IP.

- **Serveur PROXMOX : [10]**

C'est un serveur qui permet d'héberger des serveurs virtuels, il permet de virtualiser un serveur sans avoir besoin d'installer un système d'exploitation auparavant. C'est-à-dire que grâce au serveur PROXMOX, il est possible de créer plusieurs applications sans avoir besoin d'un matériel physique pour chacune d'entre elles.

Dans notre étude, il y'a deux serveur de ce type, PROXMOX 1 et PROXMOX 2, chacun d'entre eux héberge un groupe de serveurs tel que ce schéma nous le montre :

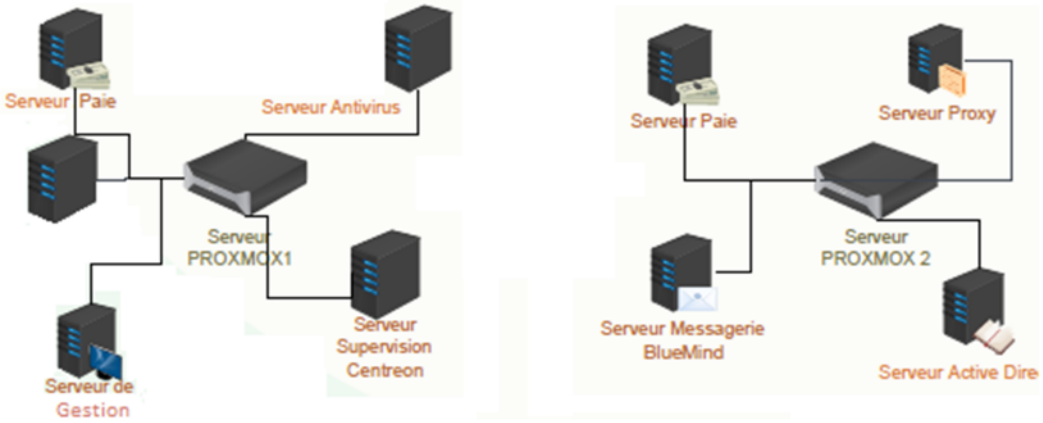

Figure 3.2 : Diagramme des serveurs Virtuels de l'ENIEM.

Les serveurs ainsi virtualisés, chacun d'entre eux a une fonctionnalité particulaire qu'on résumera comme suit :

- **Serveur proxy :**

Le serveur proxy est un équipement informatique qui sert d'intermédiaire entre deux clients, ce procédé permet la sécurisation grâce au filtrage et peut garantir l'anonymat des utilisateurs.

Il possède une mémoire cache qui sauvegarde les adresse afin d'accélérer la navigation, et possède une base de données qui permet d'enregistrer puis de convertir les noms en adresse IP.

- **Serveur paie :**

Comme son nom l'indique, ce serveur sert à gérer la paie des salariés de l'entreprise ENIEM, il contient une base de données qui stocke les noms, le poste, le nombre d'heures de travail et un algorithme s'occupe de calculer la paie de chaque salarié en fonction de ces données.

- **Serveur Messagerie BlueMind : [6]**

C'est un serveur qui gère la solution de messagerie BlueMind, il permet un travail collaboratif entre les employés de l'usine en offrant des services tel que les courriers, le partage de calendrier, la messagerie instantanée. Mais aussi la voix sur IP et le partage de documents.

- **Serveur anti virus :**

Un serveur antivirus est un serveur qui gère la sécurité de tous les équipements informatiques, il est de marque ALFATRON, il contient l'antivirus SYMANTEC ENDPOINT SECURITY 5.0, qui peut être installé automatiquement dès qu'un appareil se connecte au réseau, il gère aussi les mises à jours de cet antivirus et peut être configuré à distance.

- Serveur Active Directory :

C'est un serveur qui offre une solution de gestion centralisée des réseaux informatiques utilisant Windows, Il permet la sécurisation du réseau grâce à l'authentification et à l'identification des utilisateurs en répertoriant tous leurs comptes et leurs mots de passes dans une base de données, si le nom d'utilisateur et le mot de passe ne correspondent pas, l'accès lui sera refusé.

Il permet aussi de gérer les ressources au sein du réseau, les utilisateurs peuvent ainsi avoir accès à des applications, aux données et aux ressources partagées, et les administrateurs peuvent avoir connaissance des demandes et contrôler les droits d'accès aux ressources et à certains fichiers.

- Serveur SVN :

C'est un serveur qui contient un logiciel appelé Apache Subversion, ce dernier permet à des utilisateurs d'enregistrer un fichier sur le serveur. Dans le cas ou ce fichier est modifié par l'un d'entre eux, cette modification sera instantanément enregistrée dans le serveur.

Ce principe permet à plusieurs employés de l'entreprise de travailler en parallèle sur un même fichier et d'être constamment tenus au courant de son avancement.

- Serveur de gestion : [12]

Un serveur de gestion est un serveur conçu pour le contrôle et la gestion des éléments d'un réseau, que se soit les équipements, les données mais aussi les autres serveurs. Le serveur de gestion possède plusieurs caractéristiques, tel que :

- Le contrôle des connexions et prise en charge des applications.
- Le contrôle d'accès aux médias par les utilisateurs.
- La fiabilité du réseau en préservant la connexion aux sources.
- Le maintien de la connexion en cas de panne des nœuds.

Grâce à une plateforme de gestion, un responsable informatique pourra configurer des paramètres qui définiront les stratégies qu'adoptera le serveur dans certains cas.

- Serveur Supervision Centreon :

C'est un serveur conçu pour gérer la plateforme de supervision d'applications « centreon », il permet aux utilisateurs de se connecter au serveur et d'avoir une vue graphique du système informatique et d'accéder aux différents paramètres afin de gérer les applications du réseau.

- ## Les équipements d'interconnexion :

Les équipements utilisés dans le réseau constituant l'enceinte de L'ENIEM sont des Switch de marques Cisco, en effet on peut citer deux types :

1) Les Switch fédérateurs : [4]

Les Switch fédérateurs sont des Switch entièrement composés de ports en fibres optiques, Il existe deux versions de Switch fédérateurs qui sont utilisés dans la configuration du réseau de l'ENIEM :

- **L'ancienne version Cisco 3560 :**

La série Cisco Catalyst 3560 est une gamme de commutateurs de configuration fixe qui incluent la fonctionnalité PoE, et les configurations Fast Ethernet et Gigabit Ethernet.

Le Cisco Catalyst 3560 est un commutateur de couche d'accès idéal pour les environnements d'accès LAN ou de branche de bureau de petite entreprise, en permettant le déploiement de nouvelles applications telles que la téléphonie IP, l'accès, la vidéosurveillance, les systèmes de gestion des bâtiments et les kiosques vidéos distants.

On peut déployer des services intelligents à l'échelle du réseau, tels que la qualité avancée du service (QoS), la limitation des tarifs, les listes de contrôle d'accès (ACL), la gestion de multidiffusion et le routage IP haute performance, tout en maintenant la simplicité de la commutation LAN traditionnelle.

- **La nouvelle version cisco 3750 :**

Les commutateurs de la série Cisco Catalyst 3750 sont des commutateurs innovants qui améliorent l'efficacité de fonctionnement du réseau local en combinant une facilité d'utilisation de pointe et une grande résilience pour les commutateurs empilables. Comme son prédécesseur, la version 3750 offre la fonctionnalité PoE.

Pour les organisations de taille moyenne et les succursales d'entreprises, la série Cisco Catalyst 3750 facilite le déploiement d'applications convergentes et s'adapte aux besoins de l'entreprise en fournissant une flexibilité de configuration, un support pour les modèles réseaux convergents et l'automatisation des configurations de services du réseau intelligent. De plus, la série Cisco Catalyst 3750 est optimisée pour le déploiement Gigabit Ethernet à haute densité et comprend une gamme variée de commutateurs qui répondent aux exigences de connectivité, agrégation de petits réseaux.

2) Les Switch intermédiaire : [4]

Les Switch intermédiaires sont des équipements qui servent à commuter les données entre les équipements informatiques et les Switch fédérateurs. C'est des Switch contenant des ports RG45 afin de relier les équipements grâce aux câbles à paires torsadées, et des ports en fibre optique qui assurent une liaison avec le Switch fédérateur.

Le réseau LAN de l'entreprise contient 2 séries de Switch intermédiaire :

- **L'ancienne version Cisco 2950 :**

Ce sont des commutateurs autonomes, de configuration fixe et gérés de 10/100 Mbps fournissant une connectivité basique de groupe de travail pour les réseaux de petite à moyenne taille. Ces commutateurs de bureau à vitesse variable sont livrés avec les fonctionnalités du logiciel Standard Image et offrent des fonctions de logiciel Cisco IOS pour les services de base de données, de voix et de vidéo au bord du réseau.

- **La nouvelle version Cisco 2960 :**

Les commutateurs série Cisco Catalyst 2960 sont une amélioration de 2950 ils offrent une meilleure facilité d'utilisation, des opérations hautement sécurisées, une durabilité améliorée et une expérience de réseau sans bordure. Les commutateurs de la série Catalyst 2960 incluent une nouvelle capacité d'empilement de commutateurs, avec une connectivité 1 et 10 Gigabit et Power over Ethernet Plus (PoE +) et une connectivité d'accès Fast Ethernet.

• Les équipements :

L'entreprise ENIEM contient plusieurs terminaux à chaque extrémité du réseau, on trouve :

- **Les téléphones IP :**

Ce sont des téléphones qui utilisent le réseau IP afin de transmettre la voix, grâce au protocole SIP, les employés pourront communiquer entre eux sur de longues distances sur l'infrastructure de l'ENIEM, ces téléphones sont de marques SIP et GOBLIN, ils sont en nombres de 235 téléphones.

- **Les ordinateurs :**

Ce sont des équipements informatiques présents dans chaque bureau de chaque unité de l'usine de L'ENIEM, ce sont des ordinateurs de marques HP et ALFATRON, ils sont en nombre de 160 ordinateurs.

- Les imprimantes :

A l'exemple des imprimantes ou des scanners, ce sont tous les équipements informatiques que les utilisateurs se partagent dans le réseau. Les imprimantes présentes dans les différents bureaux de chaque unité de l'usine sont de marques CANON, HP et KYOCERA.

- ## Application :

Les applications présentes dans le réseau local de l'ENIEM sont diverses, elles sont installées sur les serveurs et chacune d'entre elles est importante et contribue au fonctionnement de l'entreprise. Nous allons les présenter sous forme de tableau :

Applications	Rôles	Bénéficiaires
PROXMOX	- Création et gestion de machines virtuelles.	L'équipe de gestion et maintenance du réseau informatique.
Centreon	- La consultation de l'état des services et des machines supervisées. - L'accès aux événements de supervision. - La gestion avancée des utilisateurs via des listes de contrôle d'accès (ACL)	L'équipe de gestion et maintenance du réseau informatique.
BlueMind	- Service de messagerie instantané. - Partage de fichiers. - Calendrier collectif. - Téléphonie IP.	Les employés de l'unité technique de l'entreprise.
Active directory	- Authentification des utilisateurs. - Gestions des ressources.	L'équipe de gestion et maintenance du réseau informatique.
Apache Subversion	- Modification des fichiers en temps réel et permet le travail collectif à distance.	Tous les employés de l'entreprise.

SYMANTEC ENDPOINT SECURITY 5.0	- Protection des équipements informatiques contre les logiciels malveillants.	L'équipe de gestion et maintenance du réseau informatique.

Tableau 3.1 : Les applications du réseau de l'entreprise ENIEM

- **Les protocoles :**

Les protocoles sont nécessaires pour le fonctionnement des applications citées précédemment, ainsi que le fonctionnement de l'ensemble du réseau.

Le tableau suivant nous montre les protocoles utilisés par le réseau LAN de l'ENIEM :

Protocoles	Rôles
Internet Protocole (IP)	Segmente les données en paquets, chaque paquet contient des informations sur le destinataire (adresse IP) et peut donc être routé jusqu'à arriver à destination.
Protocoles http et https	Permet de lancer une requête http à un serveur web dans le but d'accéder à des documents écrits en HTML.
Protocole TCP/IP	Permet l'encapsulation et le transport des données ainsi que le contrôle d'erreurs grâce à la couche TCP.
Protocole FTP	Permet un transfert de données de manière efficace entre des machines distantes.
Protocole SSH	Impose aux utilisateurs une clé de chiffrement. Grâce à ce procédé, tous les segments TCP sont authentifiés et chiffrés. Ce principe nous permet de configurer à distance les Switch de façon sécurisée.
Protocole Telnet	Permet de communiquer avec un serveur distant en échangeant des lignes de textes et en recevant des réponses sous forme de texte.
Protocole SIP	Permet de transporter la voix sur un réseau IP

Tableau 3.2 : Les protocole du réseau de l'entreprise ENIEM

III. Les besoins de sécurisation de l'ENIEM :

Après l'étude du réseau local de l'ENIEM, nous avons constaté des caractéristiques permettant la mise en place d'un système de vidéosurveillance. Toutefois, le réseau doit être amélioré si on veut remplir les besoins suivants :

- La surveillance jour et nuit des frontières de l'entreprise avec des caméras IP à infrarouge équipé de capteur de mouvement, ainsi que la surveillance de quelques bloques jugés à risque. Les différents points à surveiller dans l'entreprise ENIEM sont indiqués sur la carte suivante :

Figure 3.3 : Image satellite des zones à sécuriser.

- Le système doit être fiable et doit avoir la possibilité de faire transiter plusieurs flux vidéo simultanés.
- Un poste de surveillance pour permettre aux agents de sécurité de visionner en temps réel toutes les images vidéo.
- Une base de données où seront archivées les images de vidéosurveillances.

IV. Critique du réseau local de l'ENIEM :

Le réseau local de l'entreprise ENIEM possédant de nombreux moyens matériels et logiciels, il comprend de nombreux points fort comme :

- Des équipements haut de gamme.
- Un réseau performant notamment grâce à la technologie fast Ethernet et les liaisons en fibre optique.

- Un nombre de Switch important et disposé de sorte à couvrir tous les blocks de l'entreprise.
- Une salle dédiée à la maintenance des serveurs très bien protégée avec des onduleurs et des refroidisseurs.
- Existence de pare-feu et d'anti-virus dédiée à la sécurité des serveurs.
- Une connexion internet haut-débit.

Le réseau local actuel de l'entreprise ENIEM possèdent suffisamment de ressources matérielles et logicielles afin d'installer un système de vidéosurveillance IP. Néanmoins, Nous avons vu précédemment les besoins de l'entreprise en termes de sécurisation, et nous avons constaté qu'il existe quelques contraintes qui empêchent de satisfaire ces besoins :

Le principal problème est l'absence de couverture réseau à certains endroits de l'entreprise ENIEM ou il est nécessaire de mettre des caméras, l'image suivante nous montre les zones où les caméras doivent être installées afin de remplir les besoins ainsi que les équipements du réseau :

Figure 3.4 : Image satellite de l'emplacement des équipements du réseau informatique de l'ENIEM.

Les zones en vert sont à une distance raisonnable pour une liaison en câble à paires torsadées (moins de 100 mètres).

Par contre, les zones en orange sont à une distance trop éloignée pour une liaison avec des câbles à paires torsadées (nettement supérieurs à 100 mètres).

On rajoute à ce problème la nécessité d'installer sur le réseau local de l'ENIEM :

- Un serveur de gestion de la vidéosurveillance qui garantit la fiabilité du système.
- Un VLAN dédié à la vidéo, ce qui peut conduire à des disfonctionnement du système.
- Une plateforme de gestions d'images vidéo qu'utiliseraient les agents de la sécurité pour visionner et gérer les images vidéo.

Par conséquence, il est impératif de proposer des solutions pratiques à ces problèmes pour pouvoir satisfaire les besoins de l'entreprise.

V. Nos propositions :

Nous pourrons résoudre les problèmes vus précédemment et satisfaire les besoins en sécurité de l'entreprise ENIEM en proposant de différentes solutions, elles se résument comme suit :

1- Le serveur CamTrace :

a) Présentation : [24]

Une solution facile, fiable et robuste, capable de résoudre deux des problèmes cités précédemment, CamTrace a été conçu pour répondre aux multiples besoins de la vidéosurveillance industrielle. Elle inclut notamment :

- Un serveur de gestion de vidéo et une base de données puissante (jusqu'à 8 To) pour enregistrer les images.
- Un système d'authentification pour accéder aux images.
- La capacité de gérer plusieurs dizaines de caméras réseaux simultanément.
- Le contrôle et l'administration du système depuis n'importe quel poste du réseau ou à distance.
- La possibilité d'associer plusieurs serveurs CamTrace afin de gérer un nombre pouvant aller à des centaines de caméras réseaux.
- Un logiciel flexible et capable de réunir plusieurs images dans un seul écran.

- Un mode de visualisation de groupe adapté aux faibles débits, c'est à dire que si le débit d'internet est faible, il est possible de régler la compression des vidéo ou même de passer en « niveau de gris » pour maintenir la fluidité du flux.

b) Configuration : [25]

Pour configurer le serveur, dans un premier temps on ouvre le menu et on l'active ,ensuite nous allons accéder à l'interface réseau pour lui attribuer une adresse IP :

Grâce à cette amélioration, le réseau disposera d'une base de données puissante capable

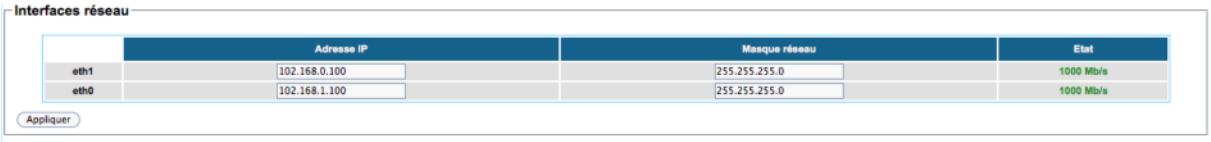

Figure 3.5 : Attribution de l'adresse IP pour le serveur Camtrace.

d'archiver les enregistrements sur plusieurs mois, ainsi que d'un logiciel spécialisé qui permettra de visionner les images de plusieurs caméras simultanément.

2- Création d'un VLAN :

L'adresse IP du serveur et l'adresse IP des caméras réseaux ne doivent pas être du même sous-réseau que la voix ou les données sous peine de graves dysfonctionnements. C'est pour cette raison qu'il est nécessaire de créer un VLAN spécialement pour le transport du flux vidéo.

La configuration d'un VLAN se fait sur un Switch, grâce au logiciel « Cisco Packet Tracer », nous allons simuler une configuration de VLAN sur Switch Cisco :

1. La première étape consiste à sélectionner dans le logiciel les équipements qui constituera le réseau :

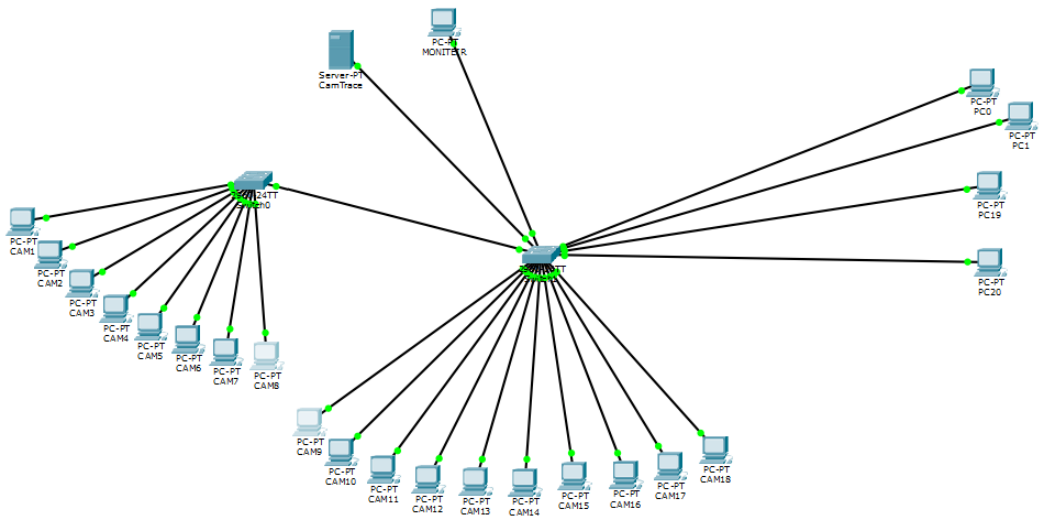

Figure 3.6 : Simulation d'un réseau sur le logiciel Cisco Packet Tracer

Ce réseau comporte :

- Deux Switch Cisco 2560 doté de 24 ports fast Ethernet.
- Un serveur CamTrace.
- Un PC qui servira de moniteur pour la vidéosurveillance.
- Quatre PC pour les données (qui ne font pas parti de notre système).
- 18 caméras réseau (on les a représentées par un PC car les caméras réseaux ne sont pas incluses dans ce logiciel)

2. Attribution des adresses IP pour les équipements :

Nous avons choisi une adresse de classe C :

- On a attribué aux équipements du système de vidéosurveillance une adresse allant de 192.164.0.1 ➔ 192.164.0.20
- Tandis que les équipements étrangers au système de vidéosurveillance se voient attribués une adresse allant de 192.164.1.1 ➔ 192.164.1.4

3. Création des VLAN :

Pour créer les VLAN nous devons tout d'abord accéder à l'interface de ligne de commande des Switch, afin d'introduire les commandes suivantes :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 4
Switch(config-vlan)#name vlan_videosurveillance
Switch(config-vlan)#exit
Switch(config)#vlan 2
Switch(config-vlan)#name vlan_donnes
Switch(config-vlan)#exit
Switch(config)#
```

Figure 3.7 : Commandes de création d'un VLAN.

Ainsi nous venons de créer deux VLAN, un pour la vidéosurveillance et un autre pour les données.

4. La dernière étape consiste à affecter des ports au VLAN :

Toujours dans l'interface de ligne de commande des Switch, nous allons affecter les ports du Switch au VLAN vidéo grâce aux commandes suivantes :

```
Switch(config)#interface fastethernet 0/6
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 4
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/7
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 4
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/8
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 4
Switch(config-if)#exit
Switch(config)#
```

Figure 3.8 : Commandes d'affectation des ports au VLAN données.

Selon le choix des ports auxquels on a branché les équipements du système de vidéosurveillance dans le logiciel, nous devons attribuer au VLAN vidéo ces ports fast Ethernet, dans notre cas, nous allons attribuer au VLAN vidéo les ports allant de 1 jusqu'à 20.

Ensuite les ports 21 jusqu'à 24 seront attribués au VLAN données :

```
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 4
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/20
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 4
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/21
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 2
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/22
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 2
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/23
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 2
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/24
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport acces vlan 2
Switch(config-if)#exit
Switch(config)#
```

Figure 3.9 : Commandes d'affectation des ports à un VLAN vidéo.

5. Vérification :

La vérification se fait grâce a la commande « sh vlan brief », cette commande permet d'indiquer tous les VLAN crées sur les Switch et les ports qui leur sont attribués :

```
Switch#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
2    vlan_donnes                       active    Fa0/21, Fa0/22,
Fa0/23, Fa0/24
4    vlan_videosurveillance            active    Fa0/1, Fa0/2,
Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Figure 3.10 : Commande de vérification de la création des VLAN.

3- Mise en place d'une solution pour les zones éloignées :

Afin de résoudre le problème de distance, nous devons tout d'abord avoir une idée de la distance maximale qui sépare ces zones des Switch les plus proches. Et pour cela nous avons utilisé l'application « Google map » pour mesurer les distances les plus éloignées. Puis nous l'avons noté sur la figure suivante :

Figure 3.11 : Image satellite de la distance entre les caméras et les Switch.

Malgré que les distances soient supérieures à 100 mètres, ce problème peu être facilement résolu soit par un répéteur régénérateur, ou bien par un point d'accès WIFI.

Nous avons opté pour la deuxième solution, car c'est la solution la plus facile à installer et à configurer, mais aussi dans le but d'éviter une détérioration de la ligne de transmission (environnement extérieur).

1. Simulation d'une solution WIFI :

Toujours en utilisant le logiciel Cisco Packet Tracer, nous avons simulé l'installation d'un point d'accès wifi :

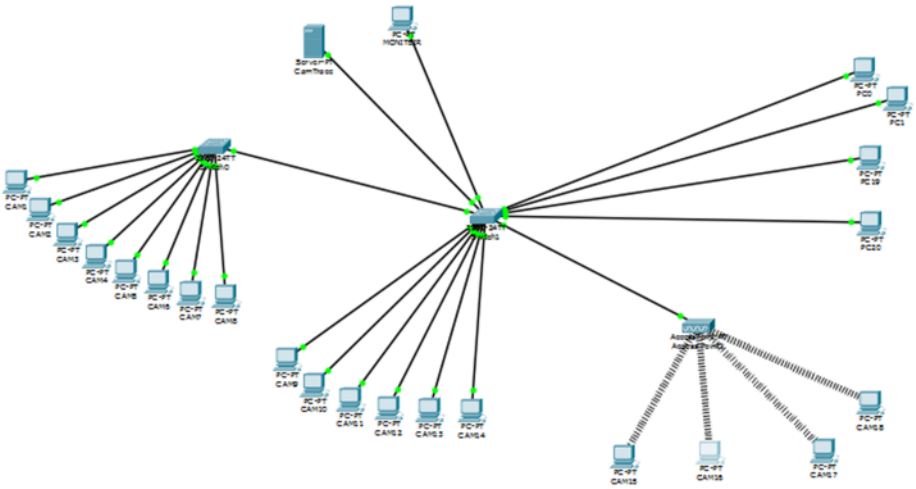

Figure 3.12 : Simulation d'un réseau avec point d'accès Wi-Fi sur le logiciel Cisco Packet Tracer.

Le point d'accès WIFI s'installe en suivant ces étapes :

- Brancher le point d'accès WIFI à un des Switch.
- Définir un mot de passe.
- Equiper les machines (appartenant au VLAN vidéo) d'une antenne WIFI.
- Se connecter au réseau en introduisant le mot de passe.

On peut s'assurer du fonctionnement du WIFI grâce à la commende « ping », on l'utilisera sur un PC du réseau initial pour vérifier la connexion avec une machine connectée au réseau par WIFI, on obtient :

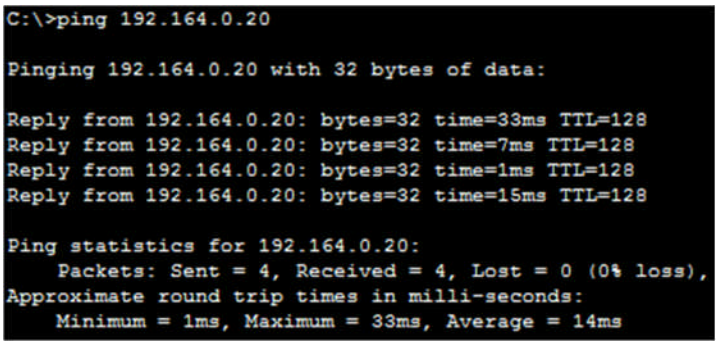

Figure 3.13 : Vérification de la connexion Wi-Fi.

0% de perte, on conclue que tout fonctionne normalement.

2. Sélection de la position des points d'accès WIFI :

Nous avons choisi un équipement qui utilise la norme 802.11g car elle permet une couverture allant jusqu'à 400 mètres (à l'extérieur) tout en gardant un très haut débit. On arrivera à couvrir ces zones en sélectionnant une bonne position des points d'accès.

Le schéma suivant montre les positions que nous avons choisies et qui remplissent cette condition :

Figure 3.14 : Image satellite de la position des points d'accès.

VI. Discussion :

Dans ce chapitre, nous avons présenté l'étendu des moyens matériels et logiciels du réseau local de l'entreprise ENIEM, et fait la critique de ce dernier.

Apres avoir fait l'étude du réseau local, nous avons apporté des propositions d'amélioration pour l'optimisation de ce réseau, afin de répondre aux besoins de sécurité grâce à un système de vidéosurveillance étendu et performent.

I. Préambule :

Le réseau informatique de l'ENIEM est maintenant adapté à recevoir le système de vidéosurveillance IP.

Dans ce chapitre, nous allons présenter le matériel que nous utiliserons, les étapes de mise en place d'un système de vidéosurveillance sur le réseau informatique de l'ENIEM. Pour cela, nous utiliserons un logiciel conçu pour simuler un système de vidéosurveillance IP, puis nous procéderons à un calcul pour s'assurer de la fluidité du système.

II. Présentation des équipements :

Nous allons présenter les équipements dont nous aurons besoins afin d'installer le système de vidéosurveillance sur le réseau local de l'ENIEM.

1) Les caméras IP :

Nous utiliserons 2 types de caméras réseaux, une de marque AXIS et une autre de marque Vivotek :

- **Caméra réseau AXIS M1124 : [26]**

L'AXIS M1124 est une caméra jour/nuit offrant une vidéo HDTV 720p à 25/30 images par seconde, elle est résistante à l'humidité et à la poussière, elle peut être installée à l'extérieur comme à l'intérieur. Elle intègre la technologie de compression H.264 qui réduit considérablement les besoins en termes de bande passante et de stockage.

Figure 4.1 : Caméra AXIS M1124.

Elle intègre aussi le logement de carte microSD pour le stockage Edge, des ports d'entrée et de sortie numériques pour le raccordement à des équipements externes, ainsi qu'un port Ethernet qui inclut la technologie PoE et elle prend en charge tous les protocoles liés à la vidéosurveillance tel que le TCP/IP, HTTPS, RTP et RTPS. Elle possède la capacité accrue pour les applications analytiques comme le compteur des personnes ou la cartographie thermique.

La camera AXIS M1124 nous offre aussi les fonctions suivantes :

- Réception d'alertes automatiques en cas de détection de mouvement par des capteurs.

- Recherche rapide dans les archives vidéos, configuration et contrôle de caméra avec le logiciel de vidéosurveillance inclus.

Notre choix s'est porté sur cette caméra car elle possède une résolution haute définition et elle offre des services qui répondent aux besoins de l'entreprise, elle est compatible avec le logiciel Camtrace, et elle est la moins chère de sa catégorie.

- **Caméra réseau Vivotek IP8336W: [27]**

La VIVOTEK IP8336W est une caméra IP conçue pour la surveillance intérieure et extérieure, équipée d'un boîtier résistant aux intempéries et d'un capteur 1Méga pixels permettant une résolution de 1280x800 pixels à 30 images par seconde. Elle intègre également un filtre infrarouge qui peut être retiré automatiquement la nuit.

Elle est dotée de la technologie IEEE 802.11 b/g/n, ainsi que de la compression H.264 standard de l'industrie avec les options MPEG-4 et MJPEG. Et peut aussi être équipée d'une carte SD/SDHC pour enregistrer les images vidéos.

Figure 4.2 : Caméra Vivotek IP8336W.

Notre choix s'est porté sur cette caméra car en plus de sa résolution haute définition, elle est compatible avec le logiciel Camtrace, et elle intègre la technologie des points d'accès que nous avons configurés « IEEE 802.11g »

2) Les câbles à paires torsadées :

Pour l'installation des caméras ,nous allons avoir besoin d'environ 800 mètres de câbles à paires torsadées droit de catégorie 5.

III. Etapes d'installation des caméras réseaux:

Les étapes d'installation d'une caméra réseau peuvent être résumées comme suit :

1) Fixation :

Afin de fixer la camera IP, nous percerons un mur et nous allons visser la caméra comme indiqué sur cette figure :

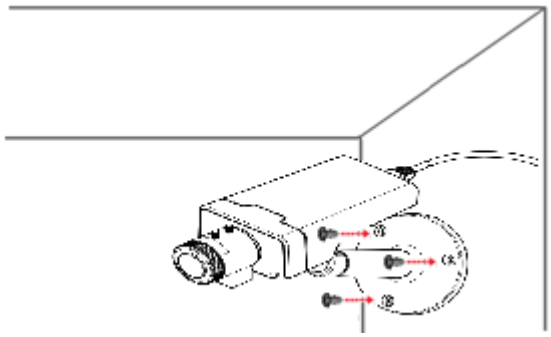

Figure 4.3 : Fixation d'une caméra réseau sur un mur.

2) Branchement :[26]

La figure 4.4 représente la face arrière d'une caméra IP :

- La flèche n°1 indique une LED qui indique la connexion au réseau LAN.
- La flèche n°2 indique un port qui sert à recevoir une carte microSD.
- La flèche n°3 indique un connecteur d'alimentation dans le cas d'un réseau dépourvu de technologie PoE.
- La flèche n°4 indique un bouton de commande qui sert à réinitialiser l'appareil aux paramètres d'usine par défaut.
- La flèche n°5 indique un port RG-45 qui sert à connecter la caméra au réseau local.
- La flèche n°6 indique un voyant d'alimentation.
- La flèche n°7 indique un voyant d'état indiquant la présence d'éventuels problèmes.

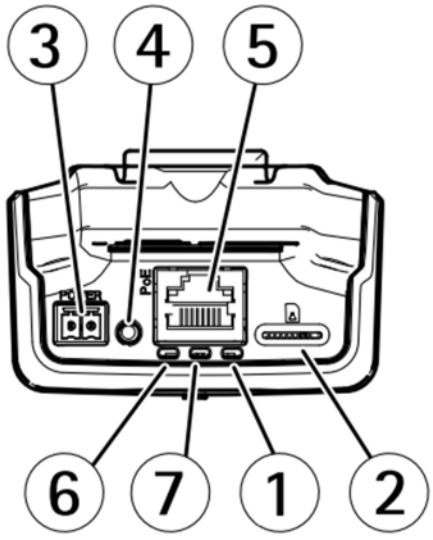

Figure 4.4 : Les ports d'une caméra réseau.

Dans notre étude, nous aurons seulement besoin de brancher le câble Ethernet à un Switch, en faisant attention à choisir un port correspondant au VLAN de la vidéosurveillance.

3) Configuration : [26]

Pour configurer la caméra réseau, il faut introduire l'adresse IP de la caméra dans un navigateur internet puis une page s'affiche, la figure 4.5 nous montre cette dernière :

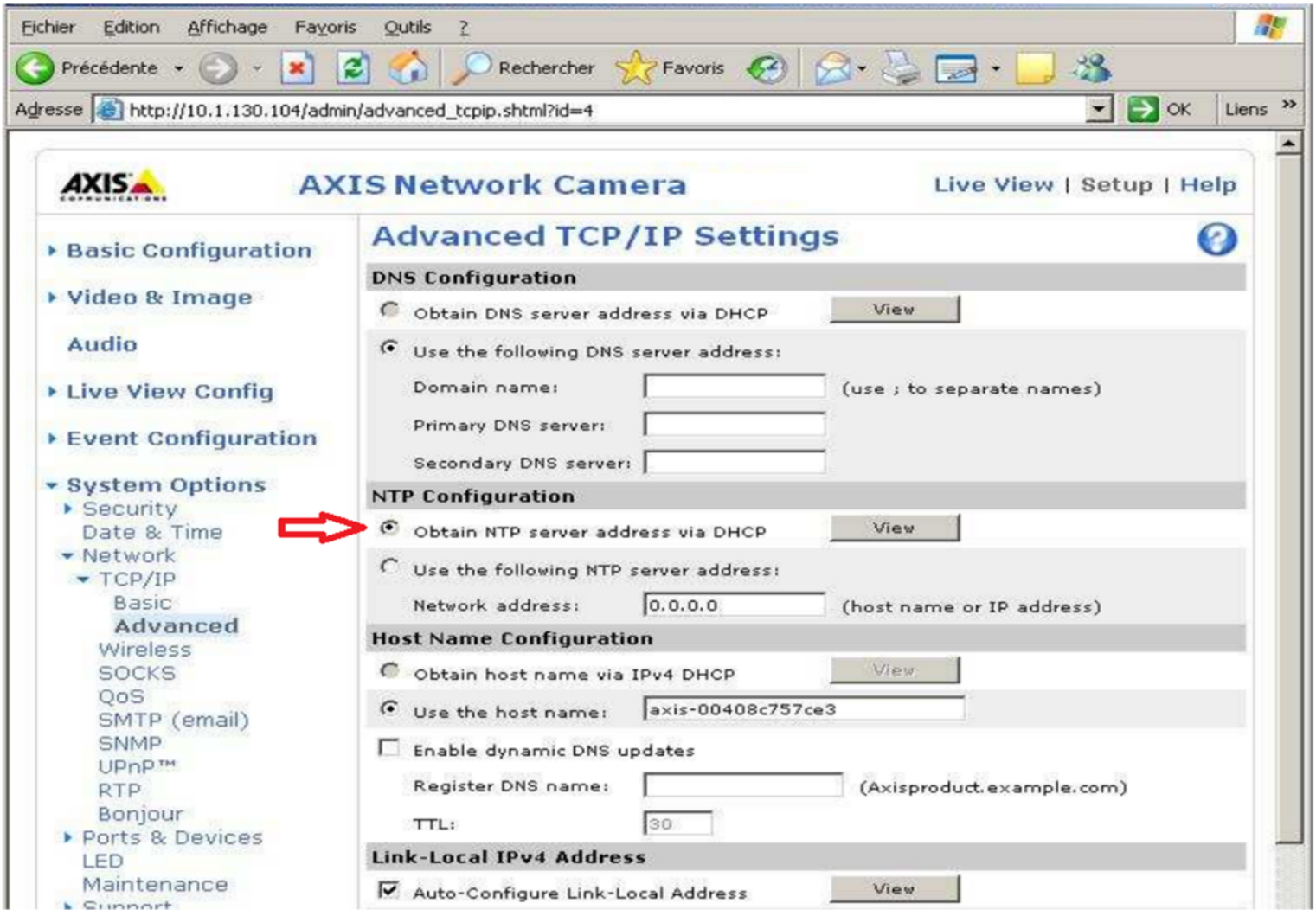

Figure 4.5 : Configuration d'une caméra réseau.

On accède aux paramètres réseaux de la caméra IP, dans la case « NTP configuration » nous choisirons « Obtain NTP server adresse via DHCP » c'est-à-dire que l'adresse IP sera attribuée par le serveur DHCP et on enregistre les paramètres.

Il est aussi possible de configurer le flux vidéo, audio, le type de compression afin d'adapter la caméra aux besoins.

4) Installation du logiciel de gestion : [25]

Les modèles AXIS M1124 , Vivotek IP8336W comprennent, une suite logicielle de surveillance complète qui facilite la configuration et le contrôle de 16 caméras maximum en même temps.

Néanmoins, le nombre de caméras présentes dans l'usine de l'ENIEM dépassera les 16 caméras, c'est pour cette raison qu'on va installer le logiciel Camtrace, qui peut assurer la gestion de plusieurs dizaines de caméras IP.

Pour installer le logiciel, il faut accéder au site de Camtrace et de télécharger le SETUP. Une fois le SETUP est lancé, on choisira d'exécuter « installation de l'application client » afin d'installer le logiciel.

Pour ajouter les caméras à ce logiciel, on doit mettre en marche le logiciel et suivre ces étapes :

- On clique sur l'icône « Administration» dans la page console principale puis sur « Système» pour afficher la page Réglage, puis on clique sur la section « Ajout de caméras ».
- Le tableau suivant s'affichera sur l'écran :

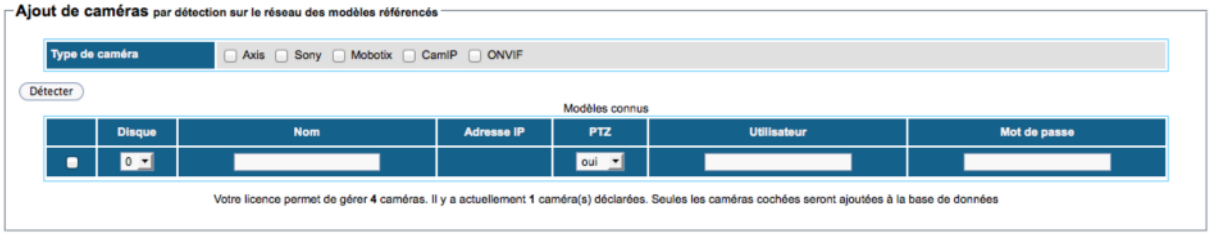

Figure 4.6 : Ajout d'une caméra réseau sur le logiciel Camtrace.

On remplit les différentes cases en introduisant les identificateurs de la caméra (marque, adresse IP, non d'utilisateur, mot de passe). Ensuite on valide en appuyant sur la touche «ajouter».

On répétera ce procédé jusqu'à ajouter toutes les caméras.

Une fois les caméras ajoutées, nous devrons configurer l'enregistreur afin que les images soient enregistrées dans le serveur Camtrace. Pour ce faire, on accède au logiciel Camtrace Client, on clique dans le menu sur « nouveau serveur » :

La fenêtre suivante s'affiche sur l'écran :

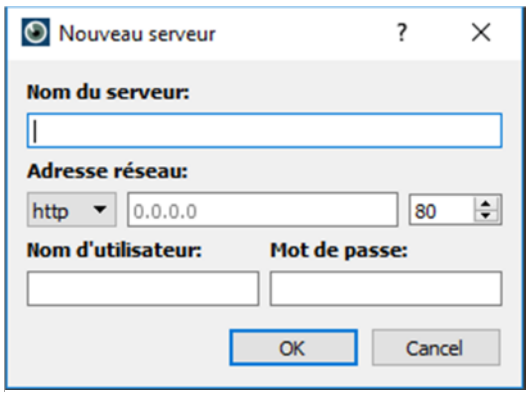

Figure 4.7 : Ajout d'un serveur sur le logiciel Camtrace.

Nous remplirons les cases avec le nom du serveur, son adresse IP, le nom d'utilisateur ainsi que son mot de passe, puis on enregistre les paramètres en appuyant sur « OK ».

IV. Simulation :

Notre simulation a pour objectif de déterminer le nombre de caméras que nous devons utiliser afin de remplir les exigences de l'entreprise ENIEM, il nous permettra aussi de déterminer la hauteur et l'angle que doit prendre la caméra afin d'élargir au maximum son champ de vision. Pour faire cette simulation, nous utiliserons le logiciel IP Vidéo System Design Tool.

1) Présentation du logiciel :

IP Vidéo System Design Tool est un outil de conception de système de vidéosurveillance IP, rapidement et Efficacement.
Les principales fonctionnalités disponibles dans ce logiciel sont :

- Trouver les meilleures positions pour les caméras.
- Obtenir les champs de vision de la caméra IP et les angles de visionnement.
- Réduire le processus fastidieux de calcul de la longueur focale de l'objectif.
- Estimation de la bande passante réseau requise pour les systèmes vidéo IP avec un nombre illimité de caméras réseau Et serveurs vidéos.
- Calculer l'espace de stockage du disque dur pour les archives vidéos.
- Importer des images d'arrière plan de JPEG / BMP.
- Importer des modèles 3D utilisateur (dans la version Pro / Business).
- Importer des dessins Auto CAD (dans la version Pro / Business).

- Exporter les calculs, dessins et images 3D vers Word, Excel, Visio ou vers d'autres logiciels.

2)Fonctionnement :

Nous allons commencer notre simulation par la modélisation de l'infrastructure de l'usine ENIEM dans le logiciel IP vidéo Design Tool, Pour ce faire, nous avons chargé une image satellite de l'entreprise, et régler l'échelle afin que le logiciel fasse correspondre les distances avec le champ de vision des caméras, puis nous avons reproduit les murs et les bloques de l'usine en 3 dimension grâce à la commande « ajouter un mur », la figure suivante est une capture d'écran de notre projet :

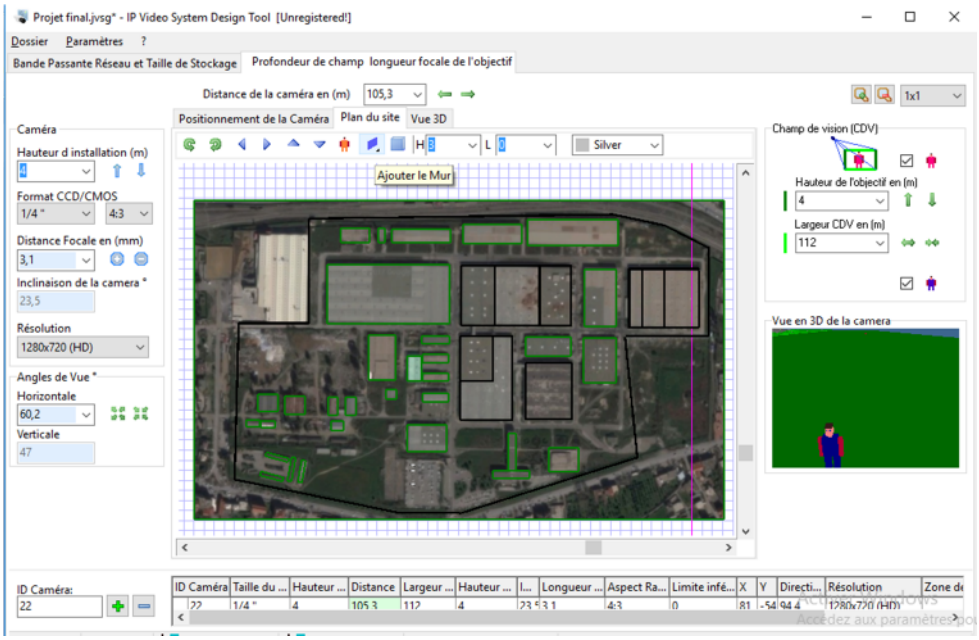

Figure 4.8 : Modélisation de l'infrastructure de l'ENIEM

Ensuite, sur la fenêtre gauche du logiciel, nous allons introduire les caractéristiques (résolution, format CCD/CMOS, distance focal…etc.) des caméras que nous utiliserons afin de créer des caméras IP virtuelles avec des capacités correspondantes à celles qui seront installées.
Puis nous allons placer les caméras afin de couvrir toute les zones à protéger.

La figure suivante nous montre un aperçu du système de vidéosurveillance IP de l'ENIEM :

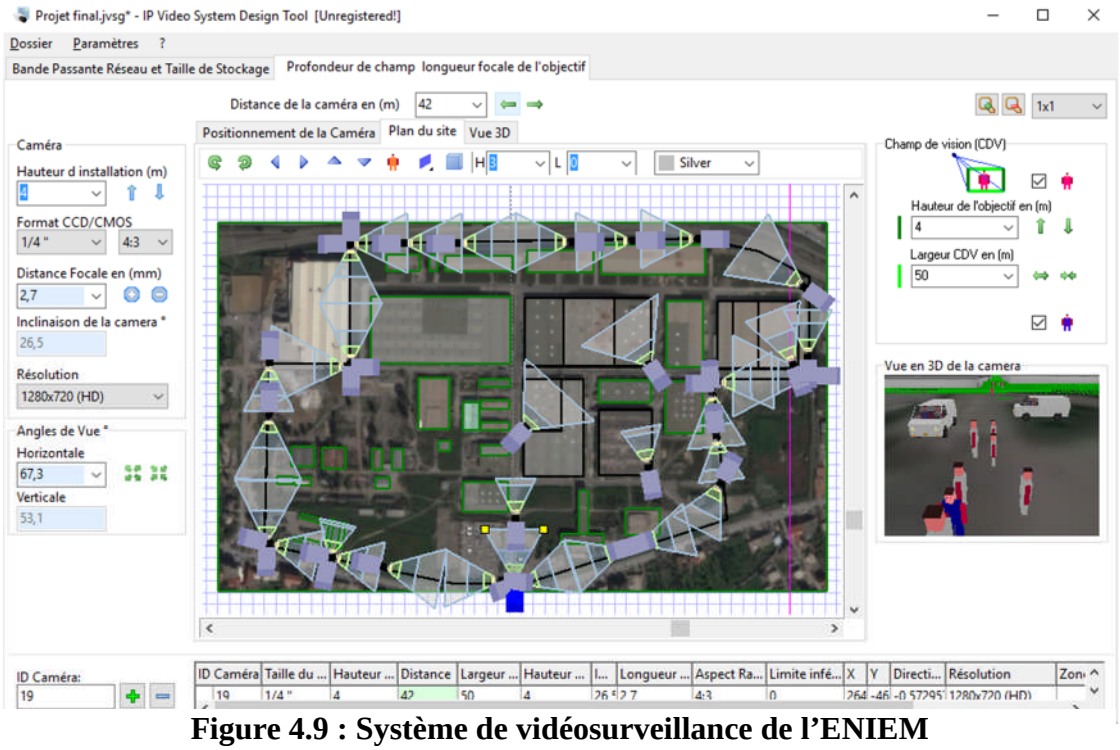

Figure 4.9 : Système de vidéosurveillance de l'ENIEM

Grâce à l'outil « vue en 3D de la caméra » à droite, le logiciel nous donne un aperçu des images captées par la caméra, nous pourrons ainsi changer la hauteur à laquelle on installera la caméra IP, et sa direction afin que le champ de vision de cette dernière corresponde aux besoins de l'entreprise. Nous avons mis en place les caméras de sorte à couvrir toute les zones à protéger.

3) Résultats de la simulation :

La simulation nous a permis d'avoir un aperçu du système de vidéosurveillance IP, mais aussi de déterminer le nombre exact de caméras dont l'entreprise ENIEM aura besoin pour répondre à ses besoins en termes de sécurité, en effet, il faudra au minimum 33 caméras afin de protéger efficacement l'infrastructure de l'ENIEM.

V. Schéma connectique du système :

Grâce à la simulation réalisée par le logiciel IP Vidéo Disgne Tool, nous avons pu déterminer le nombre de caméras et l'emplacement exact de chacune d'entres elles, et nous pouvons maintenant déterminer chaque connexion du système de vidéosurveillance avec le réseau informatique actuel de l'ENIEM, le schéma synoptique suivant représente ces connexions :

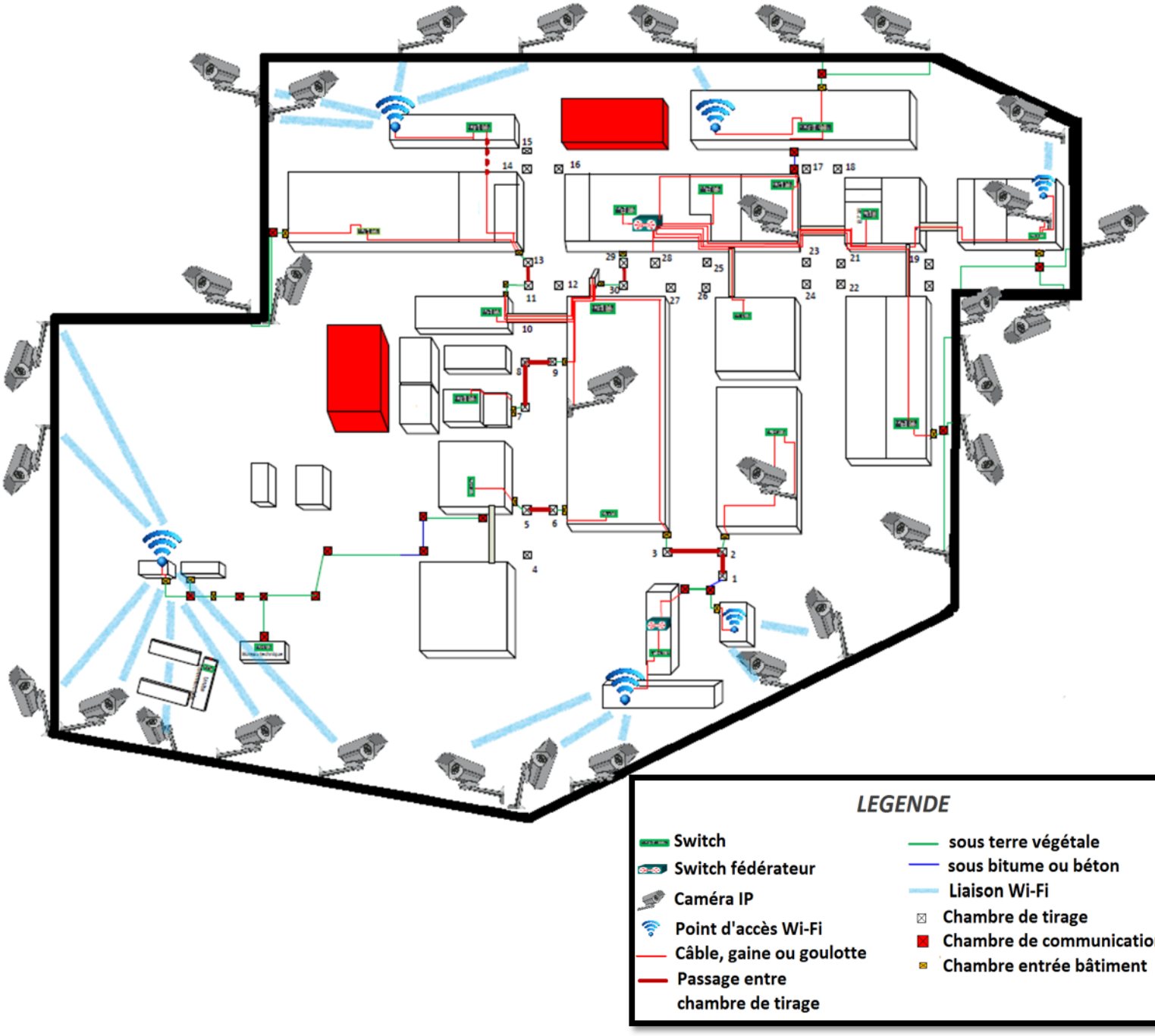

Figure 4.10 : Schéma connectique du système de vidéosurveillance IP.

Les caméras se trouvant à l'intérieur seront reliées aux Switch par des câbles à paires torsadées simplement fixées à un mur ou passant par une gaine. Par contre, les câbles reliant les caméras extérieures seront enterrées pour éviter les dégradations dues aux intempéries et au soleil.

Les chambres d'entrée des bâtiments servent à protéger la partie du câble (à paire torsadées ou fibre optique) se trouvant entre la sortie du bâtiment et le point où il traverse le sol, et les chambres de communications reliant les câbles souterrains entre eux. Dans les zones où les câbles souterrains traversent une longue distance, des chambres de tirage ont été mises en place afin de faciliter leurs manipulations et d'éviter que les câbles ne soient sectionnés pendant leur installation.

Les caméras se trouvant trop loin des Switch (distance supérieure à 100mètres) seront reliés par Wifi aux Switch grâce à des points d'accès. Les points d'accès seront installés en hauteur (sur les toits des bloques) afin de maximiser leurs performances, et ils seront reliés aux Switch par des câbles à paires torsadées.

VI. Calcul de la bande passante occupée par le système :

Une fois les caméras installées et le logiciel mis en marche, on doit s'assurer que le système de vidéosurveillance IP ne provoquera pas de latence. Pour cela, nous utiliserons le logiciel « IP Vidéo System Design Tool » qui a la capacité de nous fournir la bande passante qu'occupe une caméra IP en fonction de ces caractéristiques.

Le résultat pour les caméras que nous avons choisies est affiché sur la figure suivante :

Résolution	Compression	Taille de l'Image*,en KB	Images/Sec	Jours	Caméras	Bande Passante, Mbit/s	Espace de Stockage, GB	Ratio,kbit/s
1280x720 (HD)	H.264-10 (Haute qualité)	10	30	1	1	2,46	26,5	2458

Figure 4.11 : Débit occupé par une caméra réseau en fonction de ses caractéristiques.

Donc, chaque caméra réseau consomme en moyenne 2.46 Mbits/s de débit.

Grâce à cette donnée et en sachant que le débit moyen consommé par un PC est de 2 Mbits/s, et celui des téléphone IP est de 100 Kbits/s. Nous allons calculer la bande passante occupée par les lignes de transmission de chaque Switch concerné par le système de vidéosurveillance.

Il y a 10 Switch auxquels nous avons branché les caméras IP, ces derniers sont à leur tour branchés à 2 Switch fédérateurs par fibre optique, ils sont représentés par la figure suivante :

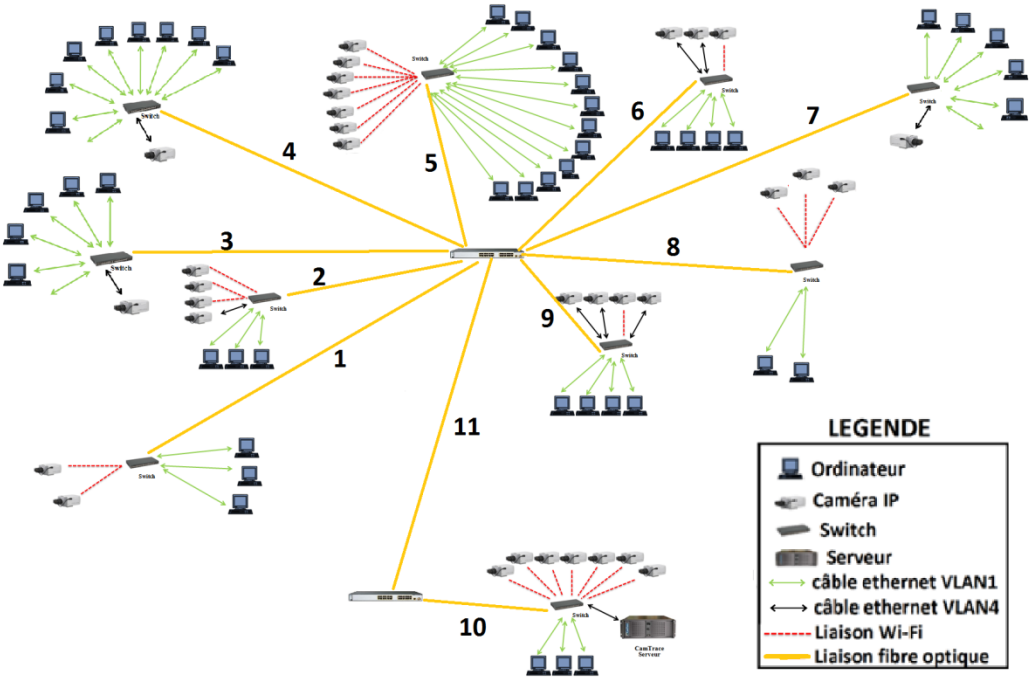

Figure 4.12 : Architecture du système de vidéosurveillance IP.

Nous allons calculer la bande passante occupée par le système de vidéosurveillance, ainsi que par les PCs sur chaque fibre optique :

La fibre optique n°1 : BP1= (2x2.46 Mbits/s) + (3x2 Mbits/s)= 10.92 Mbits/s

La fibre optique n°2 : BP2= (4x2.46 Mbits/s) + (3x2 Mbits/s)= 15.84 Mbits/s

La fibre optique n°3 : BP3= (2.46 Mbits/s) + (5x2 Mbits/s)= 12.46 Mbits/s

La fibre optique n°4 : BP4= (2.46 Mbits/s) + (8x2 Mbits/s)= 18.46 Mbits/s

La fibre optique n°5 : BP5= (7x2.46 Mbits/s) + (12x2 Mbits/s)= 41.22 Mbits/s

La fibre optique n°6 : BP6= (3x2.46 Mbits/s) + (4x2 Mbits/s)= 15.38 Mbits/s

La fibre optique n°7 : BP7= (2.46 Mbits/s) + (5x2 Mbits/s)= 12.46 Mbits/s

La fibre optique n°8 : BP8= (3x2.46 Mbits/s) + (2x2 Mbits/s)= 11.38 Mbits/s

La fibre optique n°9 : BP9= (4x2.46 Mbits/s) + (4x2 Mbits/s)= 17.84 Mbits/s

La fibre optique n°10 : BP10= (7x2.46 Mbits/s) + (3x2 Mbits/s)= 23.22 Mbits/s

La fibre optique n°11 :

BP11= BP1+BP2+BP3+BP4+BP5+BP6+BP7+BP8+BP9+BP10 = 179.18 Mbits/s

On rajoute à ce débit, les débits occupé par les 100 autres PC appartenant au réseau local de l'ENIEM ainsi que des 235 téléphones IP, nous trouvons que la bande passante totale occupée par la fibre optique n°11 est de :

200Mbits/s + 23.5 Mbits/s + 179.18 Mbits/s = 402.68 Mbits/s (dans le cas extrême où tous les appareils du réseau fonctionnent au même temps et utilisent tous la fibre optique n°11)

Nous concluons que le réseau de l'ENIEM, équipé du système de vidéosurveillance IP n'utilisera qu'au maximum 40.20% de la capacité totale de la fibre optique.

Remarque :

- Grâce au VLAN dédié à la vidéosurveillance, nous pouvons éliminer les collisions qui pourraient empêcher l'acheminement des paquets vers leurs destinations.
- Pour provoquer la saturation du réseau de l'ENIEM, il faudrait lui rajouter environ 226 caméras.
- Les calcules sont fait dans le cas où les Switch fédérateurs sont reliés entre eux avec une seule fibre optique, sachant qu'en pratique, les Switch sont reliés avec 2 fibres optiques, le débit est partagé entre les deux fibres.

VII. Discussion :

Dans ce chapitre, nous avons vu les étapes d'installation et de configuration d'un système de vidéosurveillance IP basé sur un serveur CamTrace. Après avoir fait une simulation, nous avons eu un aperçu du résultat, l'évolutivité de cette solution font d'elle la plus efficace et rentable pour sécuriser l'infrastructure de l'ENIEM.

Conclusion :

L’objectif de ce travail est de proposer une solution de vidéosurveillance sur un réseau informatique pour sécuriser l’infrastructure de l’usine de l’ENIEM.

Dans un premier temps, nous nous sommes intéressés à l’étude générale de la vidéosurveillance IP, des éléments qui la composent, des protocoles et des technologies nécessaires à son fonctionnement. Nous nous sommes ensuite focalisés sur le réseau informatique de l’ENIEM, en déterminant les besoins du réseau de l’entreprise, et les améliorations à faire dans le but d’optimiser le système de vidéosurveillance IP. Nous avons fini par montrer les étapes d’installation et de configuration des caméras IP, et réaliser une simulation pour déterminer le nombre et l’emplacement des caméras, puis nous avons procéder à des calculs afin de s’assurer de la fluidité du système.

Ce travail nous a permis de connaître tous les contours d'un système de vidéosurveillance, les paramètres qui interviennent dans la conception d'un système complet et sécurisé et aussi de voir des exemples de systèmes de vidéosurveillance utilisés de nos jours.

Au cours de notre stage pratique à l’ENIEM , nous avons pu acquérir l’expérience d’installation d’un réseau informatique haut débit, en participant à la configuration des Switch d’étages et des Switch fédérateurs, au soudage et au raccordement par fibre optique, et à la mise en place de câbles à paires torsadées. Nous n'avons pas rencontré de difficulté majeure et nous avons pu récolter un grand nombre d'informations. Nous espérons que notre étude pourra servir à l’ENIEM à des fins de réalisation du projet d'implémentation du système de vidéosurveillance IP.

Grâce à ce projet, l’entreprise ENIEM pourra sécuriser efficacement son infrastructure. Cependant, le système peut être optimisé en ajoutant une solution afin que les images puissent être visionnées à travers internet par Pc ou Smartphone.

Bibliographie et webographie :

[1] : **DOCTEUR Jean-Louis VERNEUIL** de L'UNIVERSITE DE LIMOGES, thèse de doctorat « Simulation de systèmes de Télécommunications par fibre optique à 40 Gbits/s », Le vendredi 21 novembre 2003, URL :
http://epublications.unilim.fr/theses/2003/verneuil-jean-louis/verneuil-jean-louis.pdf

[2] : **Armand Renaud Ngaamou Nana** de l'Institut supérieur des technologies et du design industriel du Cameroun, mémoire « Etude et mise en place d'un système de vidéosurveillance cas de l'immeuble Folep à Bali », le 02 septembre 2011, URL :

http://www.memoireonline.com/01/13/6765/Etude-et-mise-en-place-d-un-systeme-de-videosurveillance-Cas-de-l-immeuble-Folepe--Bali.html

[3] : **BOUBAKER Nobel El Houssine** directeur marketing de l'entreprise Topnet fournisseur de services Internet, « présentation de la technologie WIFI », en 2004, URL :

http://www.web-2-com.com/pdf/presentation-wifi.pdf

[4] : **Entreprise Cisco,** Fiche technique des Commutateurs Cisco Catalyst 3560/3750/2950/2960, en 2006, URL :

http://www.ofis-reseaux-telecoms.com/fiches/cisco/fiche-de-presentation-des-commutateurs-cisco-catalyst.pdf

[5] : **Sedjelmaci Amina Nadjet de l'Université Abou Bakr Belkaid– Tlemcen,** thèse de Magister en Systèmes et Réseaux de Télécommunication « Extension de la QoS du Wifi vers le WiMAX », année scolaire 2010-2011, URL :
http://dspace.univ-tlemcen.dz/bitstream/112/353/1/Memoire-finale%20Amina-apres-soutenance.pdf

[6] : **Journal L'Informaticien** article n°119 page : 70-73, titre « Blue Mind veut devenir l'alternative open source numéro 1 à Microsoft Exchange et Lotus Domino », paru en Décembre 2013, URL :

https://www.bluemind.net/wp-content/uploads/2016/07/l1nformaticien-BLUEMIND-201312.pdf

[8] : DOCTEUR Mohamed Said Seddiki à l'université de Lorraine, thèse de doctorat « Allocation dynamique des ressources et gestion de la qualité de service dans la vitalisation des réseaux »**,** le 14 Avril 2015, URL :
https://tel.archives-ouvertes.fr/tel-01242730/document

[9] : Entreprise **ANIXTER**, guide de vidéo surveillance IP, en 2012, URL : https://www.anixter.com/content/dam/Anixter/Guide/12H0012X00-Anixter-IP-Video-Surveillance-Guide-ECS-EN-US.pdf

[10] : Entreprise **PROXMOX,** VE ADMINISTRATION GUIDE, 3 mai 2017, URL : **https://pve.proxmox.com/pve-docs/pve-admin-guide.pdf**

[12] : Entreprise **Barco**, Description du Serveur de gestion et du contrôle des médias et des dispositifs, en 2017, URL :

https://www.barco.com/fr/Produits-et-solutions/Streaming-AV/Serveurs-de-gestion/Serveur-de-gestion-contr%C3%B4le-des-m%C3%A9dias-et-des-dispositifs.aspx

[13] : Michael LaLena fondateur du site Structured Home Wiring**,** « Types of Surveillance Cameras », URL :

https://www.structuredhomewiring.com/SurveillanceSystem/TypesOfSurveillanceCameras/

[14] : **Jean-François PILLOU** fondateur du site « CommentCaMarche.net », cour sur Le protocole FTP (File Transfer Protocol), 2017, URL : http://www.commentcamarche.net/contents/519-le-protocole-ftp-file-transfer-protocol

[16] : TAHRA Zahia de Université Kasdi Merbah -Ouargla, thèse d' 'ingénieur d'état en Informatique « Etude et simulation d'un réseau de téléphonie sur IP », juin 2008, URL : https://bu.univ-ouargla.dz/ingenieur/pdf/ing_tahra_zahia.pdf?idmemoire=963

[17] : **Stéphane DELECROIX** et **Mahmoud SKIFATI professeurs à l'**Université des Sciences et Technologie de Lille**,** cour « Les caméra infrarouge », en 2015, URL : http://www-iut.univ-lille1.fr/lp_vi/projets/soutenance_camera_infrarouge_09.pdf

[18] : Entreprise **AXIS communication**, Guide technique de la vidéo sur IP, en 2008, URL : https://www.axis.com/files/brochure/bc_techguide_60872_fr_1501_lo.pdf

[19] : **Sylvain MONTAGNY professeur à l'université Savoie Mont Blanc, cour «** introduction aux réseaux IP », année scolaire 2011/2012, URL : http://www.scem.univ-smb.fr/formations/masters/electronique-telecoms/wp-content/files/INFO-324/Cours/Cours-Initiation%20aux%20r%C3%A9seaux%20IP-internet.pdf

[20] : **Jean-François PILLOU** fondateur du site « CommentCaMarche.net », cour sur le TCP/IP, septembre 2015, URL : https://repo.zenk-security.com/Protocoles_reseaux_securisation/Le%20protocol%20TCP.pdf

[21] : **Rabha Bouzaida** de l'uiniversité virtuelle de Tunis, projet de fin d'étude **«** Etude et mise en place d'une solution VOIP sécurisée », année scolaire 2010-2011, URL : http://pf-mh.uvt.rnu.tn/620/1/%C3%89tude_et_Mise_en_place_d'une_Solution_VOIP_S%C3%A9curis%C3%A9e.pdf

[22] : Article de Wikipédia, l'encyclopédie libre, Secure Shell, en 2017, URL : https://fr.wikipedia.org/wiki/Secure_Shell

[23] : Professeur **Guillaume Burel** de l'université de Nancy, cour **«** Les serveurs », 2008-2009, URL : http://www.ensiie.fr/~guillaume.burel/download/Serveurs_cours1.pdf

[24] : Entreprise **CamTrace**, fiche technique « serveur de vidéosurveillance en réseau », Mai 2008, URL : http://www.activcam.com/adminzone/docs/camtrace/doc-camtrace-fr.pdf

[25] : Entreprise **CamTrace**, Manuel d'Installation NOVA 13, 24 décembre 2014, URL : http://www.camtrace.com/wp-content/medias/2015/02/Installation-7.13.x-18-12-2014.pdf

[26] : Entreprise **AXIS communication**, guide d'installation M1124 Network Camera, 2015, URL : https://www.axis.com/files/manuals/ig_m1124e_m1125e_1504114_en_1509.pdf

[27] : Entreprise **Vivotek**, Caméra réseau cube IP8336W, 2013, URL : http://download.vivotek.com/downloadfile/downloads/datasheets/ip8336wdatasheet_fr.pdf

[28] : **Jean-François L'haire** professeur à l'Université de Genève**,** cour sur la fibre optique**,** janvier 1999, URL : http://cvardon.fr/Fibre%20optique.pdf

Annexe A : Les réseaux informatiques

A.1 Définition :

Un réseau informatique est un ensemble de plusieurs équipements informatiques. Tel que, des PC, des téléphones IP et des imprimantes interconnectées entre eux grâce à un support physique qui peut être soit des câbles coaxiaux ,des câbles à paires torsadées , de la fibre optique ou des faisceaux hertziens.

A.2 Les différents types de réseaux :

On distingue un réseau d'un autre selon sa disposition géographique et selon le nombre d'éléments qui le constituent. Généralement on distingue trois types de réseaux :

- **Le réseau LAN** :

Les équipements appartiennent à une même enceinte, les ordinateurs sont situés sur un étendu géographique restreint, par exemple un bâtiment.

- **Le réseau métropolitain MAN :**

L'interconnexion de plusieurs réseaux LAN forme un réseau MAN, ce réseau est étendu à plusieurs dizaines de kilomètres.

- **Le réseau étendu WAN :**

L'interconnexion de plusieurs réseaux LAN et MAN forme un réseau WAN. Ce réseau a une couverture nationale (pays) ou à l'échelle internationale (continents). C'est le plus grand réseau au monde (internet).

A.3 Les topologies :

Une topologie est l'architecture ou l'arrangement physique des nœuds constituant le réseau. Il existe trois topologies de base pour former un réseau informatique.

a) Topologie en Bus :

Les ordinateurs sont tous reliés avec des câbles coaxiaux au même support de transmission qui est un bus (tronc physique).

Figure A.1 : Réseau informatique en bus.

b) Topologie en Anneau :

Les ordinateurs sont reliés entre eux avec des câbles coaxiaux, c'est une architecture qui utilise la technique d'accès par jeton. Les informations circulent d'une station à une autre suivant l'anneau dans un seul sens. Un jeton circule autour de l'anneau, et la station qui a le jeton peut émettre des données qui font le tour de l'anneau.

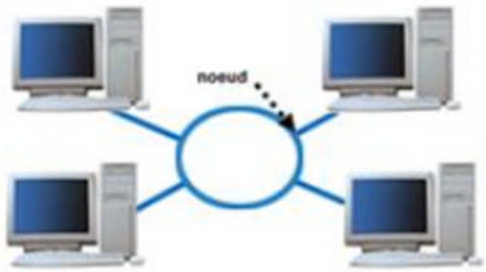

Figure A.2 : Réseau informatique en anneau

c) Topologie en Etoile :

C'est l'architecture qu'on va utiliser dans notre étude. Les ordinateurs sont reliés au point central qui peut être un concentrateur (hub) ou un commutateur (switch) avec des câbles à paires torsadés (RG45).

Figure A.3 : Réseau informatique en étoile

A.3 Différents éléments d'un réseau informatique

Un réseau informatique se compose de différents équipements ainsi que de supports de transmission.

- **Les serveurs :** un serveur est un matériel informatique qui fonctionne en permanence afin d'assurer des services au réseau et aux utilisateurs, il permet notamment de :
  - Gestion des protocoles.
  - Mise à disposition d'une gamme de logiciels d'applications.
  - Gestion des accès et authentification.
  - Stockage dans des bases de données.
  - Accéder aux informations d'internet.
  -
- **Les équipements informatiques** : On peut classer les équipements d'un réseau en deux groupes :

Afin d'interconnecter les différents équipements d'un réseau informatique et de faire transiter l'information d'un équipement à un autre, on utilise :

- **Un Hub :** appelé aussi concentrateur, c'est un équipement informatique qui sert à interconnecter physiquement plusieurs appareils et qui peut concentrer les transmissions de plusieurs équipements sur un même support .Il est très utilisé dans les réseaux locaux ayant la topologie en étoile.

- **Un Switch :** appelé aussi hub intelligent, il sert à interconnecter plusieurs équipements et il permet aussi de sélectionner l'acheminement des informations.

Les terminaux : A l'exemple des PC, téléphones IP et les imprimantes, c'est l'ensemble des équipements qui constitue la terminaison du réseau.

- **Les supports de transmissions :**

Le support de transmission est un moyen qui sert à acheminer l'information d'un matériel à un autre, on peut citer les câbles à paires torsadées (RG 45), la fibre optique, et les câbles coaxiaux mais aussi les ondes électromagnétiques (faisceaux hertziens).

Annexe B : La fibre optique

B.1 Présentation de la fibre optique : [28]

Une fibre optique est un fil en verre très fin, qui a la capacité de transporter la lumière sur de très longues distances. Elle est composée d'un cœur en verre (de l'ordre de quelques dizaines de micromètres), ce cœur est en suite recouvert par une autre couche de verre en silice appelée gaine.La différence entre le cœur et la gaine se résume par une différence de l'indice de réfraction, en effet, l'indice de réfraction de la gaine est inférieur à celui du cœur.

Cette fibre est ensuite protégée par un revêtement de protection en plastique, cette dernière permet à la lumière d'être emprisonnée à l'intérieur de la fibre.

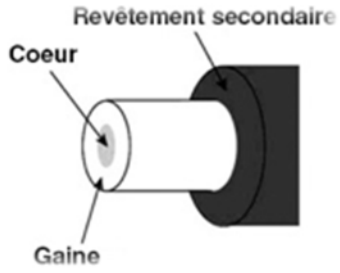

Figure A.4 : Composition de la fibre optique

B.2 Principe de propagation de la lumière sur fibre optique : [1]

La fibre optique est un guide d'onde, son cœur possède un indice de réfraction légèrement supérieur à celui de la gaine. Lorsqu'une lumière traverse la fibre, elle est constamment réfléchie à l'interface entre le cœur et la gaine grâce au principe de réflexion total interne.

En effet, quand un rayon traverse une surface plus au moins transparente, une partie de ce rayon est réfractée alors qu'une autre partie est réfléchie, tout dépend de l'angle avec lequel le rayon percute la surface de l'objet en question.

Afin de pouvoir trouver le meilleur angle pour une réflexion totale interne, des calculs sont faits en fonction de l'indice de réfraction du cœur et de la gaine comme suit :

$$\sin \emptyset = \sqrt{{n_c}^2 - {n_g}^2}$$

n_c : indice de réfraction du cœur

n_g : indice de réfraction de la gaine

$\emptyset$: bon angle du rayant lumineux

Lorsqu'un rayon lumineux est introduit avec le bon angle sur l'une des extrémités de la fibre optique, la lumière se propage en zigzagant sur les parois du cœur, et cela avec une atténuation quasi insignifiante. Cette faible atténuation permet à la lumière de voyager sur de très longues distances sans avoir de pertes d'informations même lorsque la fibre est courbée.

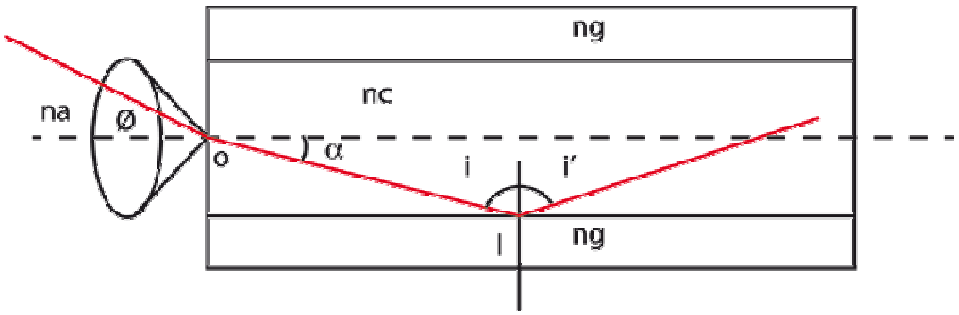

Figure A.5 : Réflexion totale interne d'un rayon lumineux

B.3 Types de fibres optiques : [28]

Les fibres optiques utilisées en télécommunication peuvent être classées en deux catégories, la fibre multimodale et la fibre monomodale.

Ces deux catégories différents par la taille de la fibre, par la longueur d'onde du rayant qu'elles transportent ainsi que du domaine d'utilisation. Elles ce présentent comme suite :

a) La fibre multimodale :

La fibre multimodale a un cœur supérieur à celui de la fibre monomode (entre 50 à 85 micromètres) elle est généralement utilisée pour de courtes distances, du fait de la dispersion modale qui atténue le signal lumineux et qui limite la distance de transmission.

Néanmoins, elle reste bien plus performante que les câbles à paires torsadées en termes de distance, avec une augmentation de la longueur d'onde ainsi que de la bande passante , on

peut atteindre quelques kilomètres alors que les câbles à paires torsadées sont limités à 100 mètres.

Elle est donc idéale pour les réseaux locaux et métropolitains, elle remplace de plus en plus les câbles à paires torsadées du fait de ses performances nettement supérieures , et de la distance de transmission offerte par celle ci.

Son mode de propagation de l'onde lumineuse se fait de deux façons, par saut d'indice ou bien par gradient d'indice, chacune possédant ses propres caractéristiques qui se résument comme suit :

Fibre optique multimodale à saut d'indice :

Possédant un cœur entre 62.5 à 80 micromètres, ce type de fibre est appelé ainsi car le cœur et la gaine présente deux indices de réfraction différents qui se joignent à l'interface, cela permet la réflexion de la lumière sur l'interface entre le cœur et la gaine grâce au principe de réfraction totale interne où la lumière se propage d'une extrémité à une autre.

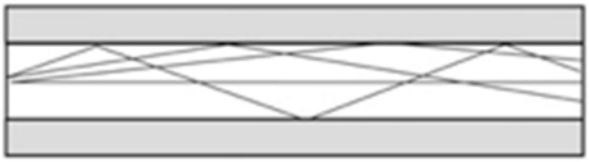

Figure A.6 : Propagation de la lumière sur une fibre optique multimodale à saut d'indice

Fibre optique multimodale à gradient d'indice :

Possédant un cœur d'environ 50 à 62.5 micromètres, ce type de fibre est appelée ainsi car l'indice de réfraction du cœur décroit en s'éloignant de l'axe optique de la fibre, cette caractéristique permet au rayon lumineux d'être constamment dévié vers l'axe, l'empêchant ainsi de s'échapper et permet son acheminement d'une extrémité à une autre.

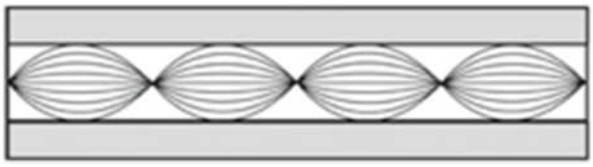

Figure A.7 : Propagation de la lumière sur une fibre multimodale à gradient d'indice

b) La fibre monomode :

La fibre monomode est une fibre très fine possédant un cœur d'une dimension très inférieure à la fibre multimodale, en effet son cœur ne mesure que 10 micromètres. Elle est généralement utilisée dans les réseaux structurants ou bien pour relier des réseaux locaux d'une distance très éloignée, et aussi pour satisfaire le besoin d'un très haut débit de transmission.

Du fait de son mode de propagation unique qui suit le chemin le plus direct possible (elle suit l'axe de la fibre), les réflexions dans l'interface sont rares, ce qui minimise les atténuations et les pertes. La fibre peut donc transmettre le signal lumineux sur de très longues distances (une centaine de kilomètres)

Figure A.8 : Propagation de la lumière sur une fibre monomode

B.4 Principe de transmission des données sur la fibre optique :

Les fibres optiques possèdent, dans la fenêtre spectrale généralement utilisée, une bande utilisable très importante (environ 15 THz autour de la longueur d'onde 1,55 μm).

Donc en théorie nous sommes en mesure d'atteindre des débits extrêmement élevés, d'autant que les besoins ne cessent de croitre. Néanmoins, nous sommes limités par la conversion des signaux électriques en signaux lumineux et vis versa à l'émission et à la réception qui eux, ne peuvent atteindre de telles fréquences.

a) La conversion électro-lumineuse :

La conversion d'un signal électrique en un signal lumineux est essentiel pour pouvoir utiliser la fibre optique comme support de transmission, il se fait par une diode électroluminescente. Cette diode permet de convertir tous les signaux électriques la traversant en onde lumineuse.

Pour pouvoir profiter des performances de la fibre optique, le multiplexage a été intégré en plus de la conversion électroluminescente ce qui permettra de transmettre plusieurs signaux sur une même fibre et d'augmenter le débit transporté sur cette ligne.

B) Le Multiplexage : [1]

Afin de conserver l'intégrité des signaux envoyés, on utilise trois types de multiplexage qui séparent les signaux aux niveaux temporels, spatials ou bien fréquentiels.

Le multiplexage temporel (TDM) :

Le multiplexage temporel (TDM) consiste à attribuer à un utilisateur la totalité de la bande passante pendant un court instant, chacun des utilisateurs y aura accès à tour de rôle pendant un intervalle de temps fixe (IT).

Le multiplexage (TDM) permet de séparer une ligne de très haut débit en plusieurs lignes de débit inferieur (le débit sera devisé par le nombre de lignes secondaires créées).

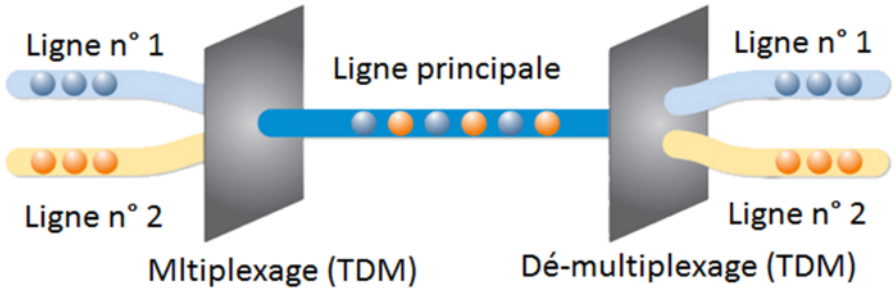

Figure A.9 : Schéma représentant un multiplexage temporel

Le multiplexage en longueur d'onde (WDM) :

Le multiplexage en longueur d'onde (WDM) consiste à transmettre sur une seule fibre plusieurs porteuses optiques avec des longueurs d'ondes différentes au même moment.

Ainsi plusieurs utilisateurs auront accès à la ligne de transmission simultanément, ce n'est plus le temps qu'ils devront se partager mais plutôt la bande passante de la fibre optique.

Ce multiplexage nécessite une diode électroluminescente capable d'émettre à des longueurs d'ondes différentes.

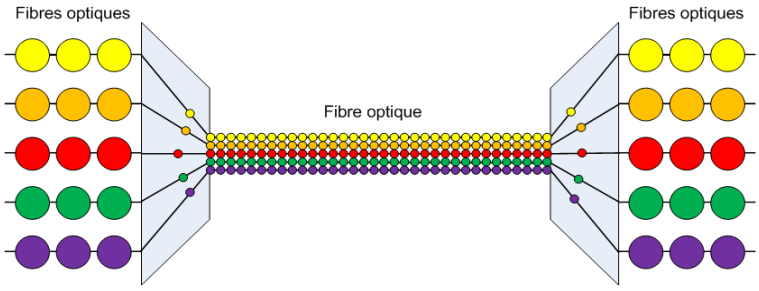

Figure A.10 : Schéma représentant un multiplexage en longueur d'onde

Remarque : Ce multiplexage s'apparente au multiplexage fréquentiel, en réalité c'est le même principe. La seule différence réside dans la marge qui sépare les longueurs d'ondes.

On appelle multiplexage fréquentiel quand la marge est minime et multiplexage en longueur d'onde quand elle est plus grande.

B.6 Transmission d'une donnée sur fibre optique :

Au départ (PC, Caméra, Téléphone IP…etc.) Nous avons un signal électrique, il sera dans un premier temps multiplexé, pour ensuite être converti en un signal lumineux grâce à la diode électroluminescente. Ce signal lumineux sera ensuite transporté à travers la fibre optique.Une fois arrivé à destination il sera reconverti en un signal électrique grâce au photo-détecteur.

Une fois ce signal reconverti, il sera démultiplexé afin de différencier la voie que prendra l'information envoyée.

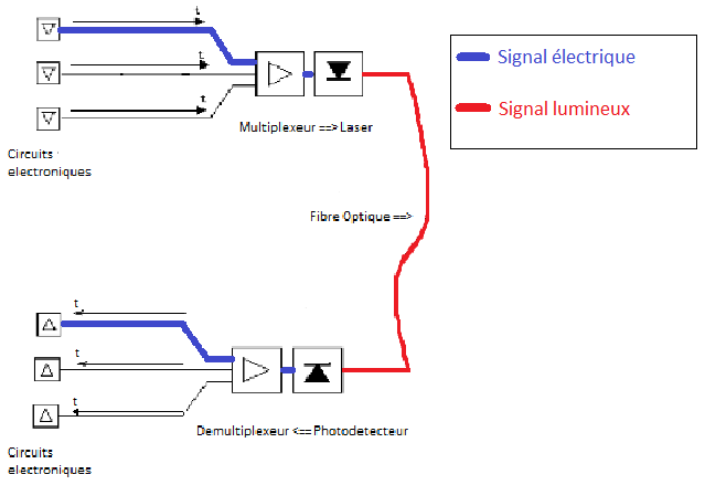

Figure A.11 : Exemple de transmission d'une donnée par fibre optique.

B.7 Protection :

La sécurisation par fibre optique Se fait en utilisant simultanément deux fibres optiques à demi-charge. Si l'une des fibres est défaillante, l'autre prendra en charge la totalité du flux le temps que la première soit réparée.

Dans le cas où le flux devient trop important, les deux fibres optiques sont utilisées à pleine charge afin que la bande passante soit augmentée.

La figure suivante montre le principe de protection :

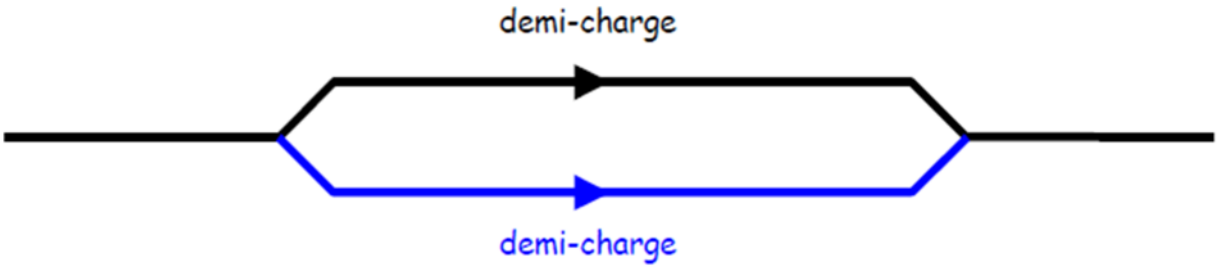

Figure A.12 : Utilisation simultanée de deux fibres optiques

B.8 Capacité de transmission de la fibre optique :

La fibre optique est connue pour être nettement supérieure aux câbles à paires torsadées, cela est dû à une énorme bande de fréquence qui permet d'avoir un très haut débit sur de longues distances.

La seule limite de la transmission par fibre optique réside dans les appareils utilisés autour d'elle. Elle est limitée en débit par le protocole Ethernet utilisé, et en distance par la bande passante choisie.

La capacité de transmission d'une fibre optique se calcule donc en fonction des autres composants du système de transmission, en fonction du protocole du réseau, de la longueur d'onde utilisée ainsi que de la fréquence de transmission.

Ce tableau résumera parfaitement les types de transmission et les capacités de chacune d'entre elles :

Type de liaison	Débit	Média	Distance
100Base FX	100 Mbps	f.o. MM OM1 1300 nm	2 km
100Base LX	100 Mbps	f.o. SM OM1 1300 nm	15 km
1000Base Sx	1 Gbps	f.o. MM OM2 850 nm	500 m
1000Base Lx	1 Gbps	f.o. MM OM1/OM2 850 nm	500 m
1000Base Lx	1 Gbps	f.o. SM 1310 nm	10 km
1000Base Zx	1 Gbps	f.o. SM 1550 nm	80 km
10GBase-SR/SW	10 Gbps	f.o. MM OM3 850 nm	300 m
10GBase-LR/SW	10 Gbps	f.o. SM 1310 nm	10-25 km
10GBase-ER/EW	10 Gbps	f.o. SM 1550 nm	40-80 km

Tableau B.1 : Capacités des fibres optiques en fonction de leurs caractéristiques.

Dans notre cas, on utilisera le protocole 1000base Sx, alors nous aurons accès à un débit de 1Ghz et d'une distance de transmission de 500 mètres par fibre. Des capacités nettement supérieures à celles des câbles à paires torsadées qui eux présentent un débit 10 fois inférieurs à celle de la fibre avec une distance limite de 100 mètres.

Annexe C : Le WIFI

Dans les réseaux locaux, la transmission par WIFI devient une solution avantageuse par rapport à celle avec des câbles à paires torsadées (Ethernet), nous allons la définir et l'étudier afin de comprendre son fonctionnement :

C.1 Présentation du WIFI : [5]

Le mot Wifi désigne une technologie réseau sans fil local WLAN conçue sur la base des travaux du groupe de travail IEEE 802.11. On peut concevoir le Wifi comme une extension naturelle du réseau LAN réussi « Ethernet » dans le monde sans fil. Les réseaux WLANs sont généralement déployés dans les entreprises comme le lien final qui lie les ordinateurs des clients au réseau local filaire de l'entreprise. On peut également les trouver dans les campus des universités et les espaces publiques comme les aéroports el les gares de train permettant aux utilisateurs anonymes d'accéder à internet ou autres réseaux publiques.

Il y a trois standards réseaux WLAN principaux, chacun avec un degré différent d'acceptation et de déploiement: IEEE 802.11a, IEEE 802.11b et IEEE 802.11g. Le standard 802.11b est le plus populaire, également connu sous le nom Wifi ou Ethernet sans fil. Actuellement, le terme Wifi est attribué à l'ensemble de la famille de norme IEEE 802.11a/b/g/n. Le Wifi fonctionne dans l'une des bandes de fréquences sans licence 2,4 GHz, 5 GHz avec une zone de couverture allant de 3 à 500m.

C.2 Architecture :

Un réseau qui utilise la norme IEEE 802.11 est un réseau informatique ordinaire, à la seule différence près qu'il est équipé d'un point d'accès branché au commutateur, ce dernier sert à envoyer des ondes électromagnétiques qui remplaceront les câbles à paires torsadées.

L'architecture d'un réseau WIFI est généralement en étoile tel que ce schéma nous le montre :

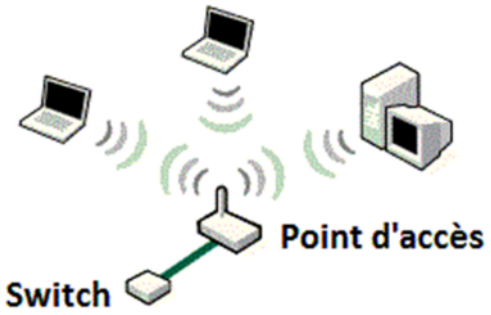

Figure A.13 : Architecture d'un réseau Wifi

C.3

Principe de transmission par ondes électromagnétique : [5]

Les paquets sont acheminés par des câbles à paires torsadées jusqu'au point d'accès, chaque bits est ensuite converti en onde électromagnétique par le couplage des deux champs, le champ électrique (E) et le champ magnétique (B). La fréquence de l'onde WIFI détermine sa portée maximale, elle voyage à travers l'air jusqu'à arriver à l'antenne de l'appareil récepteur, ce dernier convertira l'onde WIFI en un courant électrique, qui sera à son tour converti en données numériques pour reconstituer les paquets.

Annexe D : Modèle TCP/IP

Le modèle TCP/IP est constitué de 4 couches comme ce schéma ci-dessous l'indique :

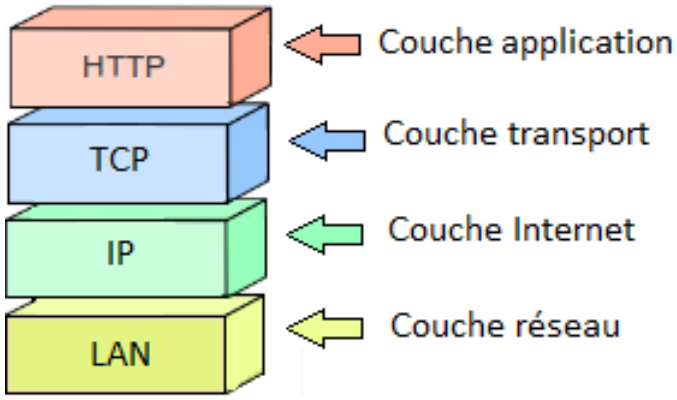

Figure A.14 : Les couches du modèle TCP/IP

1- Couche application :

Elle se situe au sommet des couche du TCP/IP, et elle met à disposition toutes les applications nécessaires afin de mettre en place une communication grâce à la couche transport, et des applications utilitaires afin d'assurer une interface avec le système d'exploitation.

Les différentes applications gérées par le protocole TCP/IP sont :

- Le protocole http une fois qu'il a accès à une page web, il utilise le TCP/IP afin d'envoyer et de recevoir des fichiers HTLM.
- Le protocole FTP qui utilise le TCP/IP pour envoyer et recevoir des fichiers.
- Le protocole DNS qui sert à convertir un nom en adresse IP et qui lui aussi utilise le TCP/IP selon les besoins.

2- Couche transport :

La couche transport permet à des machines distantes de communiquer entre elles indépendamment des autres couches, elle se fait grâce à deux protocoles :

- TCP qui est orienté connexion, c'est-à-dire qu'il assure le contrôle des erreurs.
- UDP qui lui est non orienté connexion, et qui n'assure pas le contrôle aux erreurs.

Le plus utilisé des deux est le TCP en grande partie grâce au contrôle des erreurs, c'est d'ailleurs pour cela que le nom du protocole contient le mot « TCP ».

La couche transport contient des informations sur les ports où transite les données de l'expéditeur jusqu'au destinataire.

3- Couche internet :

C'est la couche qui permet l'acheminement des paquets jusqu'au destinataire en gérant l'adressage des paquets, elle permet aussi la fragmentation et le réassemblage des paquets à la réception.

La couche internet contient l'adresse IP de l'expéditeur ainsi que l'adresse IP du destinataire.

4- Couche réseau :

Grâce à la couche réseau, la machine aura un accès à un réseau physique afin de transmettre des données, elle gère aussi la synchronisation, la conversion analogique/numérique, le contrôle des erreurs, ainsi que le format des données transmises.

La couche réseau contient toute les spécifications de tous les types de liaisons vers un réseau de communication (lignes téléphoniques, transmissions en anneaux, Ethernet, Token-ring,Wi-Fi…etc).

Annexe E : Les réseaux locaux virtuels (VLAN) [8]

Un VLAN permet le regroupement de plusieurs hôtes, de façon logique et non physique indépendamment de leur connectivité physique [Pillou and Lemainque, 2012]. Il permet de créer des domaines de diffusion gérés logiquement sans se soucier de l'emplacement de ces hôtes.

Plusieurs VLAN peuvent coexister sur un même commutateur réseau et ils peuvent être locaux à un commutateur ou s'étendre sur un ensemble de commutateurs reliés entre eux. L'objectif est de contourner les limitations de l'architecture physique. Ceci conduit à l'amélioration de la gestion du réseau et de l'optimisation de la bande passante tout en séparant les flux de chaque ensemble d'hôtes. Chaque trame possède un identifiant du VLAN dans l'entête de contrôle d'accès au support (Media Access Control, (MAC)).

Les réseaux locaux virtuels fonctionnent au niveau des couches liaison de données et réseau du modèle OSI. Ils sont définis par le standard IEEE 802.1Q.

La figure 2.4 illustre le regroupement de plusieurs PCs en VLAN indépendamment de leur connectivité physique.

Annexes

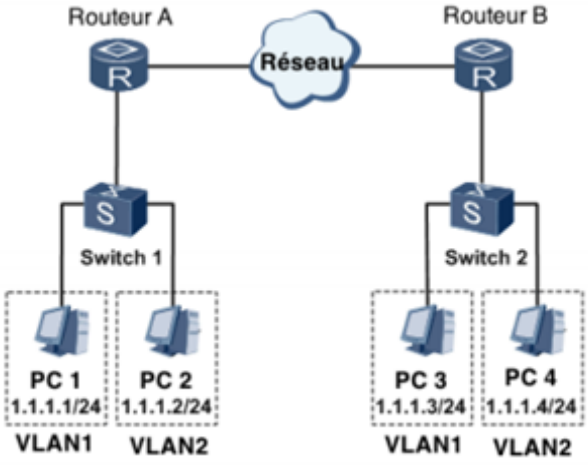

Figure A.15 : Regroupement des PCs en VLAN

On distingue trois types de VLAN [Rajaravivarma, 1997] :

— VLAN de niveau 1 ou VLAN par port (Port-Based VLAN) Il définit un réseau virtuel en fonction des ports de raccordement au commutateur. On associe un port physique de ce commutateur à un numéro de VLAN.

— VLAN de niveau 2 ou VLAN MAC (MAC Address-Based VLAN) Il définit un réseau virtuel en fonction des adresses MAC des hôtes. Le déploiement de ce type de VLAN est plus souple que le VLAN de niveau 1 puisque la machine, peu importe le port sur lequel elle sera connectée, elle fera toujours partie du VLAN dans lequel son adresse MAC est configurée.

— VLAN de niveau 3 On distingue deux types de VLAN de niveau 3.

— VLAN par sous-réseau (Network Address-Based VLAN) Il a le même principe que pour les VLAN de niveau 2 mais en indiquant les adresses IP source des datagrammes et en associant des sous-réseaux à différents VLAN. Ceci permet de modifier automatiquement la configuration des commutateurs lors d'un changement ou d'un déplacement de l'hôte.

— VLAN par protocole (Protocol-Based VLAN) Il définit un réseau virtuel en fonction des protocoles. Par exemple, il définit un VLAN pour TCP/IP. Dans ce cas, toutes les hôtes, qui utilisent ce protocole dans un même VLAN, sont regroupées

Anexxe F : Fiche technique de la caméra AXIS [26]

Caméra	
Capteur	Capteur CMOS RVB à balayage progressif 1/2.8"
Objectif	Objectif à foyer progressif, correction infrarouge, monture CS, résolution mégapixel, diaphragme DC, 3-10,5 mm, vue 91–32° [a], vue 49–18°[b]
Jour et nuit	Filtre infrarouge à retrait automatique
Éclairage minimum	Couleur : 0,25 lux F1.4 Noir et blanc : 0,05 lux F1.4
Durée d'obturation	1/143 000 à 2 s
Vidéo	
Compression vidéo	H.264 Profil de base, profil principal et profil avancé (MPEG-4 Part 10/AVC) Motion JPEG
Résolutions	1 280 x 720 à 160 x 90
Fréquence d'image	H.264 : Jusqu'à 25/30 ips dans toutes les résolutions Motion JPEG : Jusqu'à 25/30 ips dans toutes les résolutions
Flux vidéo	Flux multiples, configurables individuellement en H.264 et Motion JPEG Technologie Zipstream d'Axis e H.264 Fréquence d'images et bande passante contrôlables, VBR/CBR H.264
Réglages de l'image	WDR-Forensic Capture : Jusqu'à 120 dB selon la scène, réglage manuel de la vitesse d'obturation, compression, couleur, luminosité, netteté, contraste, balance des blancs, contrôle d'exposition (y compris contrôle du gain automatique), zones d'exposition, réglage de précision du comportement en faible éclairage, rotation : 0 °, 90 °, 180 °, 270 ° incluant le format Corridor, correction des rapports, texte et images en surimpression, masque de confidentialité, duplication des images
Panoramique/inclinaison/zoom	PTZ numérique
Réseau	
Sécurité	Protection par mot de passe, filtrage d'adresses IP, cryptage HTTPS[c], cryptage, contrôle d'accès réseau IEEE 802.1X[c], authentification Digest, journal d'accès utilisateurs
Protocoles pris en charge	IPv4/v6, HTTP, HTTPS[c], SSL/TLS[c], QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH
Intégration système	
Interface de programmation	API ouverte pour l'intégration logicielle, avec VAPIX® et plate-forme d'applications pour caméras AXIS ; caractéristiques disponibles sur *www.axis.com* Système d'hébergement vidéo AXIS (AVHS) avec connexion en un seul clic. ONVIF, Profil S. Caractéristiques disponibles sur *www.onvif.org*
Vidéo intelligente	Détection de mouvement vidéo, alarme de détérioration, détection audio, prise en charge la plate-forme d'applications pour caméras AXIS permettant l'installation d'AXIS Video Motion Detection 3, d'AXIS Cross-lineDetection, d'AXIS Digital Autotracking et d'applications tierces (visitez le site *www.axis.com/acap*)
Déclencheurs d'événements	Outils d'analyse, événements de stockage Edge, entrée externe
Actions sur événement	Téléchargement de fichiers : FTP, HTTP, HTTPS, SFTP, réseau partagé et e-mail Notification : e-mail, HTTP, HTTPS, TCP et trap SNMP Enregistrement vidéo vers une mémoire Edge Mémorisation d'images pré/post-alarme PTZ préréglé, tour de garde Envoi de clip vidéo Mode de vision jour/nuit Mode WDR Voyant d'état Port de sortie
Flux de données	Données d'événements
Ressources intégrées d'aide à l'installation	Compteur de pixels
Général	
Boîtier	Mélange polycarbonate Couleur : blanc NCS S 1002-B et noir Axis NCS S9000-N
Mémoire	RAM 512 Mo, mémoire flash 256 Mo
Alimentation	8-28 V CC ou alimentation par Ethernet (PoE) IEEE 802.3af Classe 2, max. 5,0 W, type 3,6 W
Connecteurs	RJ45 10BASE-T/100BASE-TX PoE Bloc terminal pour une entrée et une sortie (sortie 12 V CC, charge max. 15 mA) Entrée CC, bloc terminal
Stockage Edge	Compatible avec les cartes microSD/microSDHC/microSDXC Prise en charge de l'enregistrement dans un espace de stockage réseau (NAS) Pour obtenir des conseils sur la carte SD et le NAS, rendez-vous sur *www.axis.com*
Conditions d'utilisation	De -20 °C à 50 °C (-4 °F à 122 °F) Humidité relative de 10 à 85 % (sans condensation)
Homologations	EN 55022 Classe A, EN 61000-6-1, EN 61000-3-2, EN 61000-3-3, EN 61000-6-2, EN 55024, EN 50121-4, FCC Partie 15, sous-partie B Classe A, ICES-003 Classe A, VCCI Classe A, C-tick AS/NZS CISPR 22 Classe A, KCC KN22 Classe A, KN24, EN 50581, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14, IEC 60068-2-30, IEC 60068-2-78 IEC/EN/UL 60950-1, IEC 60721-4-3 Class 3M4
Dimensions	44 x 70 x 148 mm (1,7 x 2,8 x 5,8 po)
Poids	Boîtier seul : 160 g (0,35 lb) Avec optique : 200 g (0,45 lb)
Accessoires fournis	Support AXIS T91A11 blanc, Guide d'installation, 1 licence utilisateur décodeur Windows
Accessoires en option	Supports de caméra AXIS T91A04/T91A05, fixation télescopique au plafond AXIS T91A50, boîtiers série AXIS T92E20 et T93F, adaptateur secteur, connecteur pour terminal PS-P, AXIS T8006 PS12, illuminateurs AXIS T90B
Logiciel de gestion vidéo	AXIS Camera Companion, AXIS Camera Station, logiciel de gestion vidéo des Partenaires de développement d'applications d'Axis disponibles sur *www.axis.com/techsup/software*

Tableau F.1 : Fiche technique de la caméra AXIS

Annexe G : Fiche technique de la caméra Vivotek IP8336W [27]

Modèle	IP8336W
Informations système	
CPU	SoC Multimedia (System-on-Chip)
Flash	16 Mo
RAM	128 Mo
Caractéristiques	
Capteur d'image	CMOS Progressive 1/4"
Résolution maximale	1280x800
Type d'objectif	Focale fixe
Focale	f = 3,6 mm
Ouverture	F1.8
Champ de vision	56° (horizontal) 41° (vertical) 71° (diagonal)
Vitesse d'obturation	1/5 s. à 1/32 000 s.
Jour/Nuit	Filtre IR rétractable pour la fonction Jour & Nuit
Illumination minimum	0,47 Lux, 50 IRE (Couleur) 0,001 Lux, 50 IRE (N/B)
Fonctionnalités Pan/Tilt/Zoom	ePTZ: Zoom numérique 16x (4x sur plug-in IE, 4x intégré)
Illuminateurs IR	Projecteurs IR intégrés, efficaces jusqu'à 5 mètres LED IR *6
Stockage embarqué	Logement pour carte MicroSD/SDHC
Vidéo	
Compression	H.264, MJPEG & MPEG-4
Images par seconde	H.264: 30 ips à 1280x800 MPEG-4: 30 ips à 1280x800 MJPEG: 30 ips à 1280x800
Flux Vidéos	2 flux simultanés
Rapport S/B	Au-dessus de 38 dB
Flux Vidéo	Résolution, qualité et débit réglables Rognage vidéo pour économiser la bande passante
Paramètres image	Taille, qualité et débit réglables Horodatage, Incrustation de texte, Retournement et miroir Luminosité, contraste, saturation, netteté, balance des blancs, exposition, gain, compensation de rétroéclairage, masquage de confidentialité configurables Paramètres de profils planifiés
Audio	
Capacité audio	Entrée audio
Compression	G.711
Interface	Microphone intégré
Portée	5 mètres
Réseau	
Utilisateurs	Visionnage en direct pour un maximum de 10 clients
Protocoles	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, SNMP
Interface	802.11b/g/n WLAN
ONVIF	Pris en charge, spécifications disponibles à www.onvif.org
Vidéo intelligente	
Détection de mouvement	Triple-fenêtre de détection de mouvement
Alarmes et événements	
Déclenchement Alarme	Détection de mouvement, déclenchement manuel, entrée contact sec, déclenchement sur calendrier, démarrage du système, notification d'enregistrement, détection du sabotage de la caméra
Événements suite alarme	La notification des événements utilise la sortie numérique, HTTP, SMTP, FTP et un serveur NAS Téléchargement de fichiers via HTTP, SMTP, FTP et serveur NAS
Général	
Connecteurs	Entrée d'alimentation CC 12V Entrée numérique* 1
Indicateur LED	Alimentation du système et indicateur du statut
Alimentation	12V DC
Consommation d'énergie	Max. 3,4W
Dimensions	62 mm (P) x 88 mm (l) x 85 mm (H)
Poids	Net: 505 g
Caisson	Boîtier conforme IP66 résistant aux intempéries
Certifications	CE, LVD, FCC Class B, VCCI, C-Tick
Température de fonctionnement	-20°C ~ 45°C (-4°F ~ 113°F)
Garantie	24 mois
Configuration requise	
Système d'exploitation	Microsoft Windows 7/Vista/XP/2000
Navigateur Web	Mozilla Firefox 7 à 10 (Uniquement en streaming) Internet Explorer 7.x ou 8.x
Autres lecteurs	VLC: 1.1.11 ou supérieur QuickTime: 7 ou supérieur
Accessoires inclus	
CD	Manuel d'utilisation, guide d'installation rapide, assistant d'installation 2 (IW2), logiciel d'enregistrement 32 canaux ST7501
Autres	Guide d'installation rapide, carte de garantie, antenne, CD de logiciels, support de caméra

Tableau G.1 : Fiche technique de la caméra Vivotek IP8336W

Mots clés :

Vidéosurveillance

Réseau

Caméra

Fibre optique

VLAN (Virtual Local Area Network)

Sécurité

Résumé :

Notre travail s'est basé sur l'étude et la mise en place d'un système de vidéosurveillance IP à l'ENIEM .Dans ce travail nous avons étudié le réseau informatique de l'ENIEM, nous avons fait une étude et une simulation sur la mise en place des cameras réseaux et nous avons fait des calculs pour prouver que le système de vidéosurveillance ne provoquera pas de saturation.