REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

Présenté en vue de l'obtention
du diplôme de Master II académique en Électronique

Option : Réseaux et Télécommunication

Thème:

Etude d'un système de vidéosurveillance sur IP

Proposé et dirigé par: **Etudié et réalisé par:**

Mr: BERCHICHE Said

Mr: MAKHLOUF Mourad
Mr: SOULALI Takfarines

Année universitaire **2011/2012**

Remerciements

Nous tenons à exprimer nos vifs remerciements à notre promoteur : Mr BERCHICHE enseignant à l'université MOULOD Mammeri de TIZI OUZOU pour l'aide déterminante qu'il nous a accordée et pour l'intérêt qu'il nous a porté à notre projet. Qu'il trouve ici l'expression de notre profond respect.

Nous ne manquerons pas d'exprimer notre grande reconnaissance à tous les enseignants de Département électronique et tous les membres du jury pour avoir accepté de juger ce travail.

Dédicaces

Je dédie ce travail

A mes chers parents, mes grands parents, mes chers frères, mes chères Sœurs et à toute ma Famille ;

A tous mes amis ;

A toute la promotion Master II 2011/2012 ;

A mon binôme Takfarines ;

A tous ceux qui m'ont aidé durant ma vie universitaire.

Mourad

A *mes parents, ma grande mère, mon oncle et sa famille,*

Et ***A****mon grand père que Dieu le tout-puissant accorde sa Sainte Miséricorde et l'accueille en son Vaste Paradis.*

P*our l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance.*

E*t pour leurs patiences et leurs sacrifices.*

A *mes cheres cousines : Baya, Messad ;*

A *mes chères sœurs : katila, fariza, kahina, farida ;*

A *mes fréres : Missipsa, Sofiane et sa femme, Kousseila, Farid ;*

A *tous mes proches*

A *tous ceux qui m'aiment ;*

A *tous mes collègues : SAMIR, Rachid, Krimou, Adel,Sofiane, Amar…… ;*

A *tous ceux que j'aime ;*

A mon binôme Mourad

Je dédie ce mémoire.

SOULALI Takfarines

Résumé

L'évolution dans le domaine des télécommunications ne cesse de donner une grande souplesse pour trouver des solutions efficaces pour certains dangers et pour fournir une sécurité à distance des biens et des personnes. En effet, la combinaison entre les technologies IP et vidéo a permis de fournir une solution sécuritaire de vidéosurveillance sur IP. Cette solution assure, d'une manière efficace, la protection des biens et des personnes n'importe où dans le monde.

Ce projet propose de développer un logiciel de vidéosurveillance sur IP. Ce système de vidéosurveillance permet d'effectuer la visualisation en direct, la configuration à distance et l'enregistrement vidéo des caméras IP installées sur des sites éloignés. Il assure, également, la notification des utilisateurs en cas d'intrusion ou d'anomalie ainsi que d'autres traitements intelligents et de gestion des données relatives au système.

Ainsi, ce rapport s'articule sur trois chapitres : dans le premier, nous avons exposé les fondements de la vidéosurveillance sur IP en présentant les entités communes des systèmes de vidéosurveillance sur IP. Dans le deuxième, nous avons élaboré l'étude de notre système de vidéosurveillance.

Dans le troisième, nous avons présenté le développement de l'application, et le logiciel réalisé.

Mots clés

Vidéosurveillance, Caméra IP, MPEG-4, RTSP, UML, SQL, C#.

SOMMAIRE

Chapitre 2: Etude du système de vidéosurveillance sur IP

Chapitre 3: Mise en œuvre des fonctionnalités d'affichage et d'alerte du système de vidéosurveillance sur IP

Liste des figures

Chapitre 1: Fondements de la vidéosurveillance sur IP

Chapitre 2: Etude du système de vidéosurveillance sur IP

Chapitre 3: Mise en œuvre des fonctionnalités d'affichage et d'alerte du système de vidéosurveillance sur IP

Liste des abréviations

B

BIFS	Binary Format for Scene

C

CATV	Cable TV
CD	Compact Disc
CIF	Common Intermediate Format

D

DBV	Digital Broadcast Video
DVD	Digital Versatile Disc

F

FTP	File Transfer Protocol

G

GIF	Graphics Interchange Format
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications

H

HDTV	High-definition television
HTTP	Hyper Text Transfer Protocol

I

IETF	Internet Engineering Task Force
IP	Internet Protocol

ISM	Interactive Storage Media

J

JPEG	Joint Photographic Experts Group

L

MPEG-4	Moving Picture Experts Group
MO	Media Objects
MCU	Multipoint Conference Unit

H

NTSC	National Television System Committee

O

OSI	Open System Interconnection

P

PC	Personal Computer
PTZ	Pan Tilt Zoom
PAL	Phase Alternation Line

Q

QoS	Quality of Service

R

RTP	Real Time Transport Protocol
RTCP	Real Time Transfer Control Protocol
RTSP	Real Time Streaming Protocol
RFC	Request for Comments

RTSP	Real Time Streaming Protocol

S

SSL	Secure Sockets Layer
SDP	Session Description Protocol
SMS	Short Message Service
SQL	Structure Query Language
SGBD	Système de Gestion de Base de Données
SMTP	Simple Mail Transfer Protocol

T

TCP	Transmission Control Protocol

U

UDP	User Datagram Protocol
UML	Unified Modeling Language

V

VHS	Video Home System
VRML	Virtual Reality Modeling Language
VOD	Video on Demand
VC	Visio Conference

W

WAN Wide Area Network

Introduction générale

Introduction Générale

Ces dernières années ont été caractérisées par une évolution importante du marché des technologies de l'information et des télécommunications. En effet, les réseaux IP ont subi une grande évolution en termes d'utilisation, de capacité et de qualité de service. Egalement, les systèmes de compression vidéo et d'imagerie numérique ont marqué une croissance intéressante par l'apparition des caméras IP intelligentes. Ces deux technologies ont permis de répondre aux besoins de visualisation et de contrôle à distance à travers la technique vidéo sur IP.

La vidéo sur IP offre non seulement toutes les possibilités de la vidéo analogique, mais aussi un ensemble de fonctions et d'options nouvelles utilisées dans les technologies numériques.

A travers ces évolutions technologiques, la notion de sécurité occupe une place importante pour la protection des personnes, des biens et des patrimoines individuels et collectifs. Ainsi, la problématique est de trouver des solutions qui permettent de répondre aux exigences de la sécurité à moindre coût.

Ce besoin croissant de protection conjugué aux avantages offerts de la vidéo sur IP est à l'origine de l'émergence de la solution sécuritaire de la vidéosurveillance sur IP. La vidéosurveillance sur IP représente une nouvelle application de la vidéo numérique et du protocole IP. Elle constitue un moyen de vigilance et de contrôle distant qui permet de dissuader les actes de malveillance et de renforcer le sentiment de sécurité.

Dans le cadre de notre projet, nous allons étudier les aspects liés à la technologie vidéo sur IP en matière de sécurité. En effet, il s'agit de développer un logiciel qui permet d'effectuer la surveillance, le contrôle distant de plusieurs sites éloignés, la notification des utilisateurs ainsi que d'autres traitements intelligents.

Chaque caméra IP génère des flux vidéo composés d'images numérisées, transférés à travers un réseau informatique. Tout ordinateur connecté au réseau Internet et qui dispose du logiciel de vidéosurveillance sur IP peut visualiser ces images à distance.

C'est le principe de base de notre système de vidéosurveillance qui se caractérise, d'une part, par des applications diverses à grande échelle grâce au protocole IP le plus utilisé actuellement dans le domaine des réseaux. D'autre part, cette solution offre une

flexibilité d'utilisation dans plusieurs applications telles que la surveillance des maisons en absence de leurs propriétaires, des entrepôts, des entreprises, des banques, etc.

Le système de vidéosurveillance que nous proposons d'étudier doit répondre aux critères de fiabilité d'une part, et d'efficacité du contrôle distant d'autre part.

Notre travail est structuré en trois chapitres. Dans le premier, nous allons étudier les généralités sur les fondements de la vidéosurveillance sur IP.

Le deuxième chapitre est consacré au volet de réalisation de la solution à travers une spécification des besoins et des caractéristiques du système proposé suivi par une étude du système selon le modèle UML. Dans le troisième chapitre, nous présenterons un deuxième volet consacré a la partie développement logiciel. En effet, ce chapitre débute par une présentation du langage choisi et les résultats de notre contribution sont également exposés. Enfin, nous terminerons notre travail par une conclusion générale.

Chapitre 1

Fondements de la vidéosurveillance sur IP

1.1. Introduction

De nos jours, la vidéosurveillance sur IP est omniprésente et on la retrouve dans de nombreux secteurs d'activité (banque, transports, industrie, grande distribution, etc.) ou lieux de vie (villes, immeubles de bureaux, équipements collectifs, etc.), dans le but de surveiller et de protéger des personnes et des biens. Dans ce chapitre, nous allons examiner les composants essentiels d'un système de vidéosurveillance sur IP : la caméra réseau, les protocoles de transport de données pour la vidéo sur IP, les techniques de compression vidéo et la manière d'interaction entre les différents éléments d'un système.

1.2. Architecture d'un système de vidéosurveillance sur IP

1.2.1. Présentation de la vidéosurveillance sur IP

La vidéo sur IP – souvent appelée IP-Surveillance dans le cadre d'applications spécifiques de vidéosurveillance, de sécurité et de contrôle distant – est un système permettant à ses utilisateurs de visualiser et d'enregistrer des images vidéo via un réseau IP (LAN/WAN/Internet).

À la différence des systèmes analogiques, la vidéo sur IP utilise le réseau informatique plutôt qu'un système de câblage point-à-point pour transmettre les informations. Le terme vidéo sur IP englobe à la fois les sources vidéo et audio véhiculées par le système. Dans une application de vidéo sur IP, les flux d'images vidéo numériques peuvent être transférés n'importe où dans le monde via un réseau IP câblé ou sans fil, permettant une visualisation et un enregistrement vidéo en tout point du réseau [1].

La première étape d'un tel processus consiste à capter le contenu vidéo qui sera traité, compressé, stocké et édité sur un serveur vidéo. Ces transmissions sont ensuite adressées à un ou plusieurs postes pour être visionnées en différé ou en simultané.

L'architecture type d'un système de vidéosurveillance sur IP est traitée dans la section suivante.

1.2.2. Architecture du système de vidéosurveillance sur IP

La figure 1.1 décrit un exemple de configuration type d'un système de vidéosurveillance sur IP.

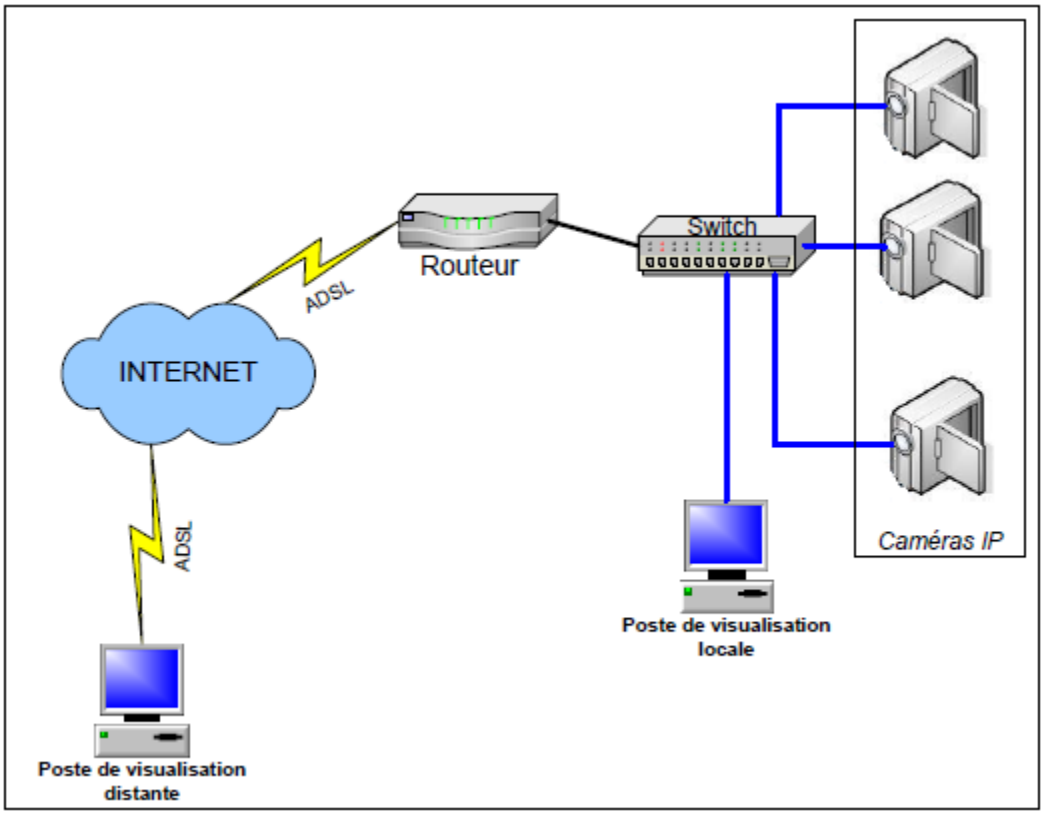

Figure 1.1 : Architecture type d'un système de vidéosurveillance sur IP

Un système de vidéosurveillance sur IP est composé des caméras IP pour la capture des séquences vidéo, des postes de visualisation et de traitement des opérations de vidéosurveillance via un logiciel dédié. Les caméras peuvent être

accessibles soit localement, via un réseau local, soit à distance via la technologie IP.

Chaque caméra fournit un flux vidéo composés d'images numérisées, compressé selon un format déterminé. La transmission de ces flux via le réseau IP suit un protocole de streaming vidéo compréhensible par les postes de visualisation. A la réception, ces flux peuvent être soit visualisés en temps réel ou bien stockés sur disque dur pour une utilisation ultérieure.

La chaîne complète d'un système de vidéosurveillance sur IP peut être simplifiée par la représentation de la figure 1.2.

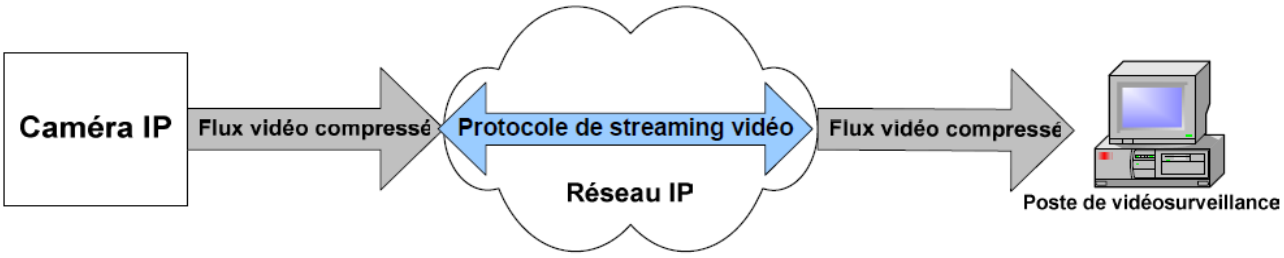

Figure 1.2 : Schéma synoptique du système de vidéosurveillance sur IP

Dans ce qui suit, nous allons étudier de prés la technologie des caméras IP, les techniques de compression vidéo et les protocoles de streaming vidéo.

1.3. Caméras vidéo sur IP

1.3.1. Présentation

Une caméra réseau ou IP est une caméra qui se connecte directement au réseau (et non pas à un PC), elle possède sa propre adresse IP. La caméra réseau réunit les fonctions optiques d'une caméra et la capacité d'un petit ordinateur équipé d'un serveur web interne.

Une caméra réseau possède donc une prise RJ45 pour connexion directe sur un hub ou un Switch. Cette caméra diffuse ses images à tout poste qui en fait la demande via un navigateur sur le réseau IP.

1.3.2. Principe de base

- Une caméra IP diffère d'une Webcam car elle n'a pas besoin d'être reliée à un PC pour fonctionner, en réalité c'est un serveur qui stocke des images qu'il fourni à la demande.
- Une caméra réseau possède sa propre adresse IP.
- La caméra peut être consultée de plusieurs postes à la fois et fournir des images différentes au même moment selon la requête.
- On peut consulter les images à partir d'un simple explorateur (Internet explorer etc..) mais les progiciels spécialisés sont beaucoup plus conviviaux et reprennent la plupart des fonctions de vidéosurveillance, ils permettent également de visualiser plusieurs caméras du même site ou de site différents au même moment.
- Lorsque l'on veut rendre accessible une caméra à l'extérieur d'un site il faut la connecter à une liaison ADSL (IP fixe) par l'intermédiaire d'un routeur ADSL.
- Pour visualiser sur le réseau des caméras vidéo classiques analogiques, il existe des serveurs vidéo/IP pouvant recevoir de 1 à plusieurs caméras.
- Il existe principalement deux sortes de technologies de compression dans les caméras IP : MJPEG et MPEG-4 qu’on y reviendra après au cours de ce chapitre.

Contrairement aux caméras analogiques, les caméras réseau présentent non seulement des capacités de capture et d’affichage d’images, mais aussi de gestion et

de compression numérique pour le transfert réseau. La qualité de l'image peut varier considérablement. Elle dépend d'un ensemble de facteurs tels que le choix de l'optique et du capteur d'images, les capacités de traitement et le type de la compression vidéo.

1.3.3. Les avantages de la vidéo IP

La vidéo IP présente plusieurs caractéristiques dont nous nous intéressons aux caractéristiques du flux images délivré et les différentes manipulations qui peuvent êtres appliqués dessus. En effet, les images peuvent être :

- ✓ ***Visualisées*** sur l'ensemble des postes du réseau local ou distant.
- ✓ ***Stockées*** sur un disque dur ou un serveur pour une utilisation ultérieure.
- ✓ ***Imprimée****s* ou ***transmises*** par mail (format JPEG).

Il suffit d'une prise réseau pour connecter une caméra réseau (plus de câble coaxial dédié) vu sa structure physique et les ports d´entrée/sortie dont elle dispose.

De plus, une des caractéristiques de l'IP-Surveillance est sa flexibilité. En effet, il offre des possibilités d'ajoutez des caméras, des serveurs vidéo et des enregistreurs vidéo numériques réseaux (DVR) au sein des systèmes de surveillance à architecture IP rapidement et facilement, quand vous le souhaitez.

En outre, Les serveurs vidéo se connectent sur les caméras analogiques existantes, numérisent les images et les transfèrent sur le réseau IP.

Les caméras réseau se connectent directement sur les réseaux IP. Celles plus élaborées incorporent à la fois des connecteurs de sortie analogique et numériques, permettant la connexion simultanée dans les deux mondes [2].

1.3.4. Exemple de caméras IP

Figure1.3: Camera WIFI D-Link DCS 2100+

1.4. Les techniques de compression/décompression vidéo

1.4.1. Types de compression

La compression vidéo fait rappel à une variété d'algorithmes de codage qui exploitent les différents types de redondance de l'image. Le choix et l'association de ces algorithmes se fait en fonction des applications visées et des débits souhaités.

On distingue deux grandes catégories d'algorithmes de compression. Ceux dits «sans pertes» (losless en anglais) effectuent un traitement totalement transparent, permettant de retrouver intégralement les données d'origine après décompression. Malheureusement, ils ne conduisent qu'à des taux de compression très faibles, en tout cas insuffisants pour la plupart des applications vidéo (mais ils sont les seuls à pouvoir être utilisés en informatique).

Les algorithmes « avec pertes » (lossy en anglais) aboutissent à des taux de compression nettement supérieurs, mais imposent de négliger certaines informations de l'image, en tenant compte de sa nature et de notre perception

visuelle. Si elle se fait dans des propositions limitées, l'élimination de ces informations peut passer inaperçue pour un téléspectateur ; on parle alors de compression virtuellement transparente. Si, en revanche, la réduction de débit doit être réalisée dans des facteurs élevés, le prix à payer est l'apparition d'artéfacts et distorsions plus ou moins visibles. Précisons cependant que ces dégradations se distinguent fondamentalement de celles qui peuvent perturber un signal analogique. Les conséquences les plus caractéristiques d'une compression trop poussée sont : une perte de définition, une saccade dans les mouvements, un figement de certaines parties de l'image, un effet de pixellisation dans les mouvements et les fondus (effets de blocs), une solarisation sur les dégradés de couleurs, ainsi que l'apparition d'une sorte de frange autour des contours marqués (en particulier sur les textes en incrustation) [3].

Les méthodes de compression suivent également deux approches différentes par rapport aux normes de compression : compression des images fixes et compression vidéo. Mais, dans le cadre de notre étude, nous étudions uniquement le cas du codec vidéo et précisément la norme MPEG-4 utilisée dans notre système de vidéosurveillance.

1.4.2. Normes de compression vidéo

1.4.2.1. La compression M-JPEG

M-JPEG (Motion Joint Photographic Experts Group) est la norme la plus répandue parmi les systèmes de vidéo sur IP. Une caméra réseau, tout comme un appareil numérique permettant la capture d'images immobiles, saisit des images individuelles, et les compresse 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.

1.4.2.2 H.263

La technique de compression H.263 est conçue pour une transmission vidéo à débit fixe. L'inconvénient du débit fixe est que l'image perd de sa qualité lorsque les objets sont en mouvement. La norme H.263 était initialement destinée aux applications de vidéoconférence et non à la surveillance où les détails ont plus d'importance que la régularité du débit.

1.4.2.3. 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 entre elles deux images compressées destinées à être transmises sur le réseau. La première des deux images servira de trame de référence. Sur les images suivantes, seuls seront envoyées les zones qui diffèrent de la référence. 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. La

première des deux images servira de trame de référence. Sur les images suivantes, seuls seront envoyées les zones qui diffèrent de la référence comme le montre la figure 1.4.

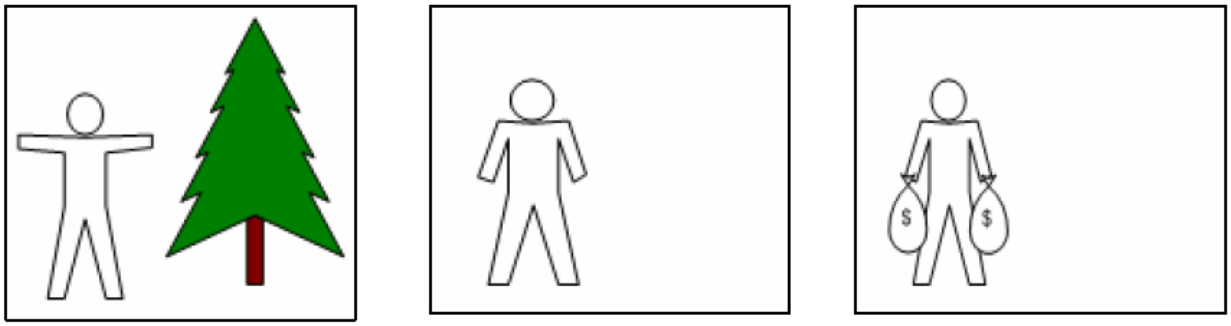

Figure 1.4 : Principe du codage MPEG

L'encodeur réseau reconstruit alors toutes les images en fonction de l'image de référence. Cette méthode implique bien souvent des techniques ou des outils supplémentaires permettant de gérer certains paramètres tels que la prédiction du mouvement dans une scène ou l'identification des objets.

La compression vidéo MPEG réduit le volume de données à transmettre via le réseau.

Il existe différentes normes MPEG : MPEG-1, MPEG-2 et ensuite MPEG-4.

- MPEG-1, lancée en 1993 et destinée à l'archivage des données vidéo numériques sur CD. La plupart des encodeurs et des décodeurs MPEG-1 sont conçus pour un débit d'environ 1,5 Mbit/s en résolution CIF. MPEG-1 met surtout l'accent sur le maintien d'un débit relativement constant, au détriment de la qualité d'image, laquelle est variable et comparable à la qualité vidéo VHS [4].

- MPEG-2, approuvée en 1994, était destinée à la vidéo numérique de qualité supérieure (DVD), à la télévision haute définition (HDTV), aux supports d'enregistrement interactifs (ISM), aux systèmes d'émission vidéo numérique (DBV) et à la télévision par câble (CATV). Le format MPEG-2 visait à accroître la technique de compression de la norme MPEG-1 afin de couvrir des images plus grandes et de meilleure qualité, mais aux dépend d'un taux de compression plus faible et d'un débit d'images plus rapide [4].
- MPEG-4, a été pensé pour gérer de la vidéo à bas débit pour des applications multimédias, elle offre une vidéo de qualité, mais une bonne implémentation de MPEG 4

  était jusqu'à récemment restée trop chère pour être incorporée à une caméra IP dédiée. Toutes fois, les couts, les performances et la consommation des capteurs et du matériel de compression MPEG-4 se sont améliorés au point que cette technologie est devenue accessible. La qualité vidéo, transmise via réseau et décodée sur moniteur analogique ou affichée sur application informatique est identique à celle d'une vidéo analogique [5].

Le principe adopté dans MPEG-4 est celui d'une description autonome du contenu : l'image n'est plus codée dans sa globalité mais elle apparaît comme une composition réalisée avec différents « objets » audiovisuels [6]. Ces objets peuvent être de différentes natures : image fixe (par exemple, le décor du fond, un tableau), objets vidéos (le personnage sans le décor), objets audio (la voix de la personne, le fond musical), etc.

1.5. Méthodes de transmission de la vidéo sur IP

Il existe trois méthodes pour la transmission de la vidéo sur IP: diffusion individuelle, multidiffusion et radiodiffusion.

1.5.1. Diffusion individuelle (Unicast)

L'émetteur et le récepteur communiquent entre eux via une liaison point-à-point. Les paquets de données sont adressés à un seul récepteur. Aucun autre ordinateur du réseau n'a besoin de traiter ces informations [7].

1.5.2. Multidiffusion (Multicast)

Communication entre un seul émetteur et plusieurs récepteurs sur un réseau. Les technologies de multidiffusion permettent de réduire le trafic sur le réseau lorsque plusieurs récepteurs souhaitent visualiser une même source en même temps. Un seul flux d'information peut ainsi être envoyé à des centaines de récepteurs. La différence majeure par rapport à la diffusion individuelle est que le flux vidéo ne doit être envoyé qu'une seule fois. La multidiffusion est fréquemment utilisée en conjonction avec les transmissions RTP [7].

1.5.3. Radiodiffusion (Broadcast)

Type de transmission de un à tous. Sur un réseau LAN, le Broadcast est en principe limité à certains segments spécifiques et ne s'applique pas en pratique aux transmissions vidéo sur IP [7].

1.6. Protocoles de transport de données pour la vidéo sur IP

Les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont les deux protocoles IP utilisés pour l'envoi des données. Ces protocoles de transport jouent le rôle de « transporteurs » pour de nombreux autres protocoles. Ainsi, le protocole HTTP (Hyper Text Transfer Protocol), qui est utilisé pour parcourir des pages Web sur des serveurs dans le monde entier via Internet, est transporté par TCP.

Le protocole TCP constitue un canal de transmission fiable et base sur les connexions. Il gère le processus de division de gros blocs de données en paquets de petites tailles et garantit que les données envoyées d'une extrémité sont reçues à l'autre extrémité. La fiabilité obtenue par retransmission peut cependant causer des délais importants. En général, le protocole TCP s'utilise lorsque la fiabilité de la communication a priorité sur la latence du transport.

Le protocole UDP est un protocole dit sans « connexion » qui ne garantit pas la livraison physique des données envoyées et laisse donc à l'application le soin de vérifier et de contrôler les erreurs [8].

Le tableau 1.1, montre les Protocoles TCP/IP et ports couramment utilisés dans le cadre de la vidéo sur IP.

Protocole	Protocole de transport	Port	Utilisation courante	Utilisation dans le domaine de la vidéo sur IP
FTP (File Transfer Protocol)	TCP	21	Transfert de fichiers sur Internet/intranets	Transfert d'images ou de vidéos depuis une camera réseau ou un encodeur vidéo vers un serveur FTP ou une application
SMTP (Send Mail Transfer Protocol)	TCP	25	Protocole d'envoi de messages électroniques	Une caméra réseau ou un encodeur vidéo peut envoyer des images ou des notifications d'alarme à l'aide de son client de messagerie intégré
HTTP (Hyper Text Transfer Protocol)	TCP	80	Permet de parcourir le Web, c'est-à-dire récupérer des pages Web a partir de serveurs Web	Méthode la plus courante pour transférer de la vidéo depuis une caméra réseau ou un encodeur vidéo, selon laquelle le périphérique de vidéo sur IP fonctionne essentiellement comme un serveur Web qui met la vidéo à disposition de l'utilisateur ou de l'application demandeuse

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)	TCP	443	Permet d'accéder à des pages Web de manière sécurisée, à l'aide d'une technologie de cryptage	Transmission sécurisée des vidéos à partir de caméras réseau ou d'encodeurs vidéo
RTP (Real Time Protocol)	UDP/TCP	Non définit	Format de paquet RTP normalise pour la remise de données audio et vidéo sur Internet-souvent utilisé dans les systèmes de diffusion multimédia par flux ou pour la vidéoconférence	Méthode courante de transmission de vidéo sur IP H.264/MPEG et de synchronisation des données vidéo et audio. Le protocole RTP fournit une numérotation séquentielle et un horodatage des paquets de données, ce qui permet de les réassembler dans l'ordre correct. La transmission peut être en monodiffusion ou en multidiffusion.
RTSP (Real Time Streaming Protocol)	TCP	554	Permet de configurer et de contrôler les sessions multimédias sur RTP	

Tableau 1.1: Protocoles TCP/IP et ports couramment utilisés dans le cadre de la vidéo sur IP.

1.6.1. Le streaming vidéo

1.6.1.1. Définition de streaming

Le streaming consiste à diffuser une vidéo d'un serveur vers un client à travers le réseau Internet. En effet, en émission, le serveur segmente la vidéo en paquets susceptibles d'être diffusés sur le réseau. Ces paquets seront ensuite assemblés par le client afin de reconstituer la vidéo. A la différence d'un simple transfert de fichier, la vidéo est jouée au fur et à mesure que les paquets arrivent.

Il existe actuellement trois protocoles permettant de faire du streaming. Les deux premiers, HTTP et FTP, sont des protocoles de transfert de fichier. On peut néanmoins parler de streaming dans la mesure où les vidéos peuvent être affichées

au fur et à mesure du téléchargement. Le troisième protocole, RTP (Real Time Protocol), est celui qui permet de faire convenablement du streaming.

1.6.2. Le protocole RTP

Le principe du protocole RTP (Real Time Protocol) consiste à envoyer les paquets en temps réel sur le réseau. Les paquets sont marqués temporellement de manière à être réordonnancés par le client afin d'afficher la vidéo de manière cohérente. Grâce à ce protocole, on peut diffuser des vidéos préenregistrées ainsi que des images en direct [9].

Il permet des services de type unicast ou multicast sans garantie de qualité de service (QoS). Par opposition à http et FTP qui fonctionnent au dessus de TCP (mode connecté), RTP fonctionne au dessus d'UDP (mode non connecté) [10].

De la même manière que TCP est ajouté à IP, RTCP (Real Time Transfert Control Protocol) contrôle le RTP. Egalement, pour améliorer les performances de RTP, un protocole spécifique au streaming permet de contrôler la diffusion du contenu. Il s'agit de
RTSP (Real Time Streaming Protocol) [10] qu'on va détailler dans le paragraphe suivant.

1.6.3. Le protocole RTSP

RTSP « Real Time Streaming Protocol » est un protocole de Streaming temps réel développé par l'IETF et publié en 1998 en tant que « RFC 2326 ». Il s'agit d'un protocole de niveau applicatif qui sert à contrôler les propriétés temps réel du contenu délivré. Il est adapté aussi bien à la diffusion de données préenregistrées que de données diffusées en direct.

1.6.3.1. Les fonctions de RTSP

RTSP offre des fonctionnalités typiques d'un lecteur vidéo telles que : lecture, pause, arrêt, etc. Il peut être utilisé pour rechercher un média sur un serveur de médias, inviter un serveur de médias à rejoindre une conférence (par exemple dans le e-Learning), ou ajouter un média à une présentation existante. Il assure aussi la synchronisation de plusieurs flux audio ou vidéo. Inspiré de HTTP et incluant ses mécanismes de sécurité (SSL et authentification), RTSP autorise le maintien de connexion nécessité, par exemple, par la fonction pause, l'étiquetage des contenus, le paiement électronique. Il autorise la commande et le contrôle à distance des serveurs multimédias indispensable au client lecteur [10].

La figure 1.5 donne un panorama complet des protocoles utilisés pour la diffusion vidéo sur IP y compris le protocole RTSP.

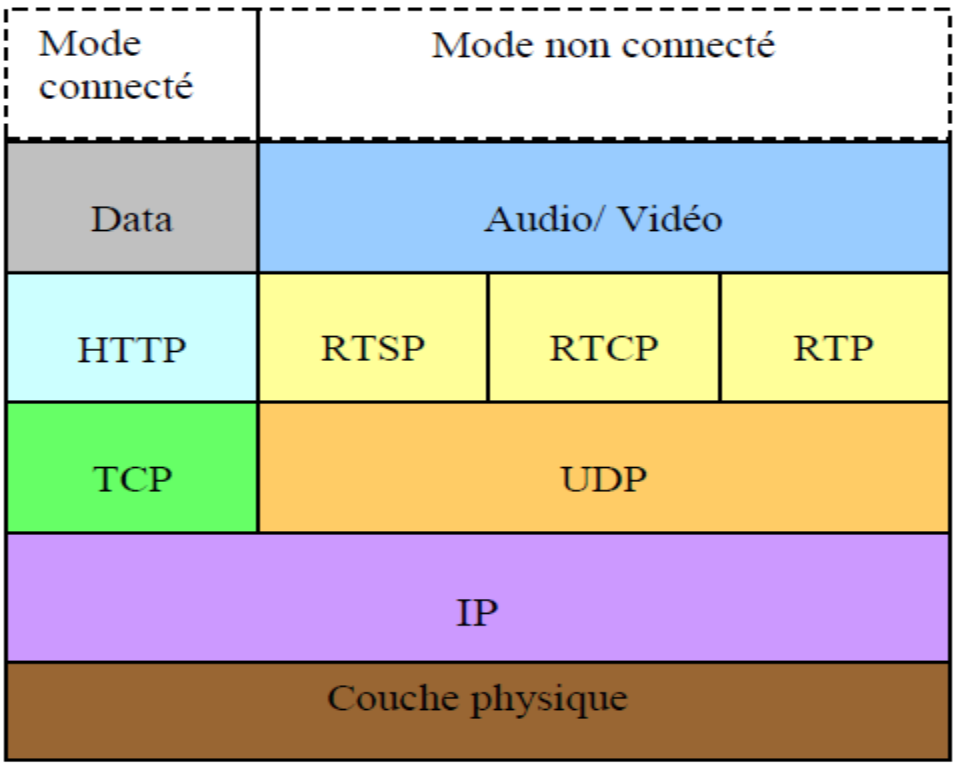

Figure 1.5: Pile protocolaire de la diffusion vidéo sur IP

- Le protocole UDP (User Datagram Protocol) fonctionne sans contrôle d'erreurs, sans remise en ordre des paquets à l'arrivée, sans réémission des données perdues et sans procédure d'acquittement. Il présente l'avantage d'être plus rapide que TCP permettant des processus temps réel de multi diffusion ou de streaming.
- Au cours d'une même session, les deux protocoles TCP et UDP peuvent être simultanément utilisés conjointement avec IP en fonction des caractéristiques des données à transmettre : TCP pour les données ne souffrant aucune perte (textes, tableaux) et UDP pour la transmission des signaux audio et vidéos pour lesquels une transmission en temps réel est exigée mais où des pertes peuvent être tolérées.

Ces protocoles majeurs ont été complétés par des protocoles spécifiques et par des mécanismes particuliers destinés à optimiser la transmission des données audiovisuelles.

- Le protocole RTP (Real time Transport Protocol) contrôle les flux vidéo et audio dans les applications en temps réel. Il assure la numérotation des séquences, ajoute une référence temporelle (time stamp) qui indique l'instant exact d'émission du paquet à la source permettant ainsi à l'arrivée de replacer les paquets dans le bon ordre, et de rétablir la régularité temporelle (RTP permet ainsi d'assurer un jitter inférieur à 40 ms). Les en-têtes RTP indiquent, également, la nature du codage audio ou vidéo.
- RTSP peut être utilisé aussi bien dans des applications unicast que multicast.

1.6.3.2. Le streaming unicast

Le client contacte le serveur de streaming grâce au protocole RTSP. En réponse à cette requête, le serveur retourne via RTSP une description de la session de streaming qu'il va ouvrir. Une session de streaming est composée d'un ou

plusieurs flux (Stream), audio ou vidéo. Le serveur informe le client du nombre de flux. Il donne aussi des informations décrivant les flux comme le type du média et le codec de compression. Les flux sont quant à eux diffusés via le protocole RTP [10].

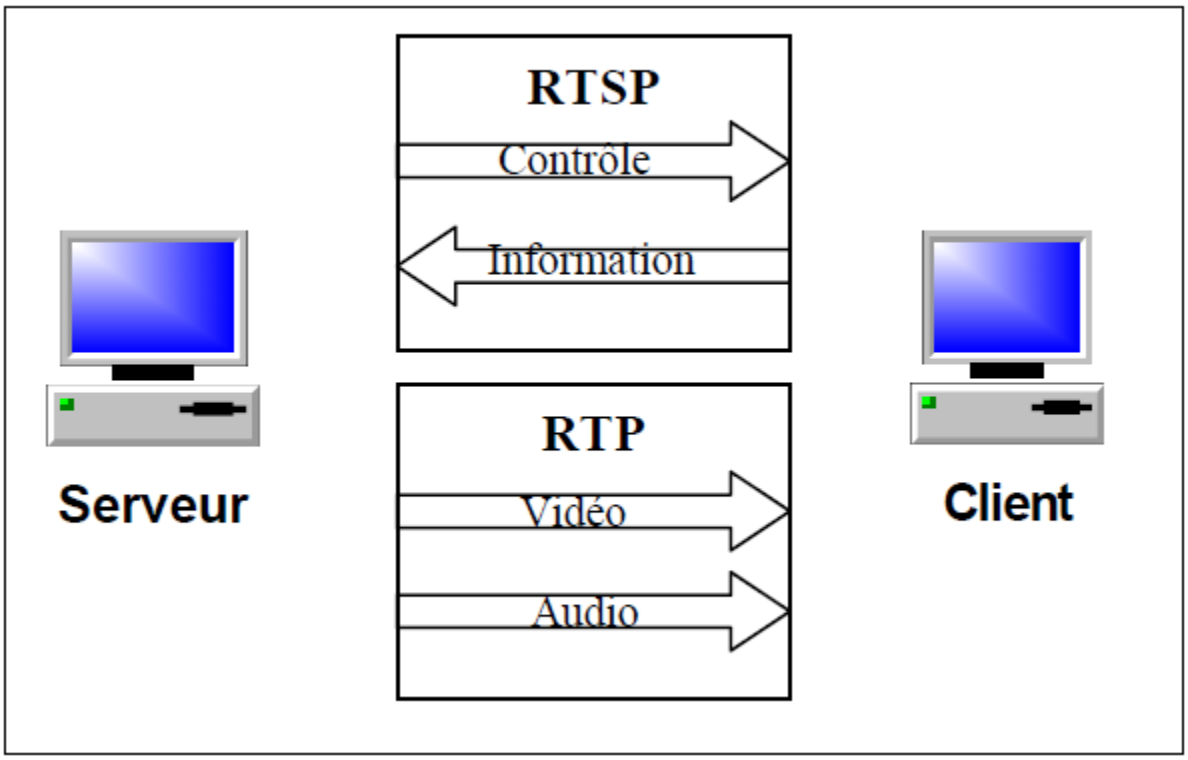

Figure 1.6: Streaming Unicast

1.6.3.3. Le streaming multicast

Dans le cas du streaming multicast, une seule copie de chaque flux est envoyée sur chaque branche du réseau, ce qui permet de réduire considérablement le trafic lors d'une diffusion vers plusieurs clients.

Une diffusion multicast est annoncée par un ficher SDP (Session Description Protocol) qui est téléchargé à partir d'un serveur web classique (Apache, IIS). Ce fichier contient les informations nécessaires pour recevoir le flux multicast, adresse

IP du serveur, numéro du port et les informations de description des flux (même informations que celle envoyées par RTSP dans le cas d'une diffusion unicast) [10].

La figure 1.7 représente le principe du streaming multicast.

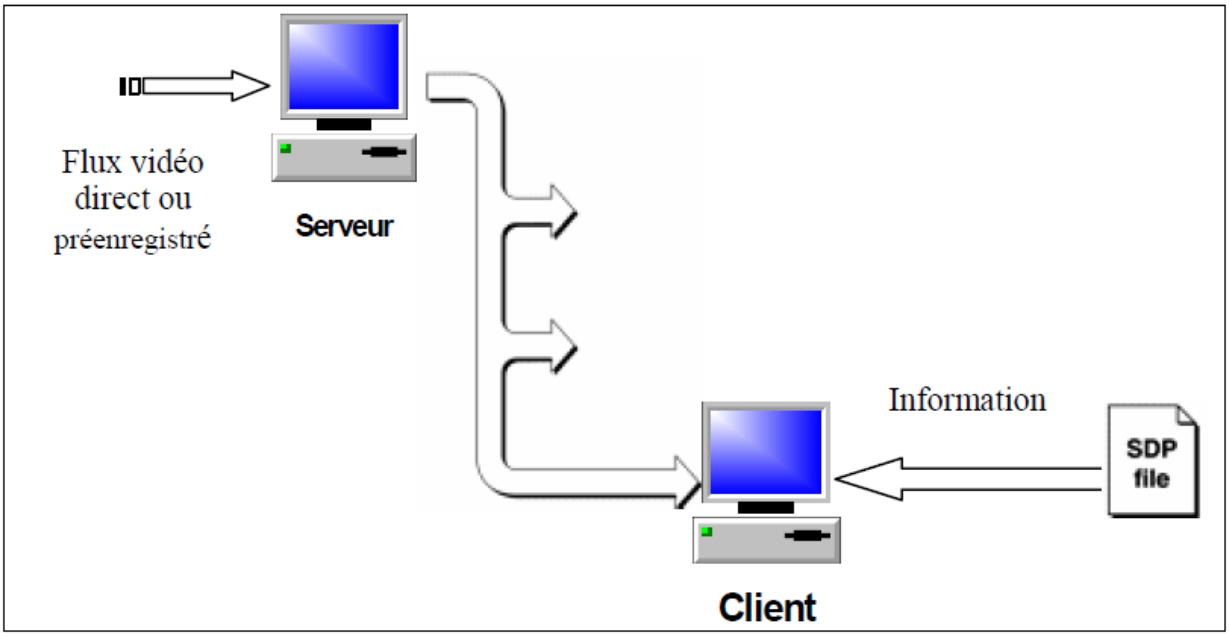

Figure 1.7 : Processus de la diffusion Multicast

Le principal frein à l'utilisation massive du multicast vient du fait que les routeurs doivent supporter cette technologie, ce qui n'est malheureusement pas le cas de l'ensemble des infrastructures constituant l'Internet. Subséquemment, afin de permettre aux clients, situés derrière ces routeurs, d'accéder aux données multicast, il est possible d'installer un serveur de streaming qui va agir comme une passerelle entre multicast et unicast. Ce serveur est connecté aux flux multicast et sert aux clients, qui se connectent à lui, ces flux sous la forme de flux unicast en utilisant RTP et RTSP. Cette opération s'effectue en temps réel, ce qui permet de retransmettre aussi bien des vidéos préenregistrées que des images en direct [10].

La figure 1.8 représente le processus de la diffusion Multicast-Unicast.

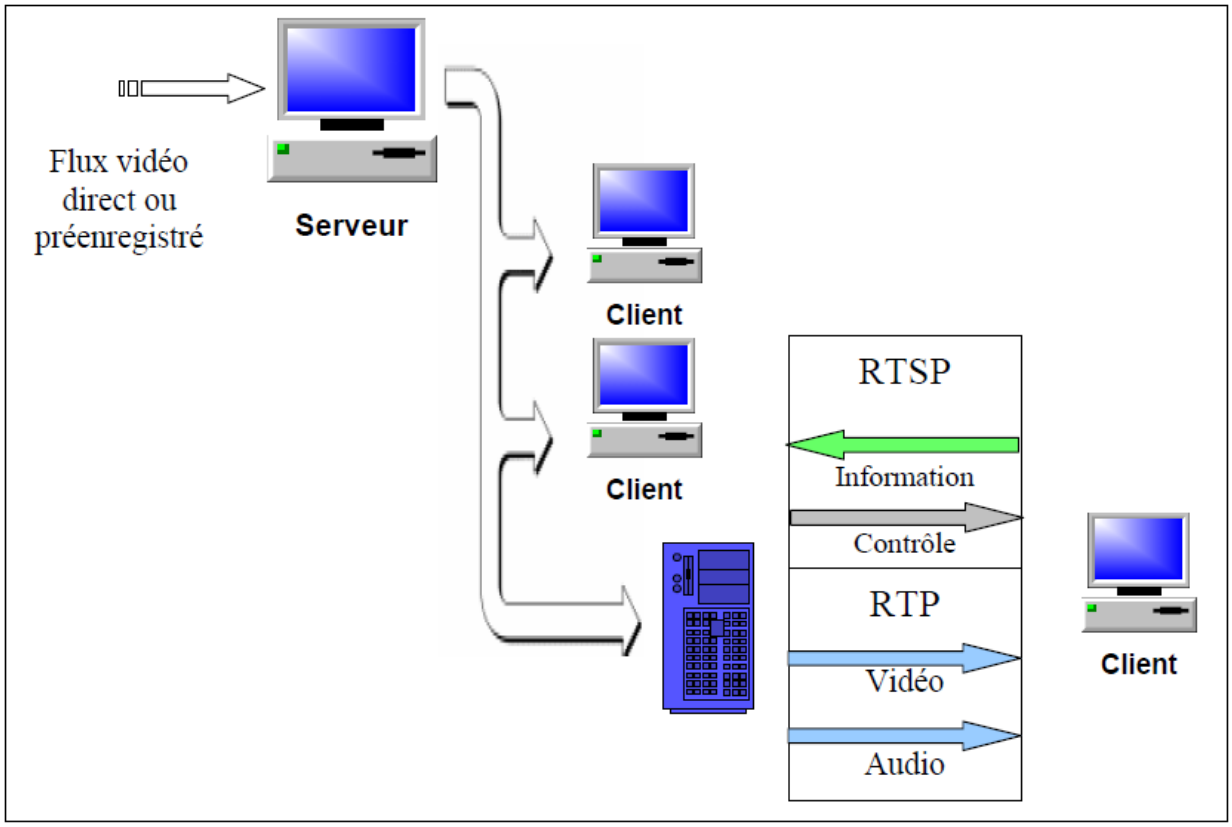

Figure 1.8 : Processus de la diffusion Multicast-Unicast

1.6.3.4. Principe de fonctionnement

a. Notion de session

Le protocole de streaming vidéo RTSP repose sur la notion de session pour accomplir un échange commode entre un serveur et un ou plusieurs clients. En effet, pour chaque session, le serveur attribue un identificateur sous forme d'une chaîne de caractère de longueur arbitraire pour que sa découverte soit plus difficile. Le protocole RTSP ne se contente pas de transmettre les données du serveur et les requêtes du client, mais il est capable de reconnaître à quel instant un paquet de données doit être transmis au client par une étiquette temporelle inscrite sur chaque

paquet. Cette méthode permet la mise en œuvre de stratégies de filtrage des données du côté du serveur (à la source) [11].

b. Protocole à « état »

RTSP est un protocole avec états qui utilise la notion de session. Cette caractéristique est importante pour effectuer le transfert de média continus [11]. En effet, la présentation d'objets de type média continus est caractérisée par une évolution entre différents états de présentation comme le montre la figure 1.9.

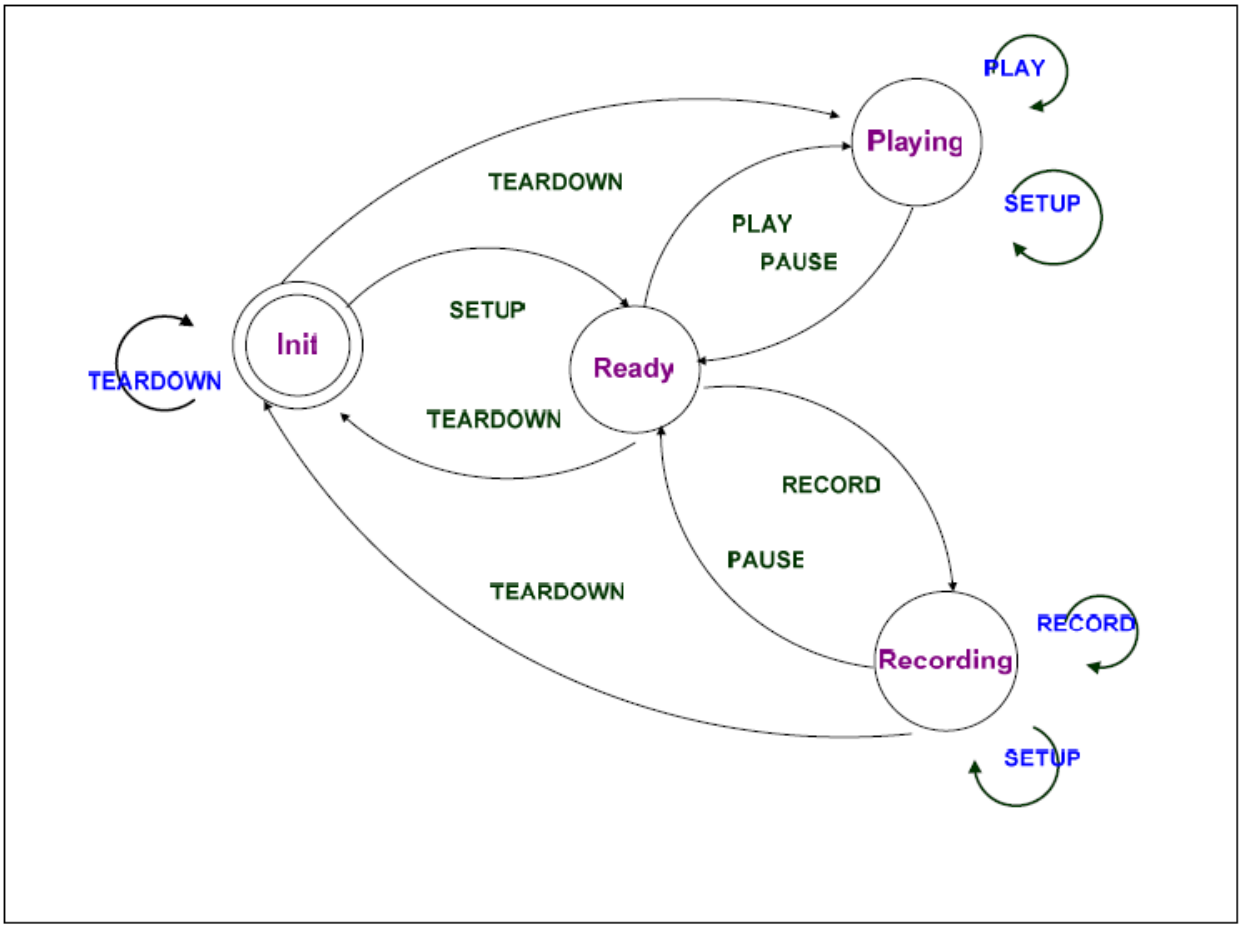

Figure 1.9 : Machine d'états du protocole RTSP

L'évolution des transferts de données est décrite par une machine d'états associée au client et au serveur. Le serveur change d'état quand il reçoit une requête du client, et le client change d'état quand il envoie une requête au serveur. Pour

chaque transfert de données, le serveur RTSP maintient une session qui est désignée par un identificateur unique. Cet identifiant permet au client RTSP d'ouvrir et fermer plusieurs connexions de transport avec le serveur RTSP en gardant la correspondance entre l'état courant du côté client et celui du côté serveur [11].

c. La qualité de service (QoS)

Au niveau du protocole, RTSP permet de surveiller la qualité de la transmission à travers RTCP. Pour cela, le client émet périodiquement vers le serveur (boucle de contrôle ou feed-back) des rapports sur la qualité de la transmission, contenant le pourcentage et le nombre de paquets perdus, le délai de transmission et la gigue. Le serveur reçoit ces rapports et apprécie s'il y a congestion. Dans ce dernier cas, le serveur réduit le débit d'émission : c'est le principe du contrôle de flux [12].

d. Les messages

- RTSP hérite la syntaxe de HTTP.
- L'URL a la même forme qu'une adresse http: (rtsp://192.168.0.61/mpeg4live.mp4)
- Dans l'entête des messages, il y'a toujours comme en HTTP une ligne de la forme :

RTSP Version = "HTTP" "/" 1*DIGIT "." 1*DIGIT.

Exemple : RTSP / 1.0 200 OK

- Les principales méthodes utilisées dans l'échange client –serveur, selon [12], sont :
  - DESCRIBE : utilisée par le client pour récupérer la description d'une présentation ou d'un objet média sur un serveur RTSP.

- ANNOUNCE : Si elle est émise par le serveur, elle permet de changer la description d'une présentation en temps réel, lors par exemple de l'introduction d'un nouveau média. Lorsqu'elle est émise par le client, elle permet d'envoyer une description de présentation à un serveur.
- SETUP : utilisée par le client pour spécifier au serveur les paramètres de transport du flot média comme le type de protocole de transport (RTP), le mode de transport (point à point ou multipoint) et le numéro du port de communication. Le serveur renvoie alors une identification de session utilisée jusqu'à la fermeture de la session.
- PLAY : Elle signale au serveur qu'il peut commencer à envoyer les données via le mécanisme spécifié dans la méthode *SETUP*. Elle permet également de lire un ou plusieurs sous intervalles de la durée d'un objet média
- PAUSE : utilisée par le client pour demander au serveur d'interrompre temporairement le transfert du flux média. Le client peut reprendre la transmission du flux en envoyant la requête *PLAY* au serveur.
- TEARDOWN : Elle est utilisée par le client pour demander au serveur d'arrêter définitivement le transfert du flux média.
- GET_PARAMETER : permet de retrouver la valeur d'un paramètre d'une présentation ou d'un flux multimédia. En outre, elle peut être utilisée pour tester si le client ou le serveur sont encore actifs (Ping ou keep alive).
- SET_PARAMETER : Elle permet de donner la valeur d'un paramètre d'une présentation ou d'un flux multimédia. Par exemple, modifier l'orientation et la focale des caméras.

- REDIRECT : informe le client qu'il doit se connecter à un autre serveur. Elle contient l'adresse du nouveau serveur chez lequel le client devra formuler les requêtes.
- RECORD : Elle est utilisée par le client pour démarrer l'enregistrement.
- OPTIONS : Elle permet au client d'interroger le serveur sur les requêtes qu'il doit accepter.
- SESSION : Elle permet au serveur d'envoyer au client une nouvelle description de présentation.

La figure 1.10 donne un exemple d'échange client-serveur RTSP.

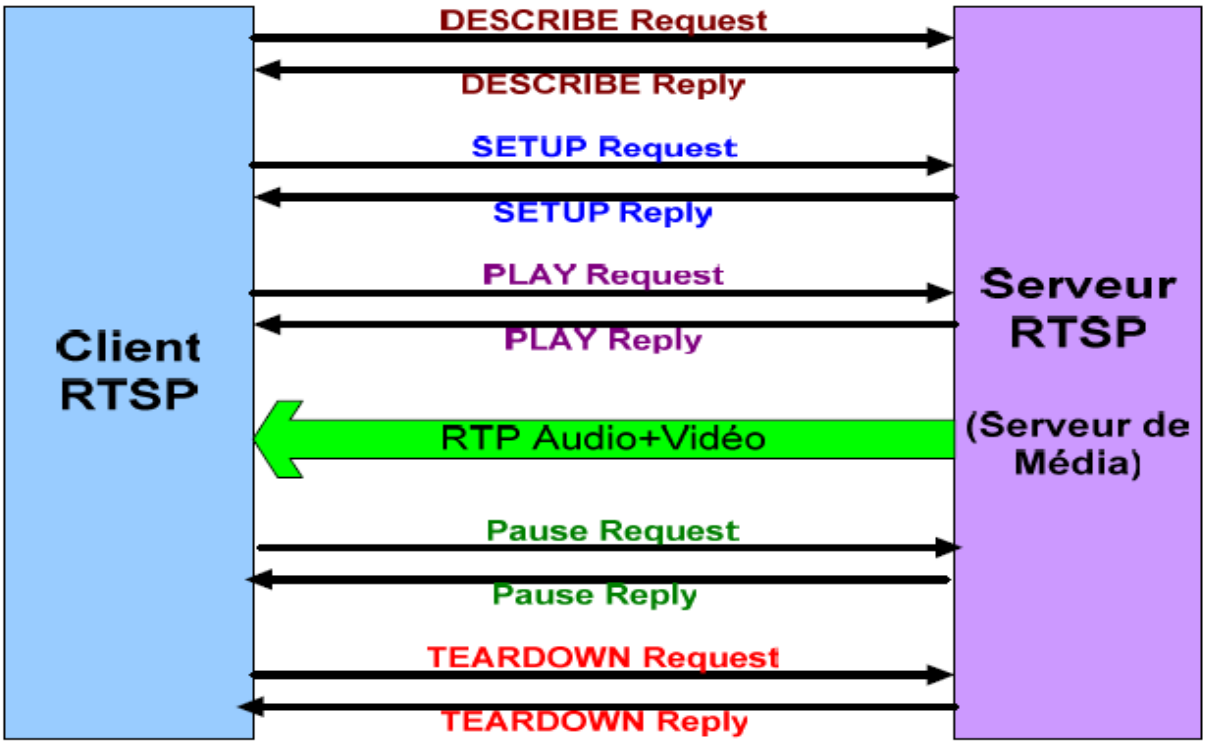

Figure 1.10 : Exemple d'échange client serveur RTSP

1.7. Architecture client serveur : 2-tiers

Le système de vidéosurveillance sur IP fonctionne en mode client serveur. En effet, chaque caméra IP joue le rôle d'un serveur vidéo à tout autre poste qui demande du streaming vidéo.

Il s'agit alors d'une architecture 2-tiers, composée de deux éléments, un client et un serveur et où le tiers fait référence non pas à une entité physique mais logique, et que l'on peut représenter via le schéma de la figure 1.11.

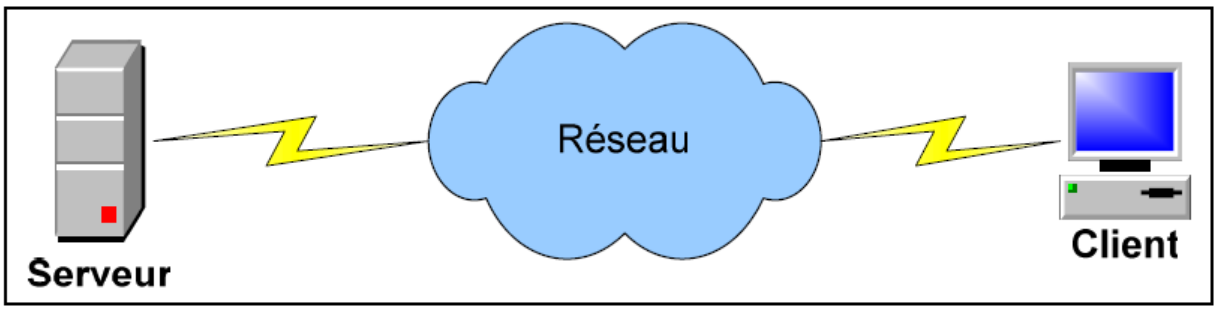

Figure 1.11 : Architecture 2-tiers

Une telle architecture est généralement recommandée pour les applications nécessitant un grand niveau de fiabilité puisqu'elle présente plusieurs avantages dont on peut énumérer :

- Les ressources sont centralisées: le serveur peut gérer des ressources communes à plusieurs utilisateurs telles que les séquences vidéos préenregistrées ou directes. Ce privilège permet d'éviter les problèmes de redondance et de contradiction [13].
- Meilleure sécurité: car dans la plupart des cas, l'accès au serveur est authentifié et le nombre de points d'entrée est limité [13].
- Un réseau évolutif: grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures [13].

Le fonctionnement du mode client serveur se fait généralement selon le modèle exposé par la figure 1.12.

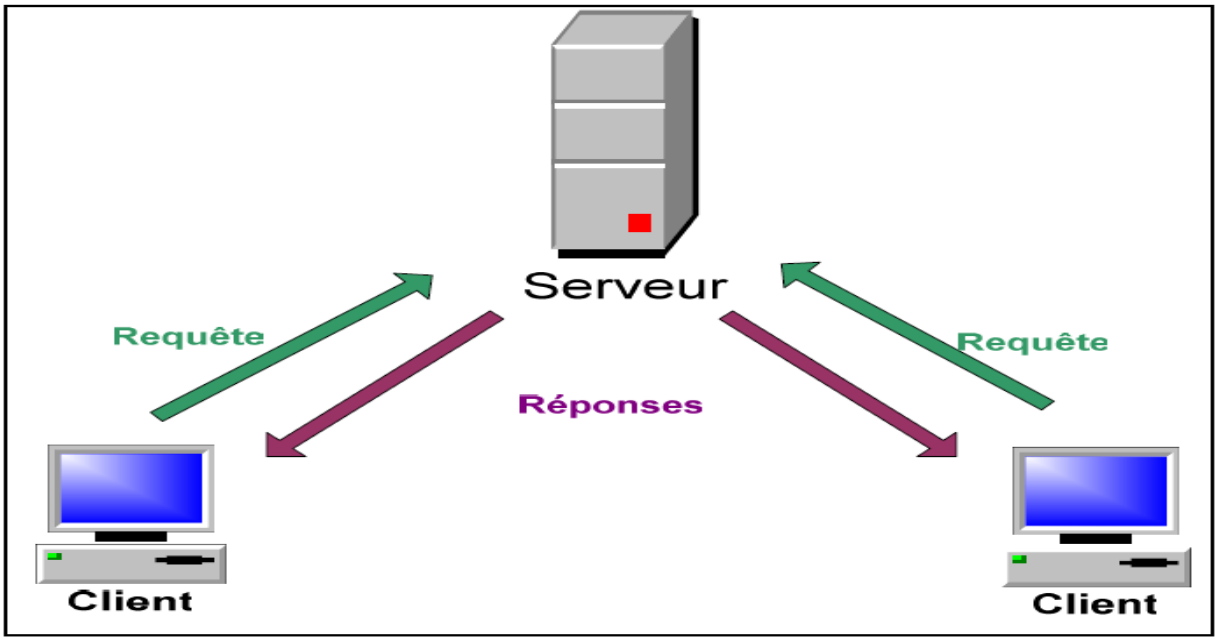

Figure 1.12 : Interaction client serveur

- Le client émet une requête vers le serveur (la caméra IP) grâce à son adresse et le port, qui désigne un service particulier du serveur. Dans notre système, le client peut être n'importe qu'elle poste connectée au réseau, le serveur c'est la caméra IP et le service demandé c'est le streaming vidéo moyennant le protocole RTSP ayant le port numéro 554.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

1.8. Domaines d'application de la vidéosurveillance sur IP

La vidéosurveillance sur IP est une technologie réputée, digne d'intérêt, non seulement pour les applications de surveillance classiques et de contrôle à distance

actuelles, qu'elle peut améliorer ou revitaliser, mais également pour un grand nombre d'applications nouvelles dans de nombreux secteurs comme par exemple :

- *Education* : sécurité et contrôle à distance des cours d'école, des couloirs, des halls et des salles de classe et sécurité des bâtiments.
- *Transport* : contrôle à distance des gares ferroviaires et des quais, des voies publiques et des aéroports
- *Banques* : applications de sécurité traditionnelles à l'intérieur des banques et de leurs succursales et partout où il y a des guichets automatiques
- *Services administratifs* : applications de surveillance de sécurité, souvent intégrées aux systèmes de contrôle d'accès actuels et futurs
- *Commerce* : sécurité et contrôle à distance pour une gestion des magasins plus aisée et plus efficace
- *Industrie* : contrôle des procédés de fabrication, des systèmes logistiques, des systèmes de contrôle des stocks et de l'entreposage (avec une variante d'un intérêt particulier et qui ne sera pas traité dans ce dossier, qui est la reconnaissance de forme dans les chaînes de fabrication).
- *Surveillance des maisons en absence de leurs propriétaires*.
- *Contrôle des accès des entreprises et des locaux politiques, etc.*

1.9. Conclusion

Nous avons découvert que la vidéo surveillance sur IP demeure incontestablement la technique qui donne les meilleures solutions qui sont aujourd'hui en pleine évolution et représente une alternative intéressante pour les problèmes de sécurité des personnes et des biens.

Apres avoir étudié les différentes notions liées à un système de vidéosurveillance sur IP et les différentes contraintes engendrées lors de la

conception de système vidéo sur Internet, le chapitre suivant sera consacré à la technique de spécification et une étude de la solution envisagée sera présentée.

Chapitre 2

Etude du système de vidéosurveillance IP

2.1. Introduction

Le système de vidéosurveillance sur IP à développer vise à surveiller à distance un ou plusieurs sites (chambre, entrepôt, Entreprise, carrefour, parking externe). Le principe général de cette solution de surveillance repose sur la capture des séquences d'images de la source, par une ou plusieurs caméras IP, et l'envoie de ces séquences à un poste de visualisation et de contrôle distant via le réseau IP. Ce dernier prend une décision suivant le résultat de l'analyse des données reçues.

Dans ce chapitre, nous allons élaborer la conception du système de vidéosurveillance sur

IP c'est-à-dire la manière dont le système doit réagir, du point de vue utilisateurs et fonctionnalités. La démarche que nous suivrons dans notre conception est indiquée par l'organigramme suivant.

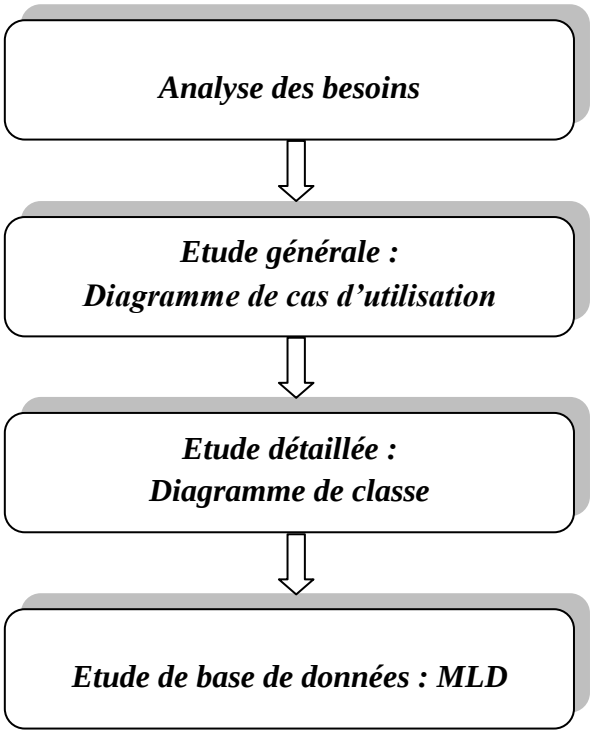

Figure 2.1 : Organigramme de la conception de notre système de vidéosurveillance

2.2. Analyse des besoins

La problématique de notre application consiste à développer un logiciel qui permet d'effectuer toutes les opérations de vidéosurveillance. En effet, il va offrir les fonctionnalités de la bas exigées par toute applications de surveillance et de contrôle distance tel que :

- La visualisation en direct des séquences vidéo en provenance des caméras IP locales ou distantes
- L'enregistrement vidéo selon différent modes : continue, planifié, sur détection des alarmes et des mouvements.
- Fonction de la recherche multiple des séquences enregistrées.
- Contrôle et configuration des caméras via un navigateur Web.*
- Fonctions de gestion des alarmes (alarmes sonores, messages affichés ou e-mail)
- Notification des alarmes par E-mail, SMS, MMS.
- Des permissions sont attribuées par groupes d'utilisateurs, leur permettant d'avoir accès ou non aux différentes fonctionnalités du logiciel.
- Un fichier journal ou historique enregistre tous les événements, les opérations et les accès qui ont eu lieu sur le système.

Cette solution de vidéosurveillance peut servir à :

- Surveillance les maisons en absence de leur propriétaire.
- Le contrôle des points d'accès des espaces commerciaux et bancaires.
- Surveiller les bébés, vieux.
- Le contrôle d'accès.
- L'éducation à distance.
- La détection d'intrusion ou la surveillance de production.

La figure 2.2 explique le principe de base d'un tel système de vidéosurveillance sur IP

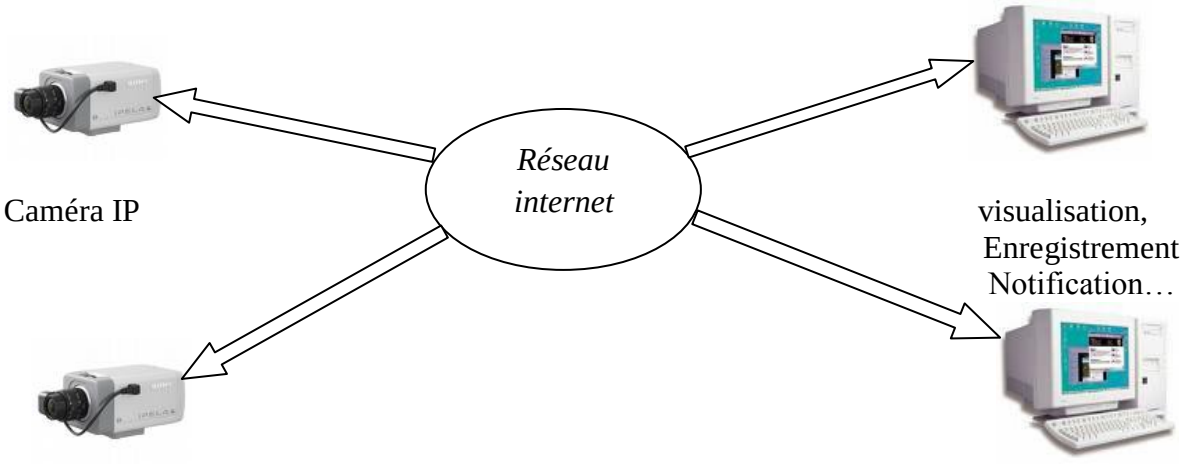

Figure 2.2 : Principe de base de la vidéosurveillance sur IP

Les spécificités du système que nous proposons de concevoir sont des cameras IP accessibles à distance. Ces cameras réseau offrent un moyen facile de visualiser et de diffuser des images vidéo de haute qualité sur tout type de réseau IP ou sur internet ce qui garantit encore l'efficacité et les performances de la solution proposée.

Dans le paragraphe suivant. Nous exposerons la conception du système de vidéosurveillance sur IP proposé.

2.3. Etude du système de vidéosurveillance sur IP

2.3.1. Vue globale sur le système

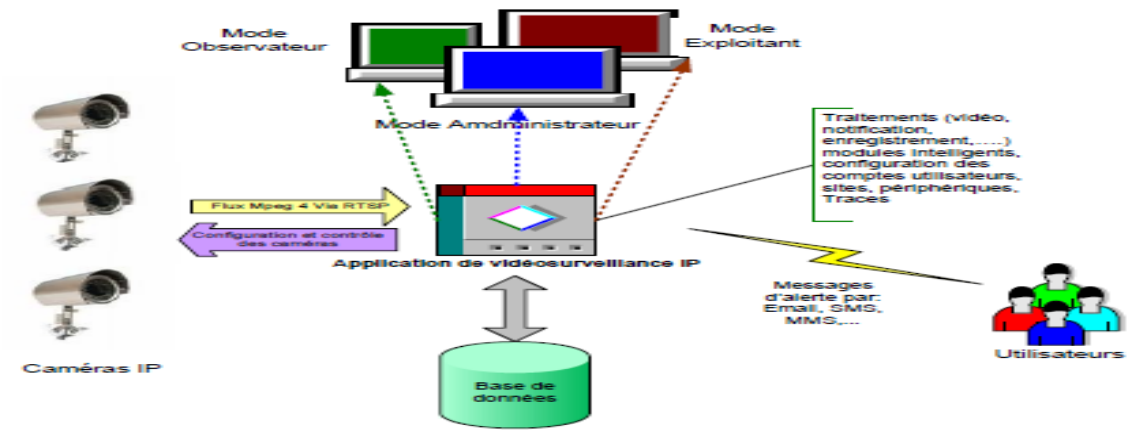

Figure 2.3: Vue globale du système de vidéosurveillance sur IP

Cette application de vidéosurveillance gère plusieurs caméras IP dont le nombre est limité par le débit et la bande passante du réseau Internet. Le flux vidéo sous le format MPEG-4 reçus au niveau du système peut être visualisé en direct ou bien enregistré sur disque dur pour une utilisation ultérieure. Plusieurs traitements peuvent être ainsi exécutés automatiquement par les modules intelligents disponibles ou bien manuellement par l'utilisateur du système. En effet, il existe trois catégories d'utilisateurs (Administrateur, Exploitant et Observateur) qui différent par leurs droits d'accès et d'utilisation du logiciel de vidéosurveillance. Notre application de vidéosurveillance peut aussi envoyer des messages de notification par Email, SMS ou MMS vers un ou plusieurs responsables de la sécurité des sites surveillés par les caméras IP.

Dans ce qui suit, nous allons spécifier les entrées, les sorties et les différentes fonctionnalités et modules de notre système de vidéosurveillance sur IP « NetCam Viewer ».

2.3.2. Choix de la méthode étudiée

Les méthodes de conception sont multiples dont chacune présente ses caractéristiques et ses outils. Parmi ces méthodes, Merise et UML. En effet, UML s'affirme comme un ensemble de formalismes pour la conception de logiciel à base de langage objet [12]. Cependant, Merise est plus tournée vers la compréhension et la formalisation des besoins du métier que vers la réalisation de logiciel.

Pour la conception de l'application, nous avons choisi l'approche orientée objet. En effet, cette approche fait désormais ses preuves et admet plusieurs avantages dont :

- Le système développé est plus facile à maintenir du fait que les objets sont indépendants. Ils peuvent donc être modifiés.

- Les objets sont considérés comme des composants réutilisables appropriés vu leur indépendance. On peut alors développer des conceptions à l'aide des objets créés dans une autre conception.
- Pour certaines classes du système, il existe une correspondance claire entre les entités du monde réel (tels que les composants matériels) et les objets du système qui les contrôlent ce qui permet d'améliorer la compréhension de la conception.

Pour la modélisation de notre application, on a choisi le langage UML (Unified Modeling Language) qui permet de modéliser un problème de façon standard. La modélisation UML consiste à créer une représentation simplifiée d'un problème, nommée modèle.

Comme outil de conception, nous avons utilisé « Rational Rose ». Dans le paragraphe qui suit, nous donnerons un aperçu sur les éléments de base du diagramme de cas d'utilisation et du diagramme de classes de notre système de vidéosurveillance sur IP.

2.3.2.1. Diagramme de cas d'utilisation

Les cas d'utilisation permettent de décrire les spécifications du système à réaliser. Pour établir le diagramme de cas d'utilisation, il faut procéder, comme première étape, à décrire le système à construire de l'extérieur, du point de vue utilisateur et fonctionnalités correspondants. Le diagramme de cas d'utilisation permet, ensuite, de représenter

visuellement une séquence d'actions réalisées par le système, produisant un résultat sur un acteur [13].

Les éléments de base d'un diagramme de cas d'utilisation sont les suivants :

a. Acteur

Un acteur, au sens UML, représente le rôle d'une entité externe (utilisateur humain ou non) interagissant avec le système. Il est représenté par un petit bonhomme.

b. Cas d'utilisation

Un cas d'utilisation (use case) est une unité cohérente d'une fonctionnalité visible de l'extérieur. Il réalise un service de bout en bout avec un déclenchement, un déroulement et une fin pour l'acteur qui l'initie. Un cas d'utilisation modélise donc un service rendu par le système sans imposer le mode de réalisation de service.

c. Relations entre cas d'utilisation

Trois types de relation standard entre cas d'utilisation sont proposés par UML :

• <<include>>: le cas d'utilisation incorpore explicitement et de manière obligatoire un autre cas d'utilisation à l'endroit spécifié,

• <<extend>>: le cas d'utilisation incorpore implicitement de manière facultative un autre cas d'utilisation à l'endroit spécifié,

• généralisation: les cas d'utilisation descendants héritent des propriétés de leur parent.

2.3.2.2. Diagramme de classes

Alors que le diagramme de cas d'utilisation montre un système du point de vue des acteurs, le diagramme de classes en montre la structure interne. Il décrit les classes que le système utilise, ainsi que leurs liens.

Une classe est une construction standard d'UML utilisée pour spécifier le scénario à partir duquel les objets seront fabriqués à l'exécution. Le modèle de classe permet de fournir une représentation abstraite des objets du système qui vont interagir ensemble pour réaliser les cas d'utilisation; il exprime aussi bien l'état statique que le comportement du système indépendamment d'un langage de programmation particulier.

2.3.3. Etude du système de vidéosurveillance sur IP

Dans cette section, nous abordons la conception de l'application. A partir de la définition des besoins, nous avons identifié les acteurs et leurs interactions avec le système, ce qui permet de déduire le diagramme de cas d'utilisation.

2.3.3.1. Diagramme de cas d'utilisation du système de vidéosurveillance sur IP

Les acteurs qui interviennent dans le système sont principalement :

- La caméra : c'est un acteur de base dans le système. c'est celle qui fournit la vidéo à distance via le réseau IP ou localement.
- L'administrateur : c'est l'utilisateur de plus de haut niveau. Il a un accès total au système. il est en fait le seul qui peut gérer les comptes d'utilisateurs. Dans la réalité, il représente l'entreprise qui conçoit et fournit le service de vidéosurveillance aux clients selon leurs besoins.
- L'exploitant : le client qui bénéficie de la solution de vidéosurveillance peut designer un responsable qui gère son système de vidéosurveillance, c'est l'exploitant. Il a un accès total à la version du système offerte par l'administrateur. En effet, il peut planifier les modes de notification, les calendriers d'enregistrement vidéo, la gestion de ses caméras, et l'aspect visuel de l'affichage vidéo.
- L'observateur : C'est l'utilisateur de plus bas niveau. Il ne permet que la visualisation directe de la vidéo en provenance des caméras, l'enregistrement en cas de détection visuelle d'anomalie et la notification selon le journal de planification qui lui a été confié par l'exploitant.

Entre ces trois derniers acteurs existe une relation d'héritage modélisée par la figure 2.4 :

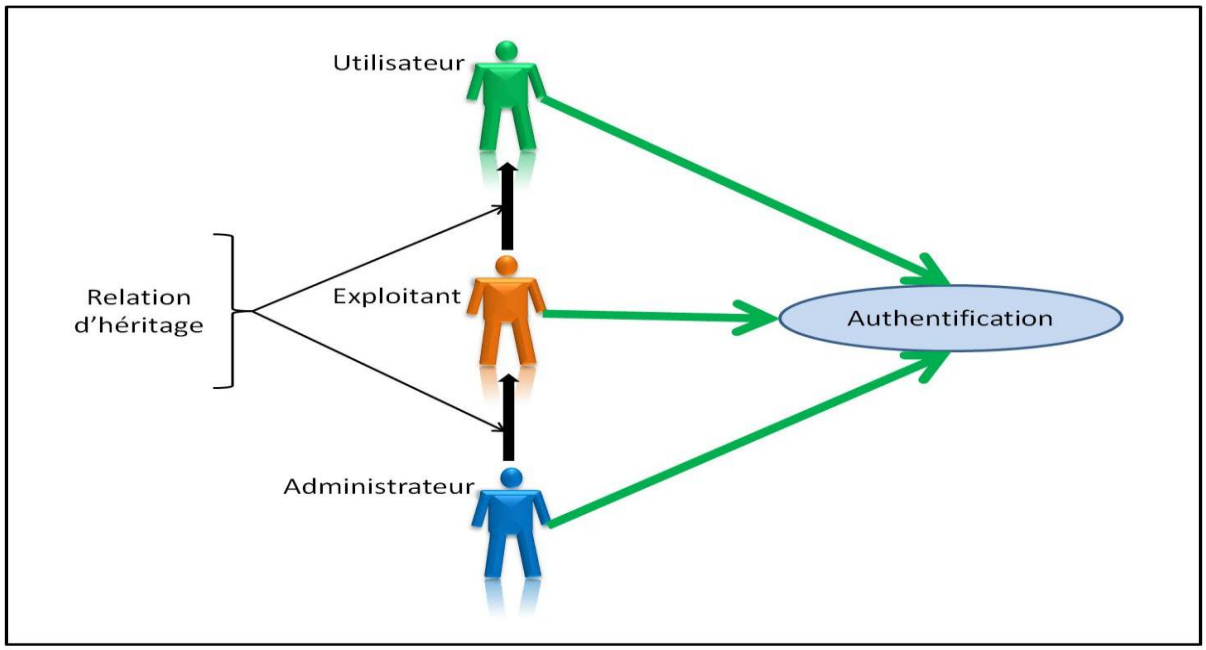

figure 2.4 : Relation d'héritage entre les acteurs

Les utilisateurs du système doivent s'authentifier à chaque tentative d'accès au système de vidéosurveillance. En fonction du résultat d'authentification, le système, en consultant les comptes d'utilisateurs, détermine à quel groupe (Administrateur, Exploitant, Observateur) appartient cet utilisateur qui vient d'en accéder. Selon le groupe, le système active ou désactive certaines fonctionnalités conformément aux droits attribués à chacun.
Dans le paragraphe suivant, nous décrirons en détail les différents cas d'utilisation du système de la vidéosurveillance.

i. Cas d'utilisation : « Gestion des Utilisateurs » et « Gestion des Sites »

L'administrateur du système (concepteur ou société de service) possède un accès total au système. En effet, selon les besoins et les contraintes du client, il lui fournit une version adaptée. Dans ce cas, il crée (modifie ou supprime) et gère les droits des comptes d'utilisateurs (exploitant et observateur) relatifs au service demandé par le client.

Et puisque le système est déterminé notamment en fonction de la nature du site à surveiller, de son mode d'exploitation (local ou distant, en temps réel ou différé, présence humaine ou non) et du budget possible, l'administrateur du système permet également de gérer les endroits surveillés par les caméras selon les demandes du client. Comme exemple de Relation d'héritage de cette administration, il indique le nombre nécessaire de caméras, enregistre leurs adresses IP dans la base de données, les responsables de leur contrôle, etc.

Notons que toute opération d'accès au système doit être précédées par une authentification pour déterminer les options à activer/désactiver selon le groupe auquel cet utilisateur appartient.

Ces deux tâches qu'on vient de noter sont modélisées par les cas d'utilisations suivants

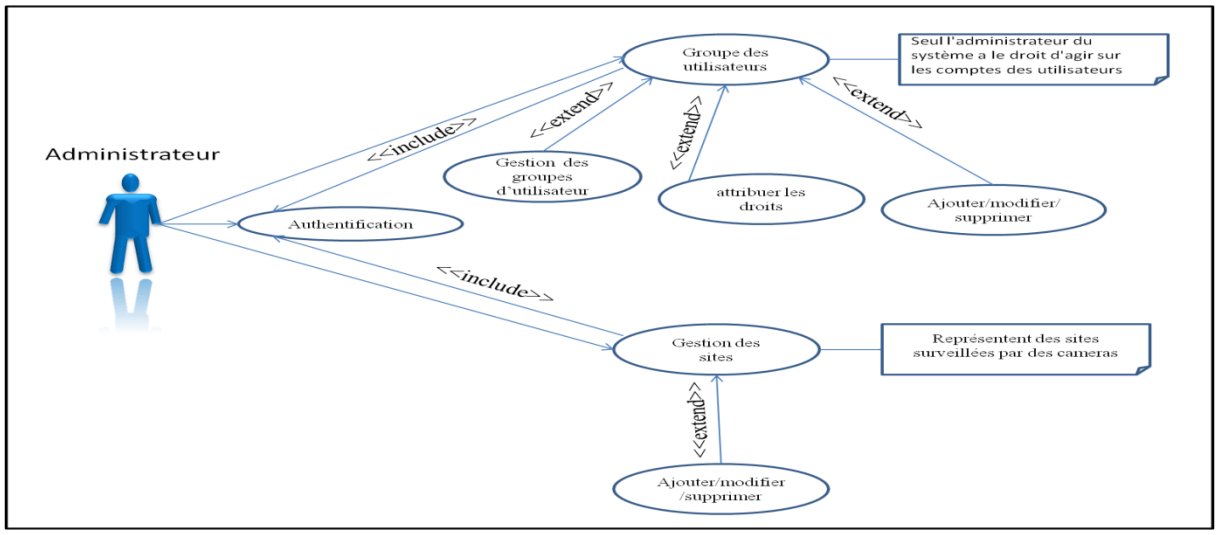

Figure 2.5 : Cas d'utilisation « Gestion des Utilisateurs » et « Gestion des sites »

ii. Cas d'utilisation : « Gestion de la base de données »

Le système de vidéosurveillance est couplé à une base de données contenant toutes les informations concernant les différents acteurs et l'historique des tâches exécutées sur le système tels que : les utilisateurs, les périphériques (généralement des caméras), les événements qui ont eu lieu ainsi que les notifications correspondantes, etc. Egalement, la base de données contient les

vidéos enregistrées des différentes caméras. Le cas d'utilisation qui modélise l'opération de gestion de la base de données est représenté par la figure 2.6.

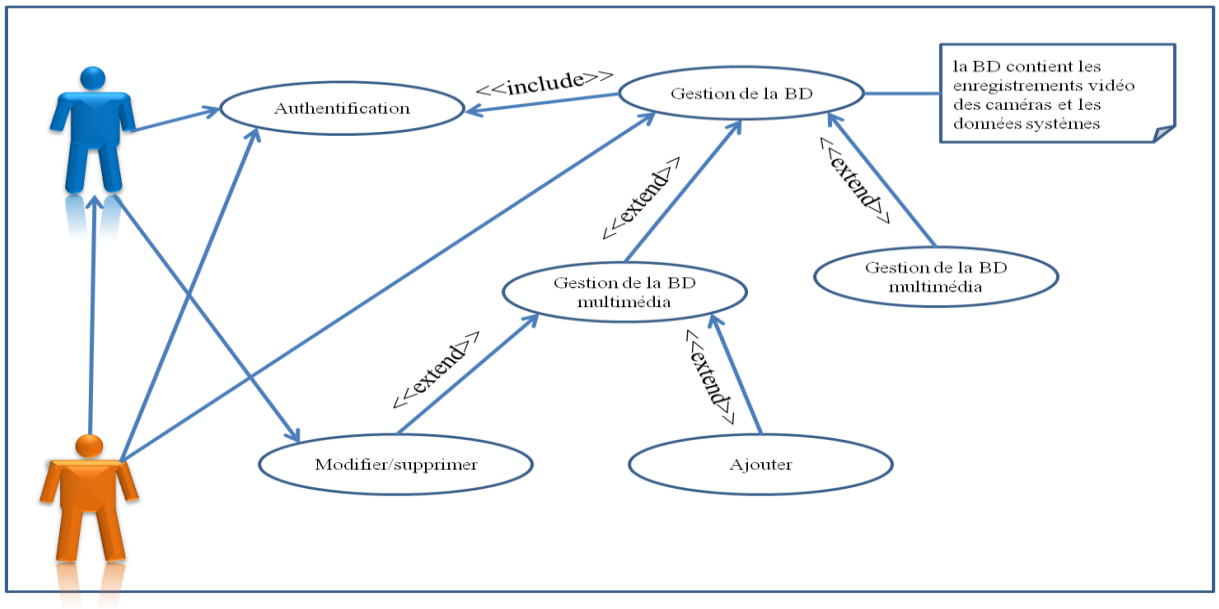

Figure 2.6 : Cas d'utilisation « Gestion de la base de données»

L'administrateur peut effectuer toute opération possible sur la base de données alors que l'exploitant ne peut que consulter ou supprimer les enregistrements antérieurs.

iii. Cas d'utilisation : « Gestion des périphériques »

Les périphériques attachés à un système de vidéosurveillance dépendent des besoins du client et de la complexité du site à surveiller. Ils sont généralement des caméras IP, capteurs, sirènes, etc. La configuration et le traitement des données relatives à ces éléments sont normalement à la charge de l'administrateur du système (lors de la fourniture de la solution au client) puis déléguées à l'exploitant qui peut à tout moment configurer, commander à distance, activer ou désactiver les caméras disponibles dans son système.

L'opération de gestion des périphériques est modélisée par la figure 2.7.

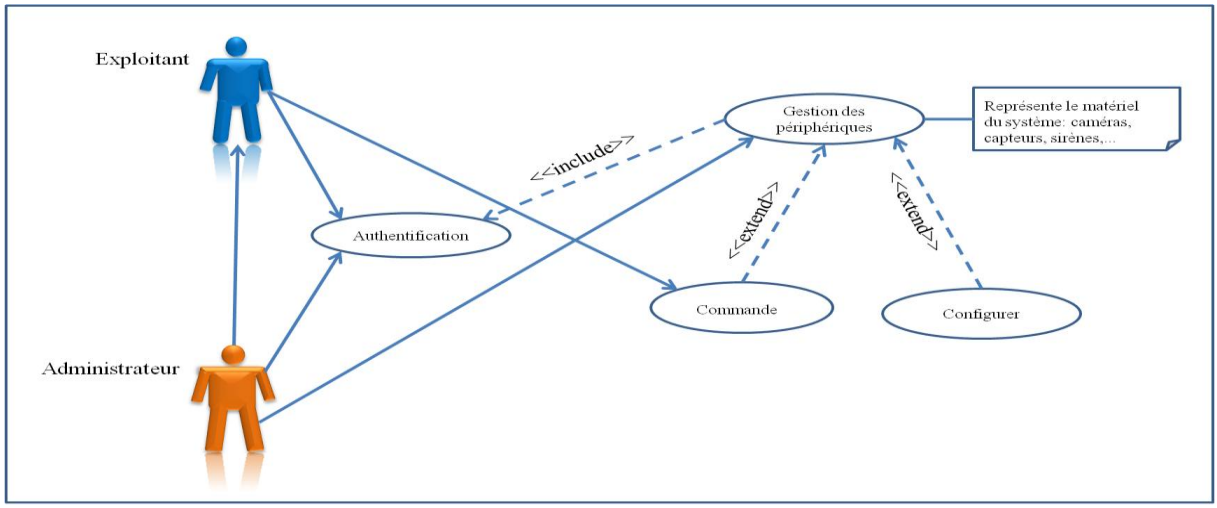

Figure 2.7 : Cas d'utilisation « Gestion des périphériques »

iv. Cas d'utilisation : « Planifier »

La planification est une tâche nécessaire pour organiser et alléger la tâche de l'utilisateur et du système. Il s'agit de planifier les alarmes (par Email, SMS, MMS), du calendrier d'enregistrements (Continu, planifié ou sur alarmes) et des modules de traitement intelligents.

L'administrateur peut effectuer toutes les opérations de planification. L'exploitant ne peut planifier que ce qui est disponible dans sa version

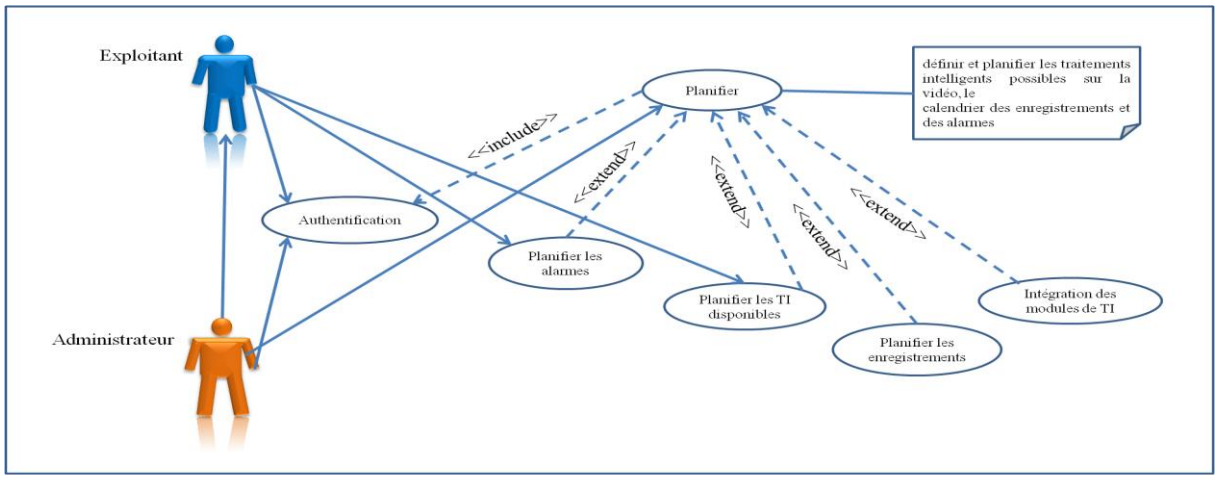

Figure 2.8 : Cas d'utilisation « Planifier »

v. Cas d'utilisation : « Visualiser »

Cette opération inclut la visualisation en direct de la vidéo en provenance des caméras, la consultation ou la lecture des séquences vidéo préenregistrées sur disque dur. Egalement l'utilisateur (quelque soit sa catégorie) peut configurer le nombre d'écran d'affichage et la détection des anomalies visuellement.

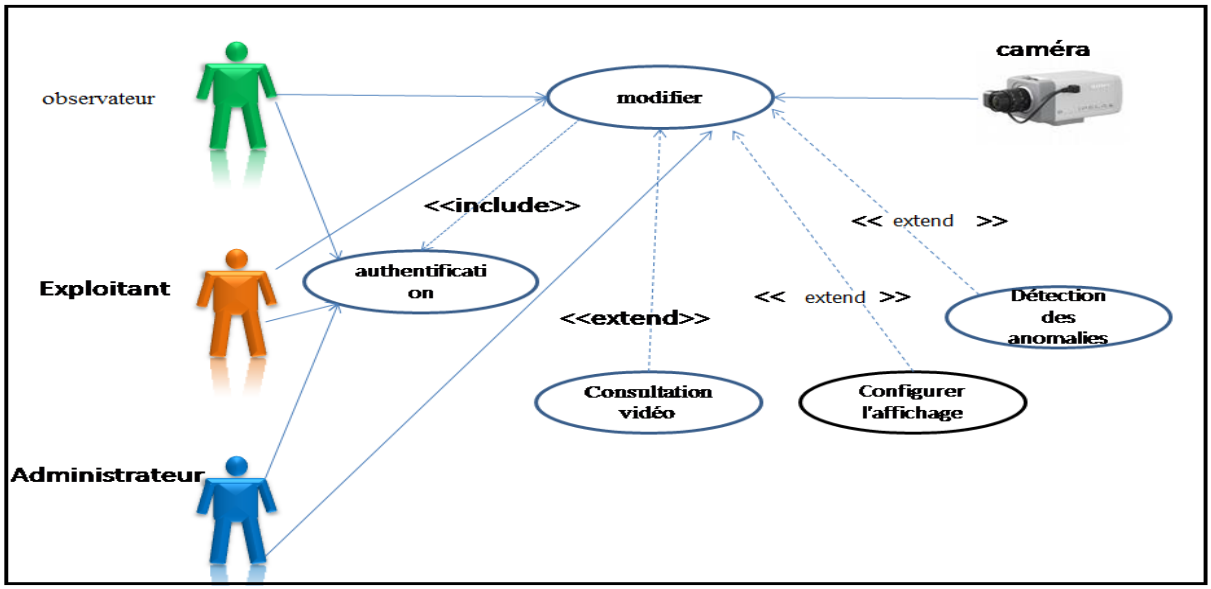

Figure 2.9 : Cas d'utilisation «*Visualisation* »

vi. Cas d'utilisation : « Notification »

La notification concerne essentiellement l'envoie et la réception, l'acquittement et l'archivage des messages d'alerte. Le système peut aussi garder un historique horodaté de tout avertissement émis par le système ainsi que l'agent responsable de cette tâche. Ce fichier ne peut être consulté que par

l'administrateur ou bien l'exploitant du système.

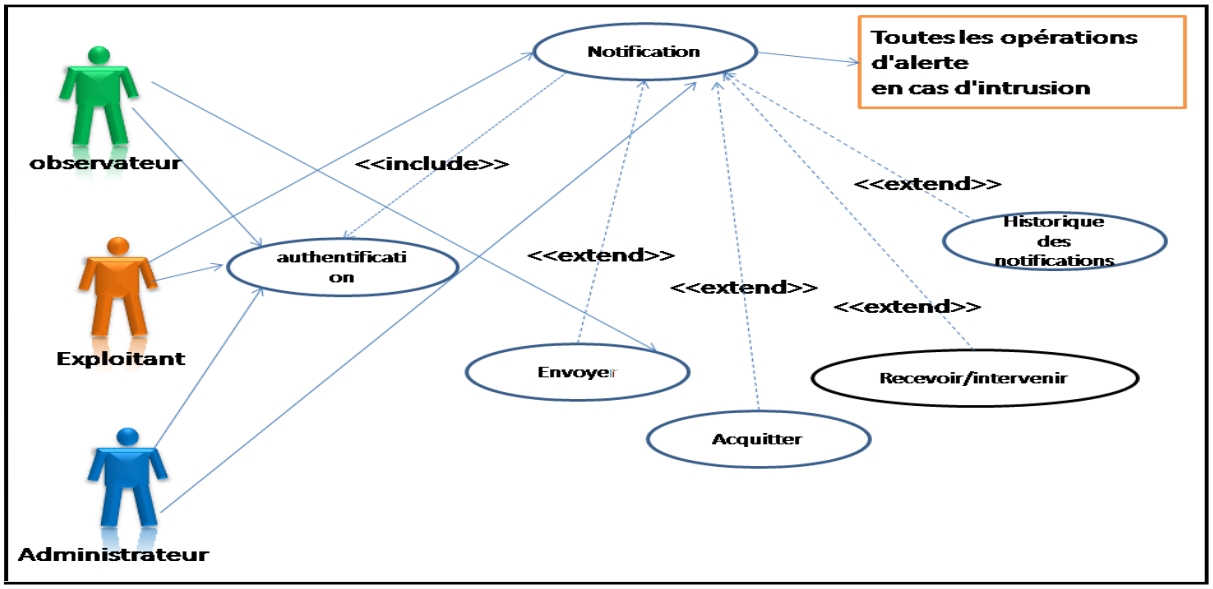

Figure 2.10 : Cas d'utilisation « Notification »

vii. Cas d'utilisation : «Authentification »

Il faut noter que lors de l'accès au système pour effectuer l'une des opérations précédentes, il faut tout d'abord s'authentifier. Un fichier contenant la trace des accès au système est gardé en secret et ne peut être consulté que par l'administrateur.

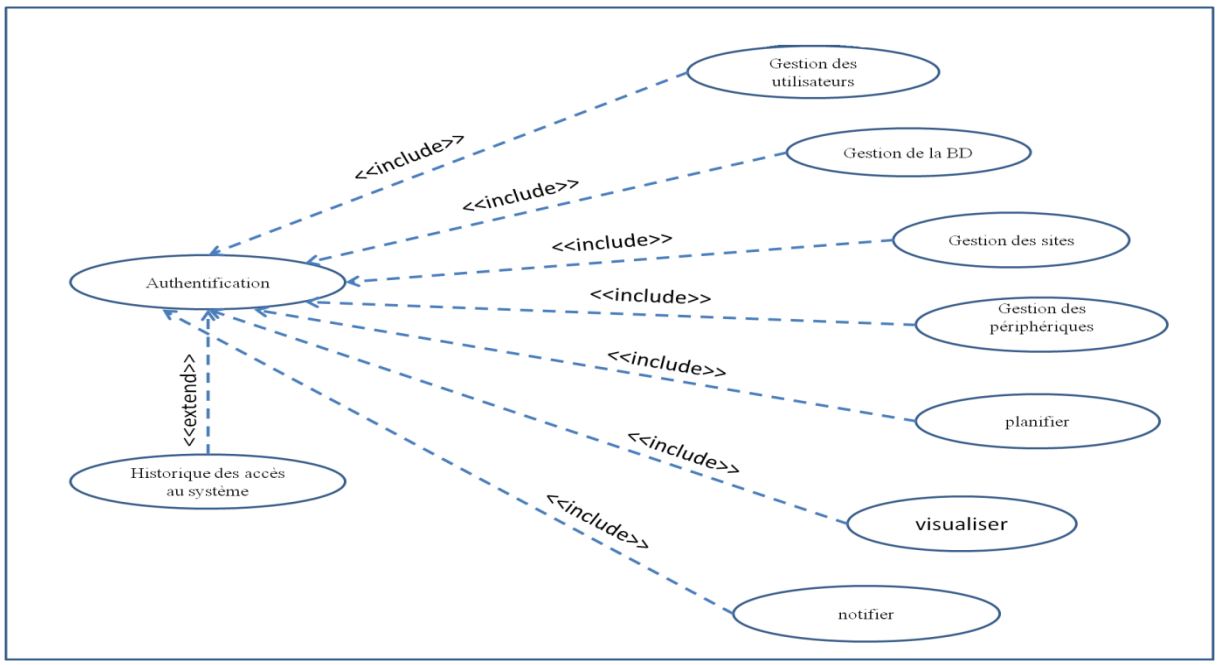

Figure 2.11 : Cas d'utilisation « Authentification »

En résumé, notre solution vise à offrir les fonctionnalités de base d'un système de vidéosurveillance. Ces fonctions sont personnalisées selon les besoins du client et selon la catégorie de son utilisateur. Le schéma global du système de vidéosurveillance est donné par la figure 2.12.

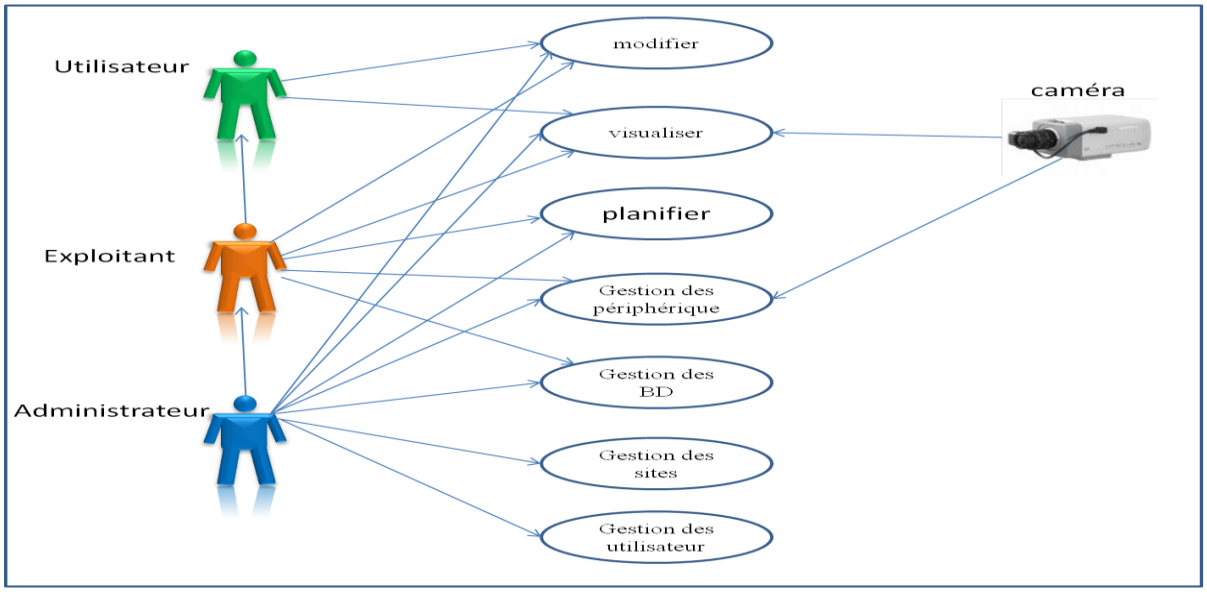

Figure 2.12 : Diagramme de cas d'utilisation du système de vidéosurveillance

Le diagramme de cas d'utilisation qu'on vient de présenter nous permettra, dans une deuxième étape, de réaliser les diagrammes de classe.

2.3.3.2. Diagramme de classe du système de vidéosurveillance sur IP

Le diagramme de classe donne une représentation optimale et cohérente des données de notre système de vidéosurveillance, il est représenté par la figure 2.13.

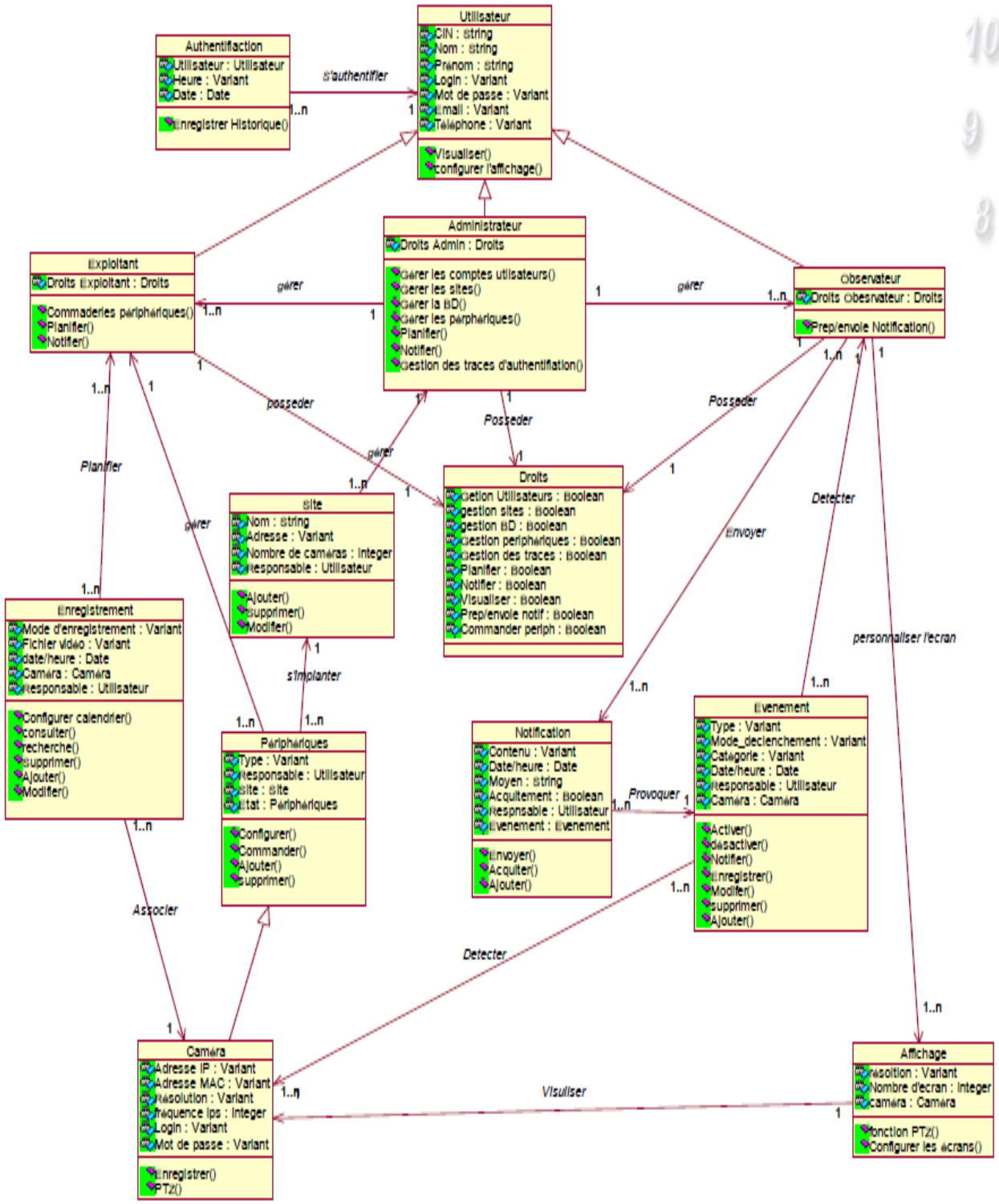

Figure 2.13 : Diagramme de classe du système de vidéosurveillance sur IP (NetCam Viewer)

Le diagramme de classe contient les classes suivantes :

- ✓ *Utilisateur* de la quelle hérite les trois niveaux (Administrateur, Exploitant ou Observateur) selon les prérogatives sur le système.

- ✓ *Droits* : cette classe contient les groupes de privilèges des catégories d'utilisateurs.
- ✓ A*uthentification* : cette classe définit quels utilisateurs ont le droit d'accéder au système en vérifiant les paramètres par rapport à la liste enregistrée dans la base de données. Elle permet de garder en mémoire un fichier log horodaté de toute tentative d'accès au système.
- ✓ *Enregistrement* : Cette classe gère l'archivage des données système et les séquences vidéo prises par les différentes caméras surveillées selon les calendriers configurés.
- ✓ *Site* : Cette classe gère les paramètres des endroits surveillés par le système de vidéosurveillance sur IP.
- ✓ P*ériphériques* : Cette classe définit les paramètres et les traitements sur les composantes qui interagissent avec le système comme les capteurs, les sirènes, etc.
- ✓ *Caméras* : la classe caméra hérite de la classe périphérique ; elle permet de gérer tous les traitements spécifiques aux caméras réseaux qui assurent la surveillance et le contrôle à distance.
- ✓ E*vénement* : Elle définit les paramètres des alertes et des anomalies qui ont été détectés par les acteurs du système et effectue tous les traitements possibles.
- ✓ *Notification* : Une fois détecté un nouvel événement, le système initialise toute une procédure d'avertissement gérée par cette classe de Notification.
- ✓ *Affichage* : C'est une classe qui effectue un traitement basique et nécessaire à tout système de vidéosurveillance et de contrôle distant. Cette opération est personnalisée selon les préférences et les dispositions de l'utilisateur du système.

Après l'élaboration du diagramme de classes, nous allons passer à l'étude de la base de données de notre application.

L'étude de la base de données passe l'élaboration de modèle conceptuel de données (MCD) puis le modèle relationnel ou modèle logique (MLD).

Le MCD est modèle très semblable au diagramme de classe déjà proposé. En fait, quand on fait un diagramme de classes en UML, on peut considérer que l'on a fait un MCD. C'est pour cette raison, lors de la présentation de notre base de données, nous se limiterons uniquement au modèle logique qui fera l'objet du paragraphe suivant.

2.3.4. Etude de la base de données

2.3.4.1. Le modèle Logique de Données (MLD)

Le MLD, également nommé schéma relationnel, est un deuxième niveau d'abstraction qui permet un haut niveau d'abstraction des données. Il fournit une base solide pour traiter les problèmes de cohérence des données en supportant des contraintes d'intégrité.

Comme SGBD (Système de Gestion de Base de Données), nous avons choisi la plateforme SQL Server 2005. Cet outil permet le développement et le débogage de bases de données de classe d'entreprise [14]. Notre choix est justifié par deux raisons principales :

- ✓ Le moteur de bases de données SQL Server 2005 dispose d'un stockage sécurisé et fiable et structurés pour les données relationnelles ce qui permet de créer et de gérer des applications de données performantes.
- ✓ SQL Server 2005 permet une interaction étroite avec Visual Studio 2005, que nous allons utiliser pour le développement de notre logiciel, vue qu'ils font partie de la même plateforme (Visual Studio .Net) de *Microsoft*.

Le modèle relationnel, représenté par la figure 2.14, contient la liste des tables qui construisent la base de données de notre système et la base de données vidéo. Les tables sont les suivantes :

- ✓ Utilisateur : représente un utilisateur du système de vidéosurveillance sur IP.

- ✓ Site : représente un site surveillé par une ou plusieurs caméras IP.
- ✓ Périphérique : c'est l'ensemble des équipements qui assurent la visualisation (caméras), la détection (capteur) et la notification (sirène).
- ✓ Notification : représente le message d'alerte émis vers un ou plusieurs utilisateurs.
- ✓ Authentification : cette entité décrit une opération d'accès au système de vidéosurveillance par un utilisateur donné.
- ✓ Enregistrement : représente un archivage vidéo à partir d'une caméra donnée.
- ✓ Planification : représente une configuration du mode de fonctionnement du système de vidéosurveillance.
- ✓ Type Utilisateurs: c'est une description des droits des utilisateurs ; c'est-à-dire les opérations autorisées à un utilisateur donné.
- ✓ Evènement : elle contient la liste des évènements détectés par le système.

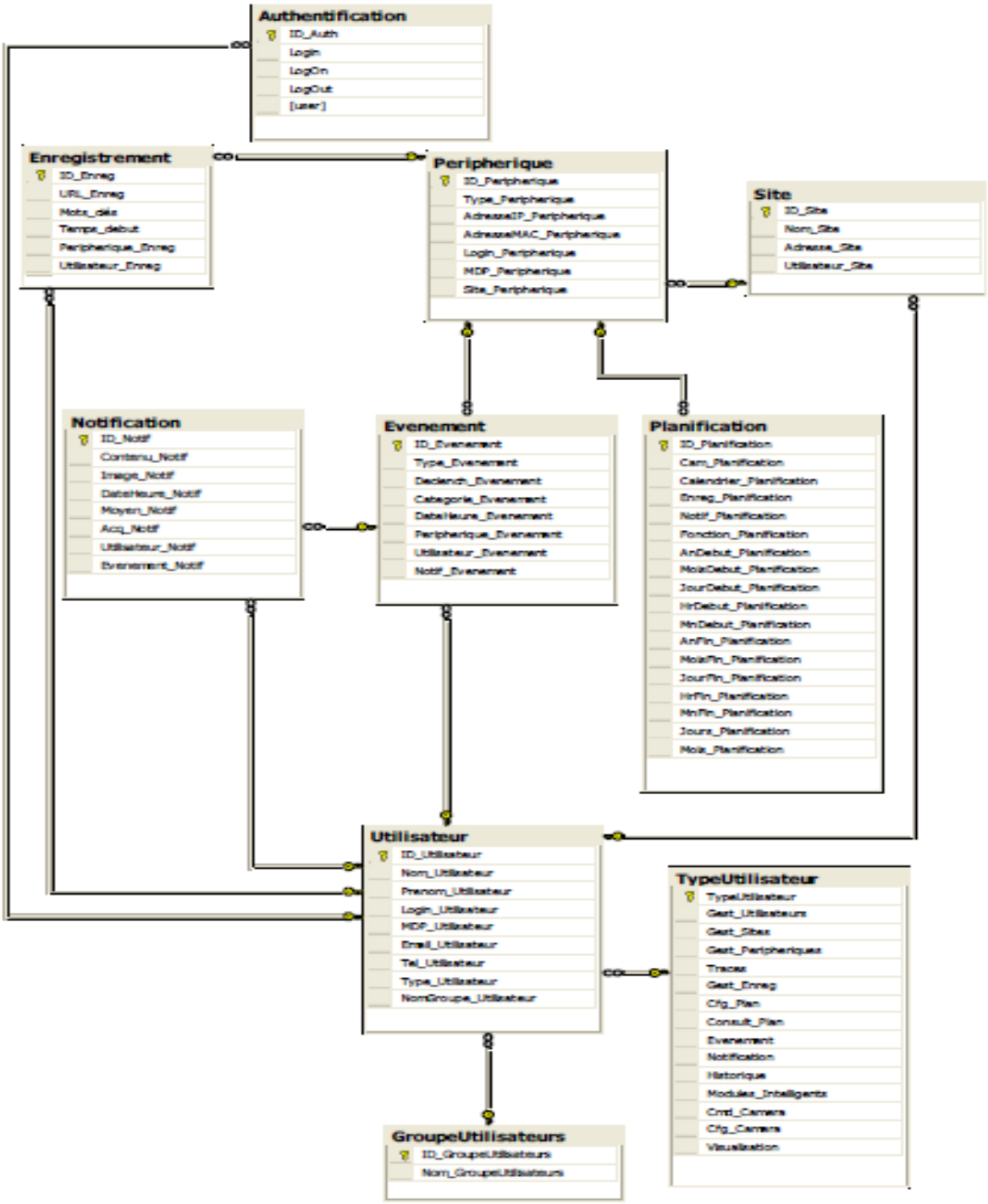

Figure 2.14 : MLD de la base de données

2.3.4.2. Dictionnaire de données

Le dictionnaire de données donne une représentation sémantique des différentes entités d'une base de données [15]. Il contient l'ensemble des tables composantes de la base.

i. Dictionnaire des données

Pour assurer la lisibilité du dictionnaire, nous l'avons établit sous forme d'un tableau. Il comporte les champs des différentes entités (tables) de la base. Une description est aussi associée à chaque code du dictionnaire. Le dictionnaire correspondant à la base de données du système de vidéosurveillance sur IP est représenté en annexe A.

ii. Description des objets de la base de données

Les tables du dictionnaire de données peuvent être consultées via des requêtes SQL.

Elles permettent à l'utilisateur de voir les objets qui lui appartiennent. La liste des objets constitutifs de la base de données du système de vidéosurveillance sur IP est détaillée par le tableau exposé par l'annexe B.

2.4. Conclusion

Dans ce chapitre, nous nous sommes intéressés à l'analyse des besoins et l'étude de notre système de vidéosurveillance sur IP. En effet, dans une première étape, nous avons analysé les besoins et établit les spécifications du système de vidéosurveillance proposé.

Ensuite, nous avons défini les différentes entités du système ainsi que la manière d'interaction entre elles grâce à une représentation simplifiée et compréhensible moyennant le modèle UML. Cette logique nous a permis, enfin, de concevoir la base de données relative à notre système. Dans le chapitre suivant, nous nous intéresserons à l'implémentation et la réalisation des fonctionnalités du système.

Chapitre 3

Mise en œuvre des fonctionnalités d'affichage et d'alerte du système de vidéosurveillance sur IP

3.1. Introduction

Dans ce chapitre, nous allons présenter, tout d'abord, l'environnement de développement que nous avons utilisé pour l'implémentation de notre solution. Par la suite, nous nous intéresserons à décrire cette phase, puis présenter les résultats de notre contribution.

3.2. Organigrammes de fonctionnement du système

La vidéosurveillance sur IP offre des fonctionnalités multiples et intéressantes que ce soit pour un simple utilisateur ou une entreprise ; c'est dans le cadre de cette section que nous exposerons, sous forme d'organigrammes et d'interfaces, les fonctionnalités globales et spécialement celles de l'affichage et d'alerte relatives à notre système de vidéosurveillance sur IP « NetCam Viewer ».

3.2.1. Organigramme général du système

La sécurité d'un système de vidéosurveillance est une notion fondamentale et nécessaire vue que la vidéo provenant des caméras distantes peut contenir des informations secrètes concernant la sécurité des biens et des personnes.

Dans l'élaboration de notre solution, nous avons pris en compte ce point fondamental.

En effet, nous avons mis en jeu une procédure de sécurité au niveau de la couche application du modèle OSI (Open System Interconnexion) ; c'est la phase d'authentification des utilisateurs. Une fois cette phase est validée, les fonctionnalités de vidéosurveillance peuvent être accessibles à l'utilisateur qui en vient de réussir l'authentification.

Les opérations de vidéosurveillance qu'offre notre application sont principalement :

- L'affichage de la vidéo préenregistrée ou bien en direct (Live).

- La détection des alarmes
- La notification des responsables en cas d'alarme.
- La gestion et la mise à jour des événements qui ont eu lieu ainsi que leurs notifications.
- La planification des enregistrements et des alarmes.
- La configuration des comptes d'utilisateurs, des sites, des périphériques, des modules intelligents.
- La gestion des traces ou les « log files » d'utilisation du système.

Pour tout autre renseignement concernant le système ou bien son utilisation, nous exhiberons aussi les deux fenêtres respectives « A propos » et « Aide ».

L'organigramme de la figure 3.1 donne une hiérarchie globale du fonctionnement de notre système de vidéosurveillance sur IP.

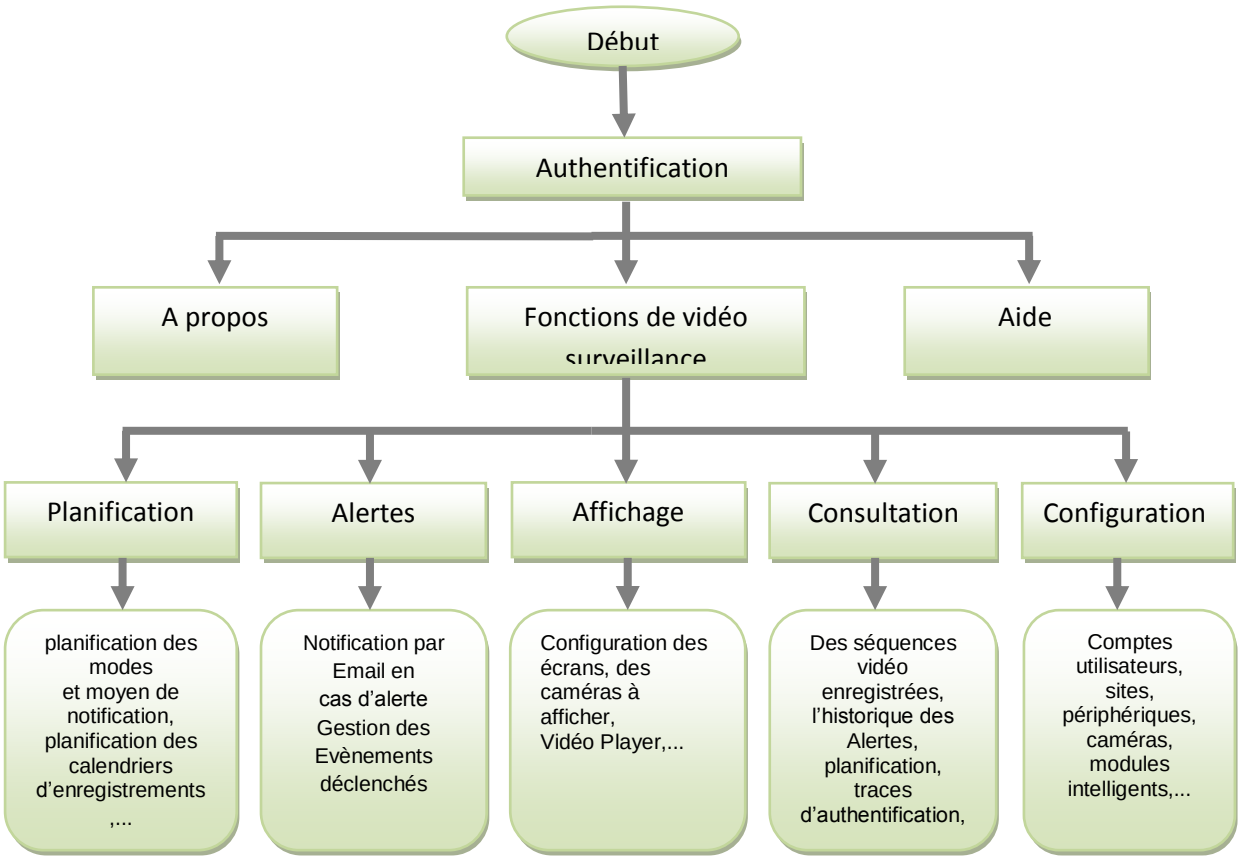

Figure 3.1 : Organigramme général du « NetCam Viewer »

Dans le cadre de notre travail, nous nous sommes focalisé sur les opérations d'affichage et d'alerte. En effet, il s'agit, d'une part, d'afficher les caméras IP de vidéosurveillance en direct, d'enregistrer la vidéo en provenance de ces caméras et de consulter les séquences enregistrées. D'autre part, le système prévoit une procédure de notification en cas d'alarme et de gestion des événements détectés.

3.2.2. Modes d'utilisation du système

Le système de vidéosurveillance sur IP réalisé offre trois modes d'exploitation selon que l'utilisateur qui en utilise est un administrateur, exploitant ou un observateur comme le montre l'organigramme de la figure 3.2.

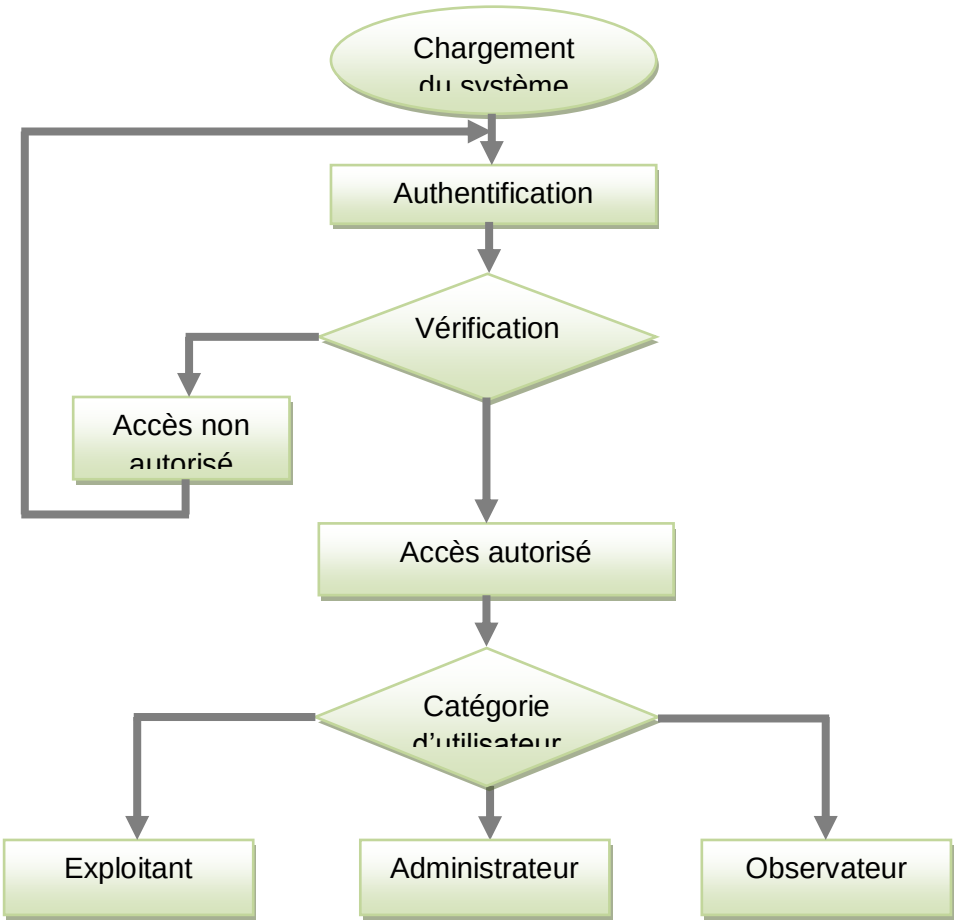

Figure 3.2 : Modes d'exploitation du système

3.2.2.1. Mode Administrateur

Le mode Administrateur est utilisé lors de la configuration initiale du système, lorsque de nouvelles caméras sont installées et chaque fois que la configuration doit être modifiée. Il est aussi utilisé pour la configuration de l'affichage du moniteur, des conditions d'enregistrement, etc.

3.2.2.2. Mode Exploitant

Le mode Exploitant est un mode dérivé du mode Administrateur. L'exploitant configure et gère toutes les fonctionnalités autorisées par l'administrateur c'est-à-dire toutes les fonctionnalités à l'exception de la configuration des comptes utilisateurs.

3.2.2.3. Mode Observateur

Le Mode moniteur n'autorise que les fonctionnalités d'affichage en direct des caméras installées, la détection des alarmes, leur notification et la mise à jour des événements déclenchés.

3.3. Environnement de réalisation

L'environnement de réalisation englobe les matériels, les logiciels ainsi que les outils de développement que nous avons utilisé pour l'élaboration du logiciel de vidéosurveillance.

3.3.1. Matériels et Logiciels

- Deux caméras IP de « Analog Devices » ayant les adresses IP respectives :

192.168.1.31 et 192.168.1.61 ;

- Un Ordinateur portable de marque HP.
- Un réseau local Ethernet 100 Mbits/s.
- Système d'exploitation : Windows 7.
- Système de Gestion de base de données : SQL Server 2005.

3.3.2. Outils de développement

- Rational Rose : outil d'aide à la conception.
- Visual Studio 2005 et précisément l'environnement C# pour le développement de l'application.

3.3.3. Présentation de la plateforme de développement : Visual C#

Pour concevoir des applications et des projets, C Sharp met en œuvre des concepteurs de fenêtres et d'outils [16] :

- *Toolbox*: La boîte à outils contient des composants et des contrôles utilisés pour créer des applications Windows. Les contrôles sont regroupés dans des catégories portant des noms logiques tels que Menus et barres d'outils (Menus and Toolbars), Data (Données), Dialogs (Boîtes de dialogue),...
- *Fenêtre Properties*: La fenêtre Propriétés nous permet d'afficher et de modifier les propriétés et les événements de composants de notre application. On peut également utiliser cette fenêtre pour ajouter ou mettre à jour un formulaire et pour contrôler les événements de ces composants.
- *Explorateur du projet* : contient tous les composants logiques d'un projet telle que les bibliothèques utilisées (References), les fenêtres conçues y compris leur dessinateur (designer) et leur code (Nom_fenêtre.cs), le programme principal (program.cs)

L'environnement de développement C # est présenté par la figure 3.3.

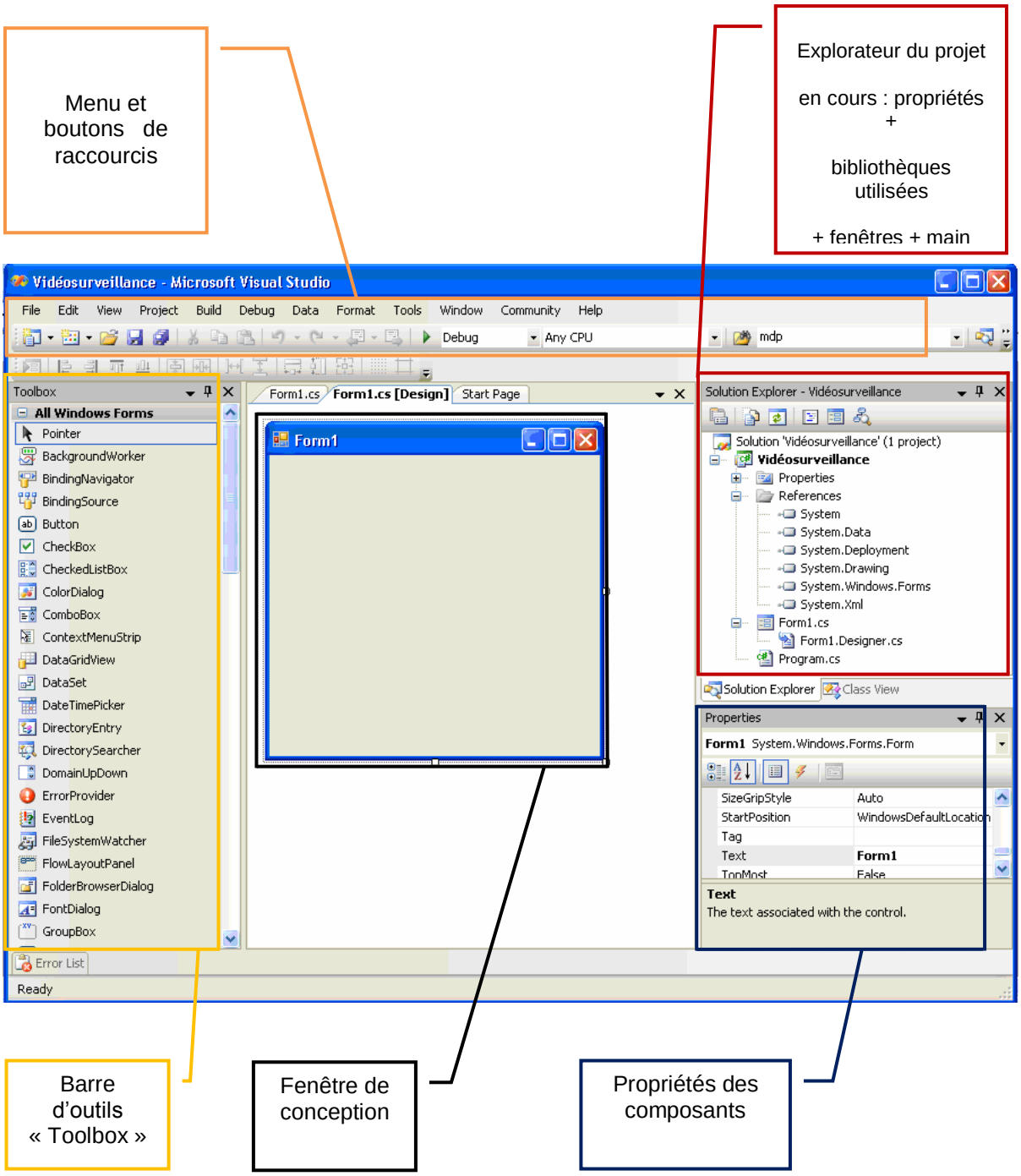

Figure 3.3 : Environnement de développement C #

Visual C# Express offre une aire de conception visuelle puissante qui permet de créer rapidement et facilement des applications Windows interactives [16].

3.3.4. Structure générale d'un programme C#

Selon le modèle UML, après analyse des besoins et la conception, nous passons à la phase codage et test. En programmation, le code est présenté selon l'approche Orientée Objet qui consiste à coder les différentes unités du modèle conceptuel en des classes. Ces programmes unitaires seront ensuite exécutés lors de l'appel à leurs constructeurs dans le programme principal ou lors de l'interaction entre les différentes classes du projet. C#, étant un langage de développement basé sur l'approche Orientée Objet, suit cette logique. En effet, la structure générale et basique d'un programme codé en C# est présentée par la figure 3.4.

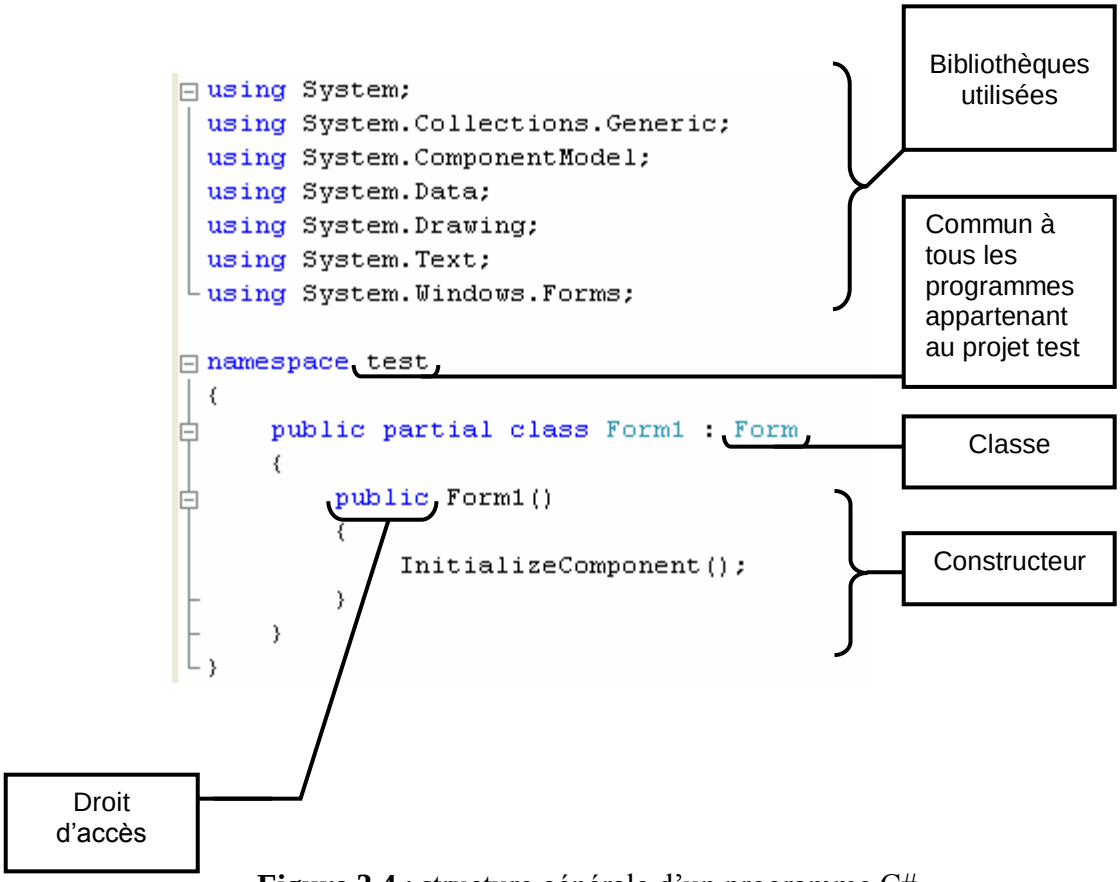

Figure 3.4 : structure générale d'un programme C#

3.4. Intégration du composant Quick time

Comme nous avons précisé dans le premier chapitre, le protocole de streaming utilisé par les caméras IP utilisées est le RTSP. Les requêtes et les

options de streaming de ce protocole ne sont pas implémentés dans l'environnement C# à l'inverse de celui de http. De ce fait, pour pouvoir lire et traiter la vidéo en provenance des caméras IP, nous nous sommes orientés à l'intégration d'un composant ou d'un DLL qui implémente ces fonctions de streaming. Et puisque, le logiciel Quick time offre ces besoins, nous l'avons intégré comme composant dans l'environnement C#. Cette opération rend possible d'utiliser les options offertes par Quick time comme celle de la lecture, pause, arrêt de la vidéo en direct ou bien en différé.

3.5. Présentation des interfaces réalisées

Dans cette section, nous présenterons les interfaces qui assurent les fonctionnalités d'affichage et d'alerte du système de vidéosurveillance. Nous avons essayé de concevoir des interfaces conviviales et simples à comprendre et à utiliser quelque soit le niveau de l'utilisateur. Ces interfaces, classées selon le rythme chronologique de l'exécution des tâches, sont présentées ci-après.

3.5.1. Fenêtre de lancement du logiciel

Lors du chargement ou du lancement du logiciel pour l'exécution, la fenêtre 3.5 s'affiche temporairement. Elle donne un aperçu sur le thème et le nom du système et le nom de la société de service.

Figure 3.5 : Fenêtre de démarrage du NetCam Viewer

Une fois le chargement du système est terminé, l'exécution des fonctionnalités autorisées à l'utilisateur courant est conditionnée par le résultat de l'authentification.

3.5.2. Fenêtre d'authentification des utilisateurs

Comme indiqué précédemment, pour accéder au système de vidéosurveillance, tout utilisateur est appelé à passer par la procédure traditionnelle d'authentification à travers la fenêtre de la figure 3.6.

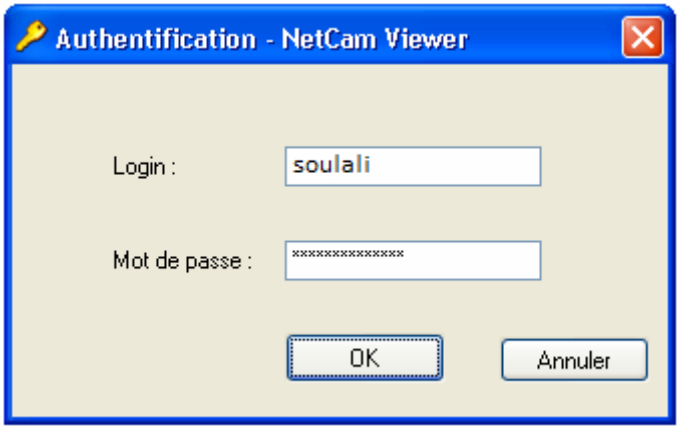

Figure 3.6 : Fenêtre d'authentification

En effet, l'opérateur saisit son login et son mot de passe et le système consulte la base de données du compte d'utilisateurs et vérifie les paramètres saisis. S'il y'a conformité, il affiche la fenêtre principale du logiciel, si non il indique qu'il y'a une erreur de login ou de mot de passe.

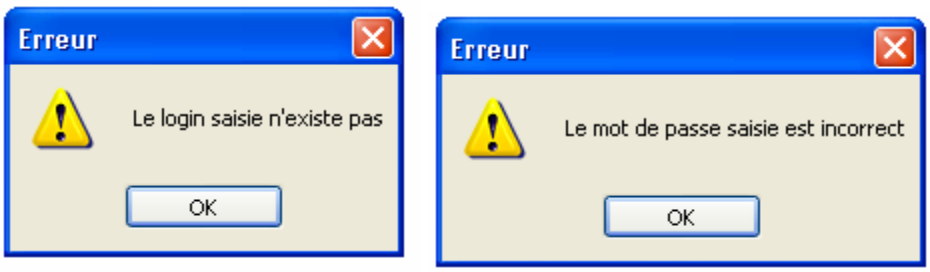

Figure 3.7 : Erreur d'authentification

3.5.3. Fenêtre Principale

Cette fenêtre donne accès aux fonctionnalités de vidéosurveillance. Elle contient un menu et un ensemble de boutons de raccourcis. Elle est aussi adaptée à la catégorie d'utilisateur.

La figure 3.8 expose la fenêtre principale du logiciel « NetCam Viewer » développé.

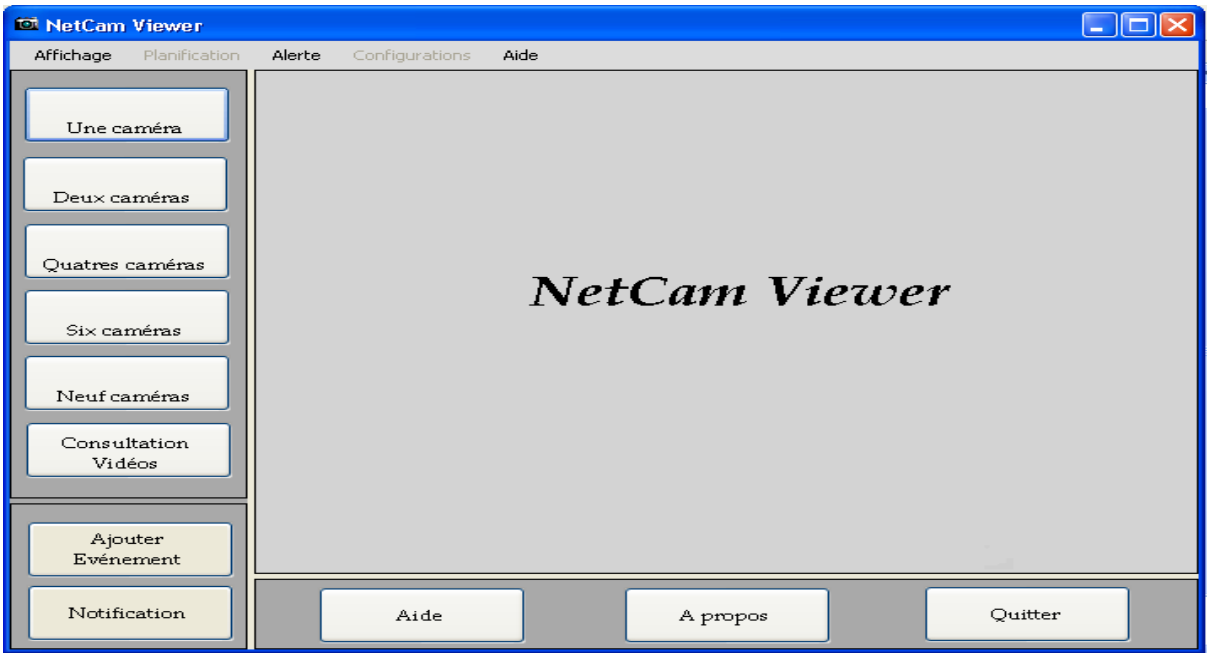

Figure 3.8 : Fenêtre principale du NetCam Viewer

Les menus concernant les fonctionnalités d'affichage et d'alerte de cette fenêtre sont détaillés par la figure 3.9.

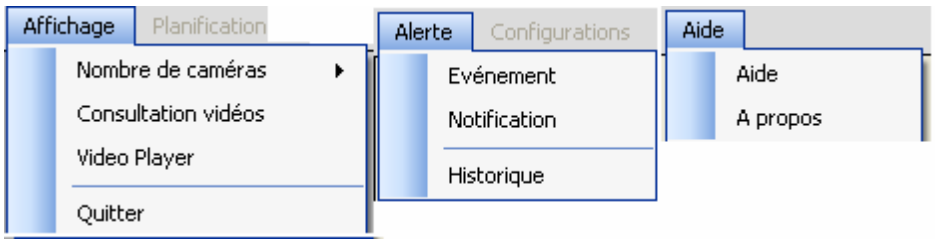

Figure 3.9 : Menus d'affichage, d'alerte et d'aide du NetCam Viewer

Dans la section suivante, nous présenterons les interfaces correspondantes aux menus d'affichages, d'alerte et d'aide.

3.5.4. Fonctions d'affichage

3.5.4.1. Affichage des caméras en direct

Pour surveiller un site particulier, on doit indiquer l'adresse IP de la caméra à visualiser puis ordonner la lecture. Si la caméra est connectée, elle répond en transmettant la vidéo capturée. Selon les disponibilités, on peut avoir l'affichage d'une seule caméra individuelle jusqu'à 9 caméras simultanées. Dans ce qui suit, nous exposerons un panorama des fenêtres de visualisation directes des caméras distantes avec deux caméras IP disponibles (ayant les adresses : 192.168.1.33 et 192.168.1.61).

Pour la visualisation d'une seule caméra, l'utilisateur devra accéder à la fenêtre représentée par la figure 3.10.

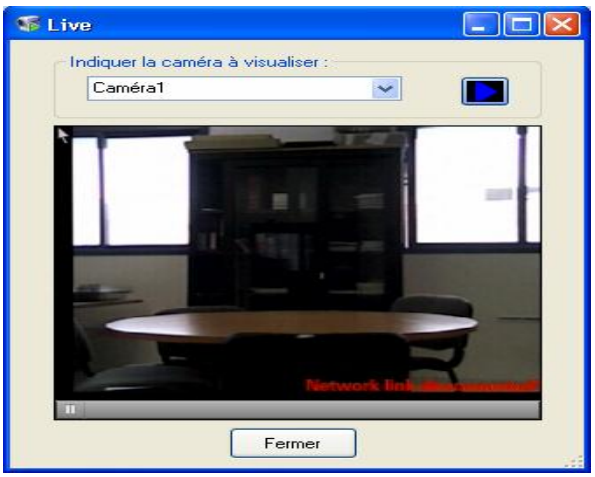

Figure 3.10 : Affichage d'une seule caméra

Les figures 3.11, 3.12, 3.13 et 3.14 représentent respectivement les écrans de visualisation de deux, quatre, six et neufs caméras IP simultanément.

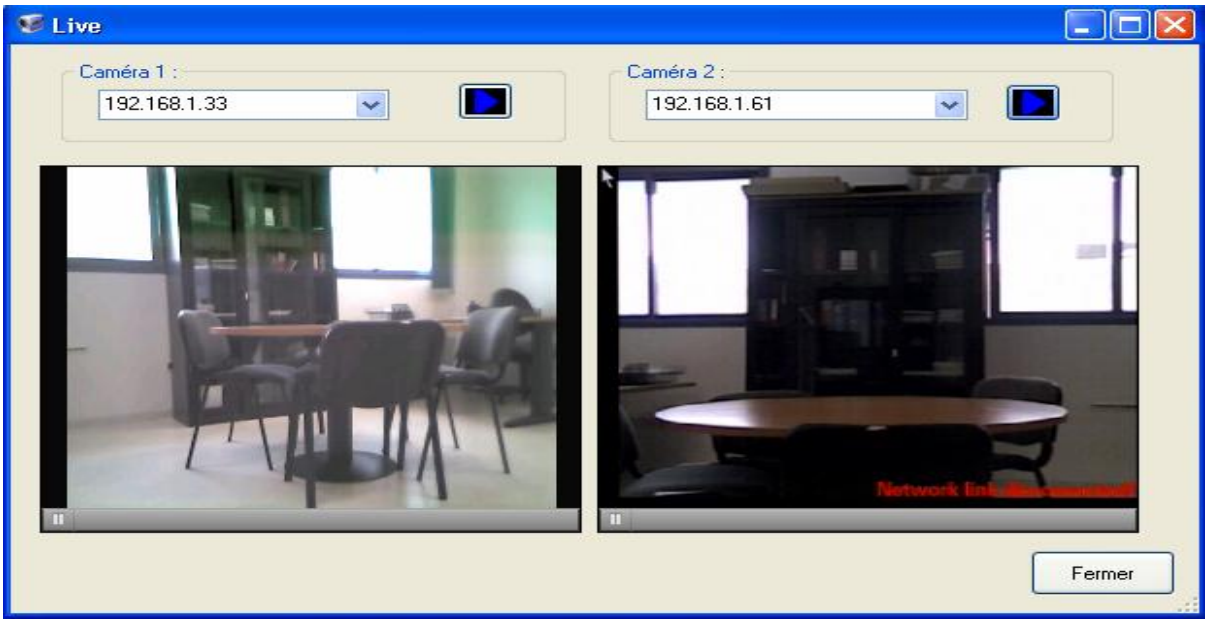

Figure 3.11: Affichage de deux caméras

Figure 3.12: Affichage de quatre caméras

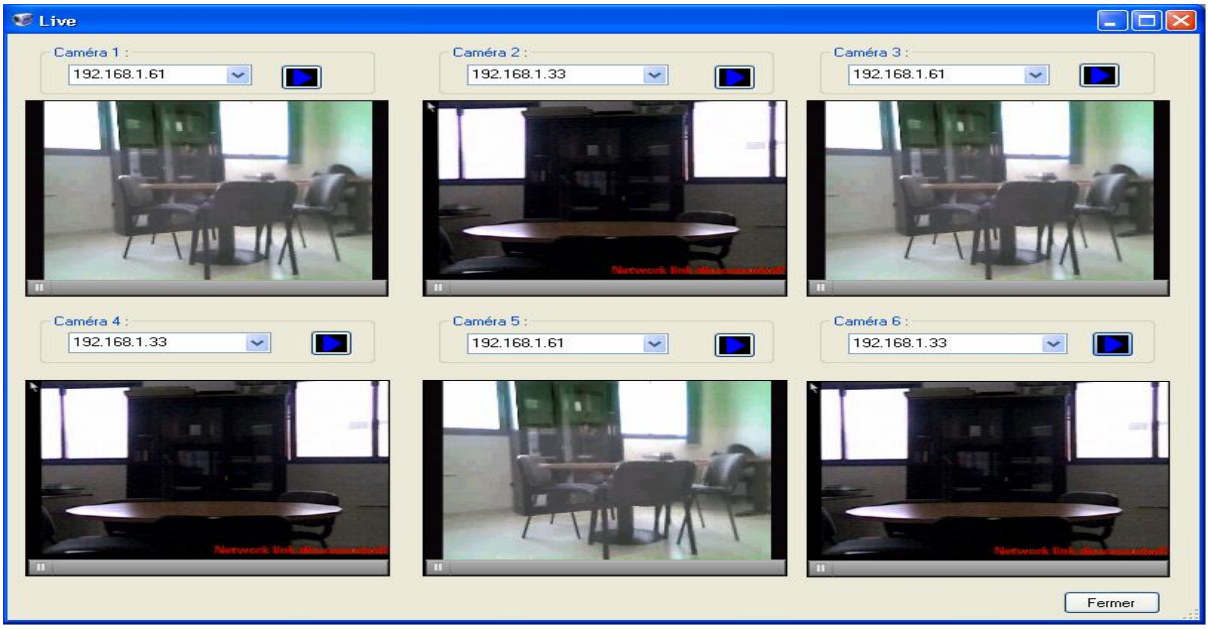

Figure 3.13: Affichage de six caméras

Figure 3.14: Affichage de neuf caméras

Plus de neuf caméras simultanées, le débit exigé par la procédure de streaming sera très important à supporter par la connexion Internet disponible. En outre, la latence sera grande et la qualité de la vidéo sera dégradée. En effet, le nombre de paquet IP qui encapsulent les datagrammes RTSP, transportant les données multimédias, augmente avec le nombre de caméras visualisées simultanément. L'affichage des images à l'écran prendra, ainsi, beaucoup de temps ce qui traduit le problème de retard. Ce problème gène beaucoup l'aspect sécuritaire de la vidéosurveillance qui nécessite le maintien de la notion temps réel de la scène visualisée.

3.5.4.2. Consultation de la vidéo enregistrée

L'interface de consultation des enregistrements permet de voir l'ensemble des enregistrements, présents dans la base de données, pour une caméra ou pour l'ensemble des caméras. Un «enregistrement» est une période de temps pendant laquelle une caméra a été enregistrée. L'enregistrement peut être actif en absence de l'observateur, sur alarme ou bien durant la période préprogrammée par l'exploitant. Les enregistrements qui ont eu lieu peuvent être consultés à partir de la fenêtre « Consultation Vidéos » exposée sur la figure 3.15.

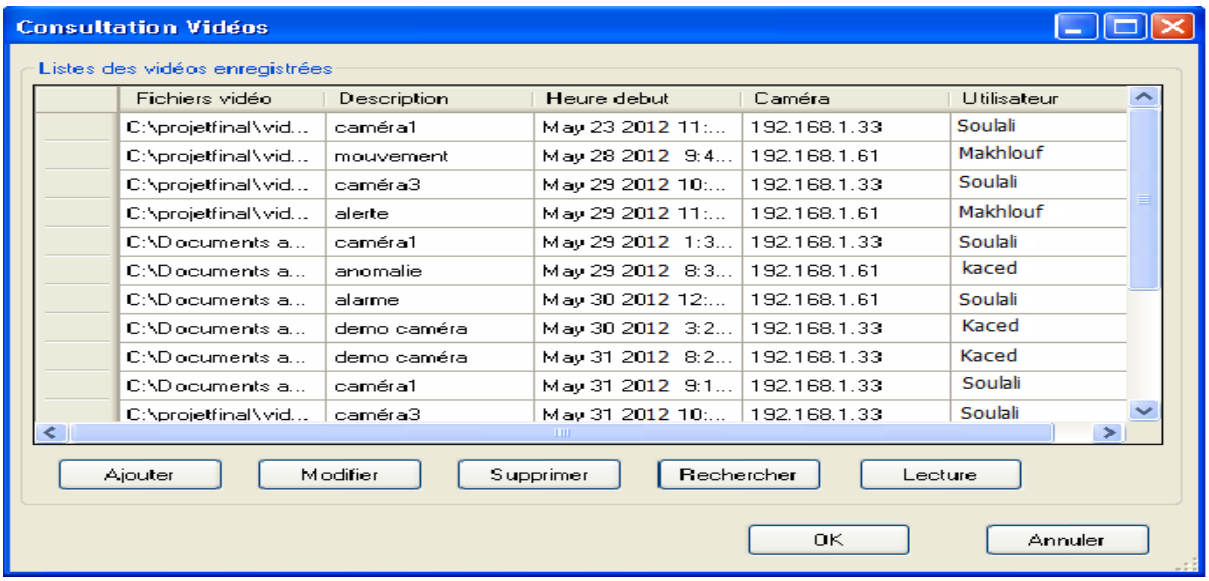

Figure 3.15: Consultation de la vidéo enregistrée

D'après cette fenêtre, une séquence enregistrée est identifiée par son nom, sa description, la date et l'heure de début d'enregistrement et la caméra source. Le responsable qui a commandé cette opération de stockage est ajouté d'une façon automatique à partir du permis d'accès (fenêtre authentification).

Seuls l'administrateur et l'exploitant peuvent ajouter, modifier, supprimer, rechercher ou bien lire un enregistrement sélectionné. Alors que l'observateur ne peut qu'ajouter un nouvel enregistrement.

En cas d'un nouvel enregistrement, l'utilisateur saisit le nom du fichier vidéo, sa description et indique de quelle caméra il provient. Sur click du bouton OK, ces champs seront ajoutés à la base de données vidéo en spécifiant le nom de l'utilisateur. Dans l'autre cas (modification), il s'agit de modifier l'un de ces champs de la ligne sélectionnée dans la fenêtre « Consultation vidéos ».

La fenêtre de la figure 3.16 assure l'ajout ou la modification d'un enregistrement vidéo.

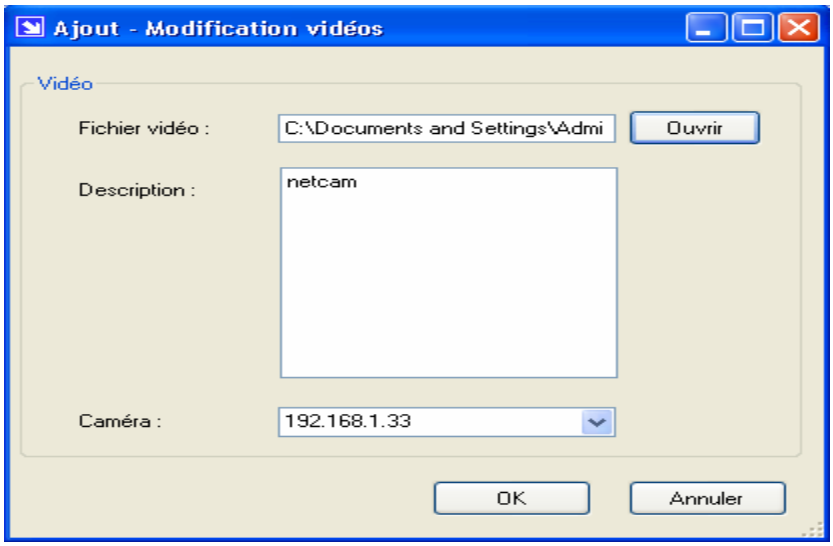

Figure 3.16: Ajout / Modification d'un enregistrement

La recherche d'un enregistrement peut se faire selon plusieurs critères tels que : le nom du fichier, sa description, la date et l'heure de début, la caméra

ou bien l'utilisateur. Ici, nous présenterons un exemple de recherche selon la caméra.

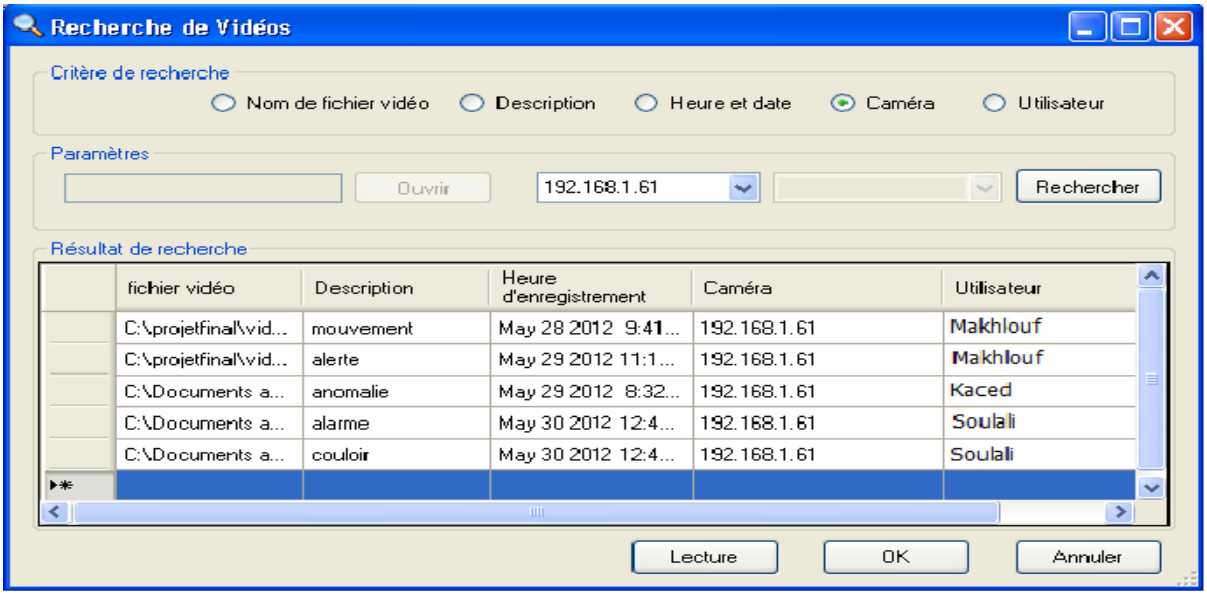

Figure 3.17: Résultat de la recherche (Exp. selon la caméra)

Egalement, l'opérateur peut lire un enregistrement quelconque à partir de la fenêtre « Consultation Vidéo » ou « Recherche vidéo » en sélectionnant le nom du fichier vidéo de la liste courante. La fenêtre « Video Player » qui nous permet d'effectuer cette tâche est présentée par la figure 3.18.

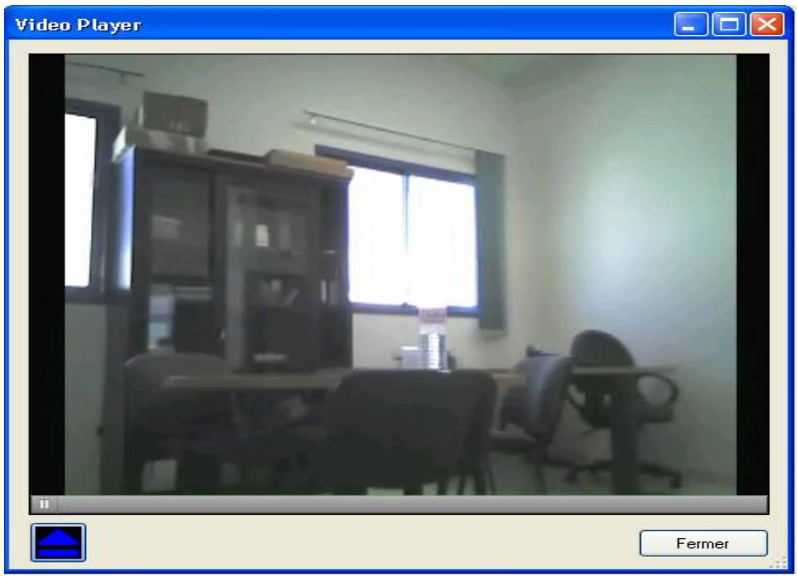

Figure 3.18: Fenêtre « Video Player »

3.5.5. Fonctions d'alerte

La solution de vidéosurveillance sur IP que nous avons développé comporte une gestion centralisée de plusieurs caméras réseau en termes de visualisation, d'enregistrement, de configuration et d'alerte. Ce dernier point consiste à détecter l'existence d'une anomalie, l'enregistrer dans la liste des évènements déclenchés et notifier les responsables par Email, par SMS ou par MMS suivant les disponibilités autorisées par l'administrateur du système.

3.5.5.1. Gestion des Evènements

Tout évènement détecté manuellement par l'observateur ou bien automatiquement par les modules intelligents implémentés (Détection de mouvement, reconnaissance de visage) est directement ajouté à la table événement avec les paramètres descriptifs suivant :

- Type de l'événement : ce champ décrit l'acte excentrique qui s'est produit dans la zone surveillée.
- Mode de déclenchement : manuel ou automatique ;
- Catégorie : décrit le niveau de danger provoqué par cet événement sur la sécurité de l'endroit sous vigilance ;
- Description horodatée de l'évènement ;
- L'adresse IP de la caméra qui surveille la zone dans la quelle l'événement a eu lieu ;
- L'utilisateur qui a constaté l'événement si le déclenchement est manuel ou bien le responsable sur le périphérique cible dans l'autre cas.

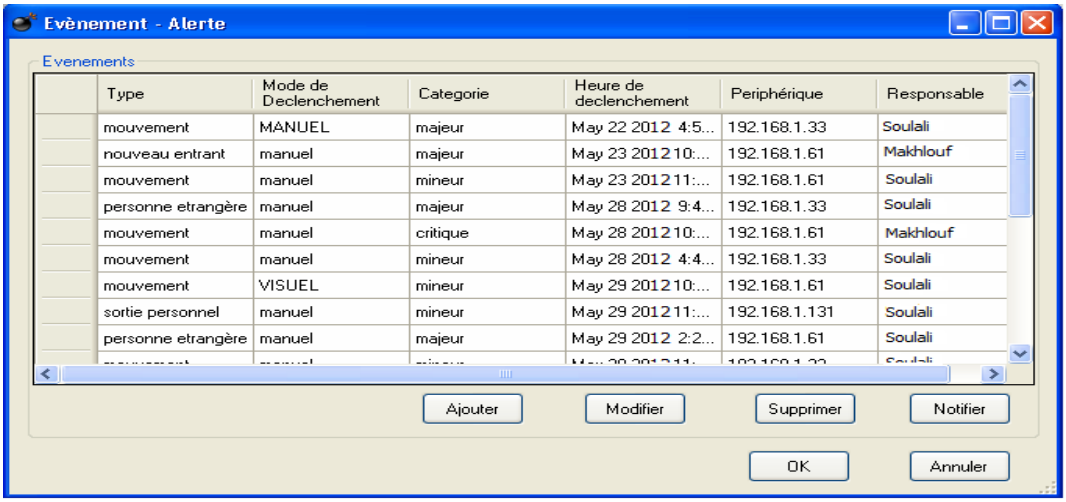

Figure 3.19: Fenêtre « Evènement - Alerte »

- Cette fenêtre autorise à l'exploitant d'ajouter, modifier, supprimer ou bien notifier un évènement.
- L'observateur ne peut qu'à ajouter une nouvelle entrée s'il constate qu'il y'a une action douteuse dans le site contrôlé. Il admet aussi l'autorisation d'envoyer une alerte par Email concernant l'événement déclenché.

3.5.5.2. Ajout/Modification des Evènements

En cas d'ajout, l'utilisateur décrit ici les paramètres clés concernant le nouvel événement tel que le type, le mode de déclenchement, la catégorie et le périphérique. Tandis qu'en cas de modification, il rectifie les paramètres relatifs à l'événement choisis à partir de la fenêtre de la figure 3.19.

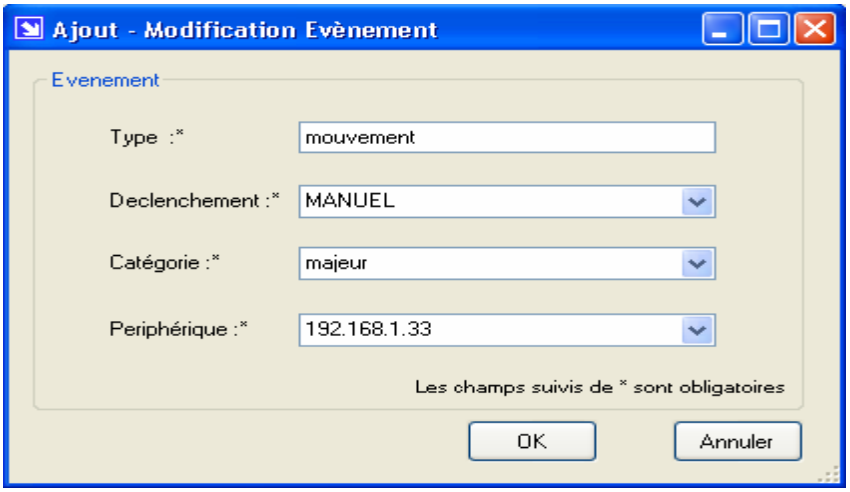

Figure 3.20: Fenêtre « Ajout/Modification d'Evènements »

3.5.5.3. Notification des Evènements

Afin d'assurer la gestion des alarmes correspondantes aux événements déclenchés par le système de vidéosurveillance sur IP et pour mettre au courant les responsables de toute anomalie que le système détecte, nous avons crée la boite de dialogue de notification. Chaque message d'alerte comporte une description de l'événement courant, l'adresse IP de la caméra source et du site surveillé.

3.5.5.3.1. Notification par Email

La procédure d'envoie d'une alerte par Email est décrite, comme le montre la figure 3.21, par les étapes suivantes :

- L'utilisateur sélectionne la liste des contacts aux quels le message sera envoyé; s'il est exploitant, il a aussi le droit d'ajouter d'autres contacts à travers la boîte de dialogue « Ajout E-mail Contacts » présentée par la figure 3.22 ;
- Il saisit un nouveau message d'alarme ou bien il choisit l'un des messages prédéfinis ;
- Les autres paramètres nécessaires au succès de l'envoie de l'Email sont définis par la fenêtre « Options E-mail » esquissées par la

figure 3.23. A partir de ce dialogue, l'utilisateur peut changer le sujet et joindre des fichiers au message. L'émetteur du message et son adresse Email sont configurés automatiquement par le système en fonction de la personne qui vient d'effectuer cette opération de notification.

- Si toute ces étapes sont exécutées, le message d'alerte peut être envoyé ; un avertissement sera affiché à l'écran pour indiquer l'état d'envoie.

Les figures 3.21, 3.22, 3.23 et 3.24 apportent une description visuelle de l'opération de notification par Email.

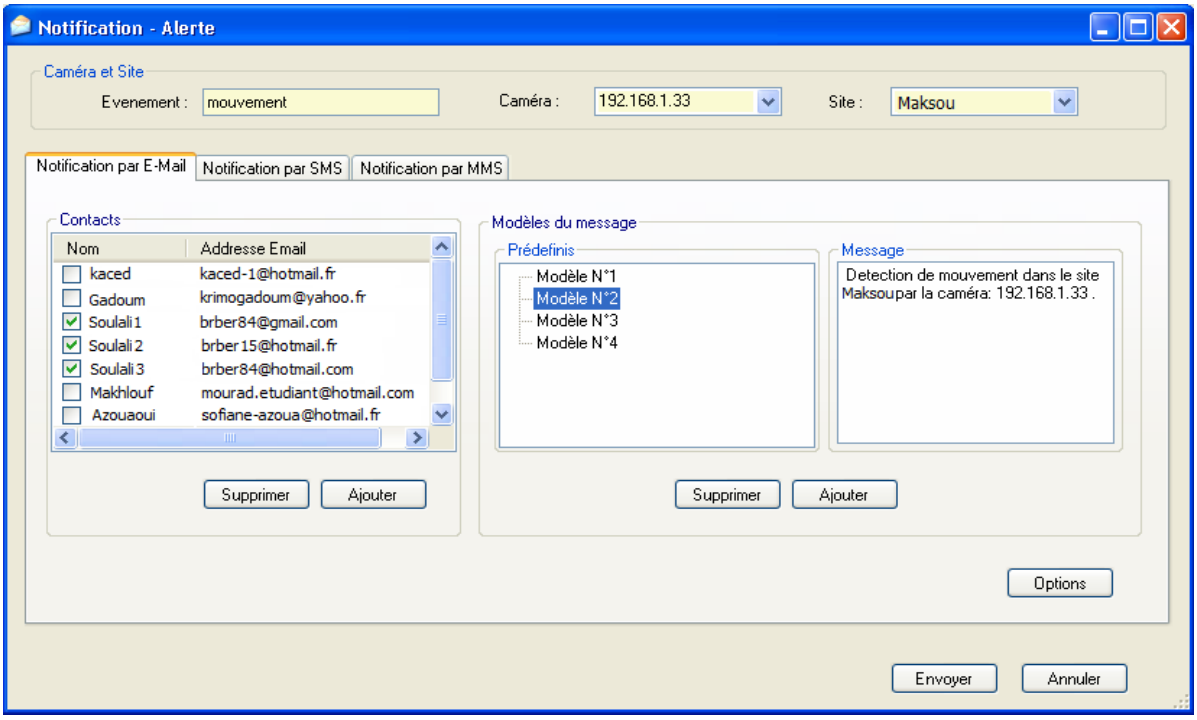

Figure 3.21: Fenêtre « Notification par Email»

Figure 3.22: Fenêtre « Ajout d'un nouveau contact »

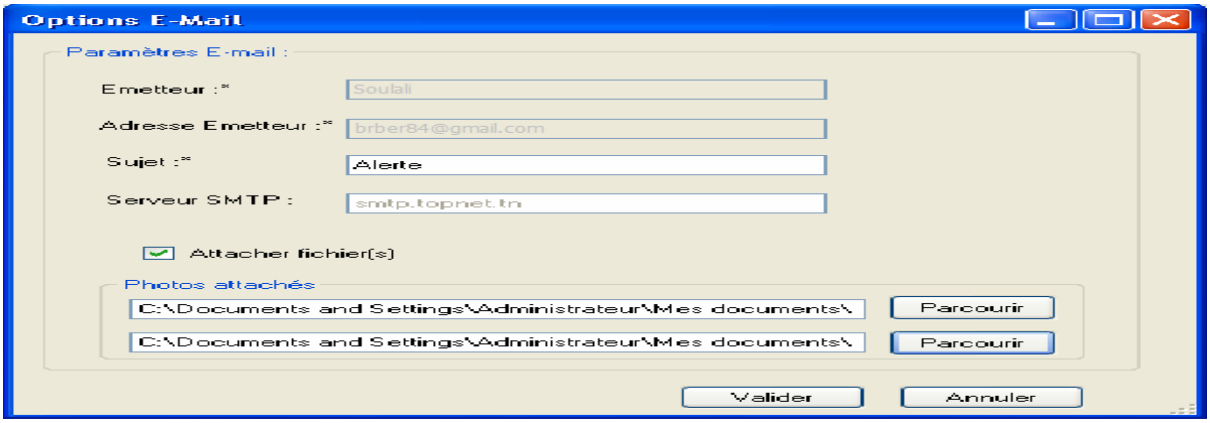

Figure 3.23: Fenêtre « Options E-mail »

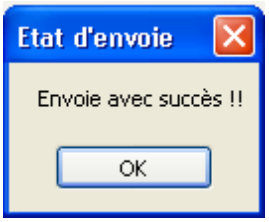

Figure 3.24: Fenêtre « Etat d'envoie de l'email »

3.5.5.3.2. Notification par SMS ou MMS

Comme nous avons présenté dans la partie conception, le système prévoit trois méthodes d'alertes : par Email, SMS et MMS. Dans la partie développement, on a accomplie le premier type de notification. Cependant, pour les modes SMS et MMS, le système procure la plateforme qui l'effectue ; il ne reste qu'à tester le fonctionnement moyennant un modem et une puce GSM. La figure 3.25 assure le procès de notification par SMS et MMS.

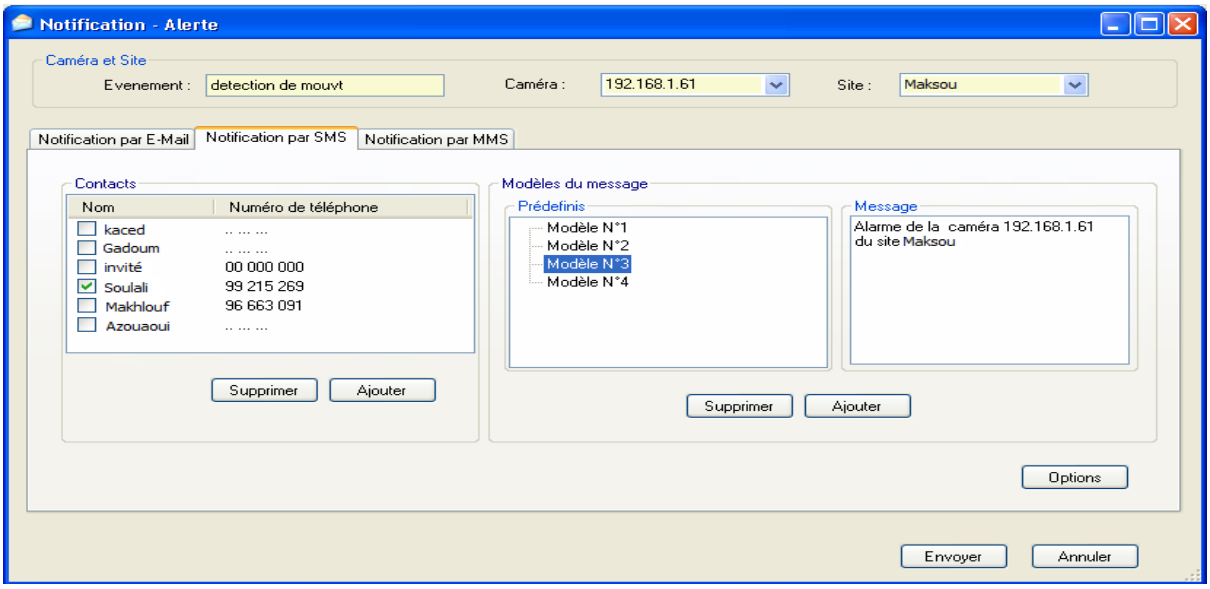

Figure 3.25: Fenêtre « Notification par SMS et MMS »

Egalement, la procédure de notification par SMS et MMS suit la même logique que celle par email. L'utilisateur sélectionne les contacts vers les quels le SMS ou le MMS sera émis et précise le message d'alerte. Sur click sur le bouton « Envoyer » le message d'alerte sera transmis via le réseau GSM. Dans le cas d'une notification par MMS, on peut attacher au message une image à partir du dialogue « Options SMS et MMS » affiché sur click sur le bouton « Options ».

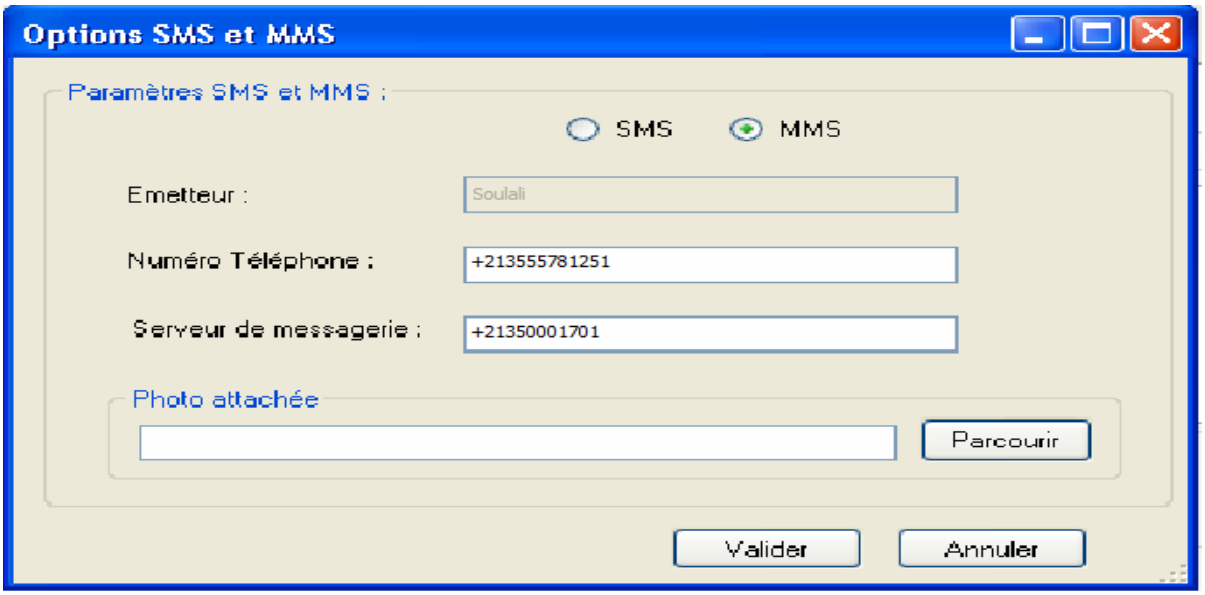

Figure 3.26: Fenêtre « Options SMS et MMS »

Le dialogue qui suit offre la possibilité d'ajouter un nouveau contact SMS et/ou SMS.

Figure 3.27: Fenêtre « Ajout de contact téléphonique »

3.5.5.4. Traces d'alertes

Notre système de vidéosurveillance sur IP envisage aussi la possibilité de gérer l'historique de tous les événements et messages d'alertes qui ont été exécutés pendant une période donnée. L'administrateur ou l'exploitant qui confère l'opération de surveillance à d'autres agents peut pré contrôler leurs tâches et l'état de la sécurité de leurs propriétés à travers le journal des alertes (événements et notification) gardé d'une façon discrète et implicite par le logiciel de vidéosurveillance sur IP. Le fichier d'historique est accessible via la fenêtre « Historique des Evénements et des Notifications ». Il comprend une description complète de tous les événements et notifications ainsi que leurs dates et heures de déclenchement.

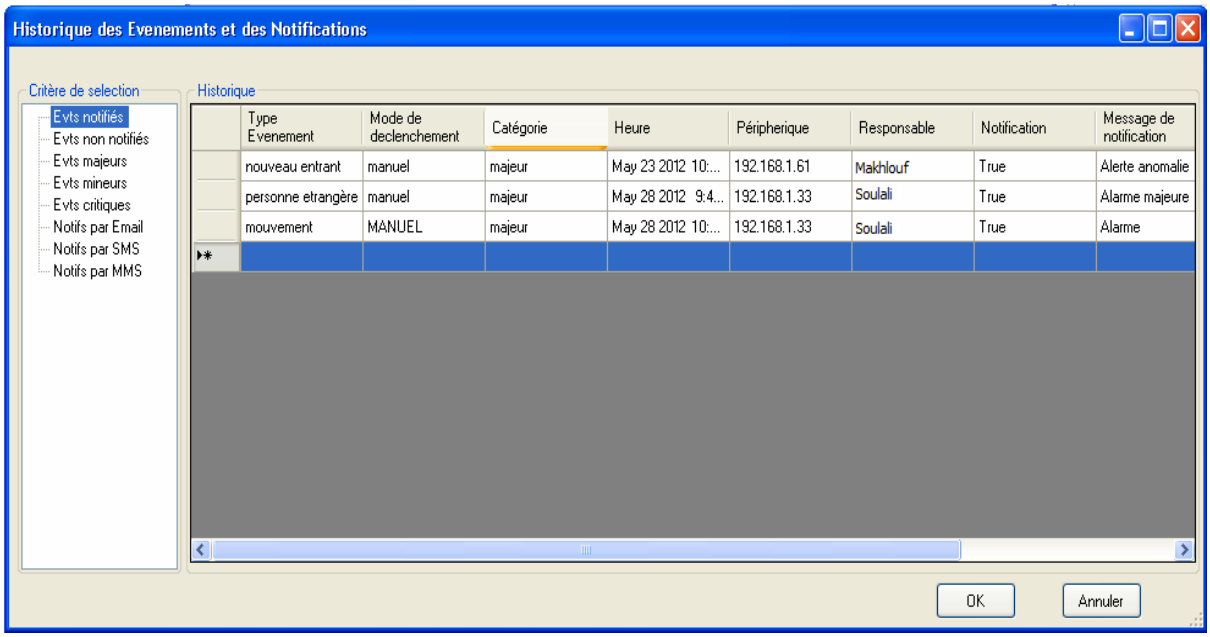

Figure 3.28: Fenêtre « Historique des alertes »

Ce classeur peut comprendre plusieurs lignes d'enregistrements qui le rendent escarpé à lire et à manipuler. C'est pour cette raison que des critères de sélection ont été prévus pour faciliter la tâche du consultant.

3.5.6. Fonctions Auxiliaires

La fenêtre « A propos » décrit l'identité du logiciel de vidéosurveillance développé. Ce logiciel, nommé NetCam Viewer, a été développé au sein de la société EB SYS partenaire de Analog Devices.

Figure 3.29: Fenêtre « A propos »

La fenêtre d'aide représente une sorte de guide pour l'utilisation du logiciel. Elle contient une présentation brève de l'utilité et des fonctionnalités du logiciel développé ainsi qu'une aide sur la procédure d'utilisation du NetCam Viewer.

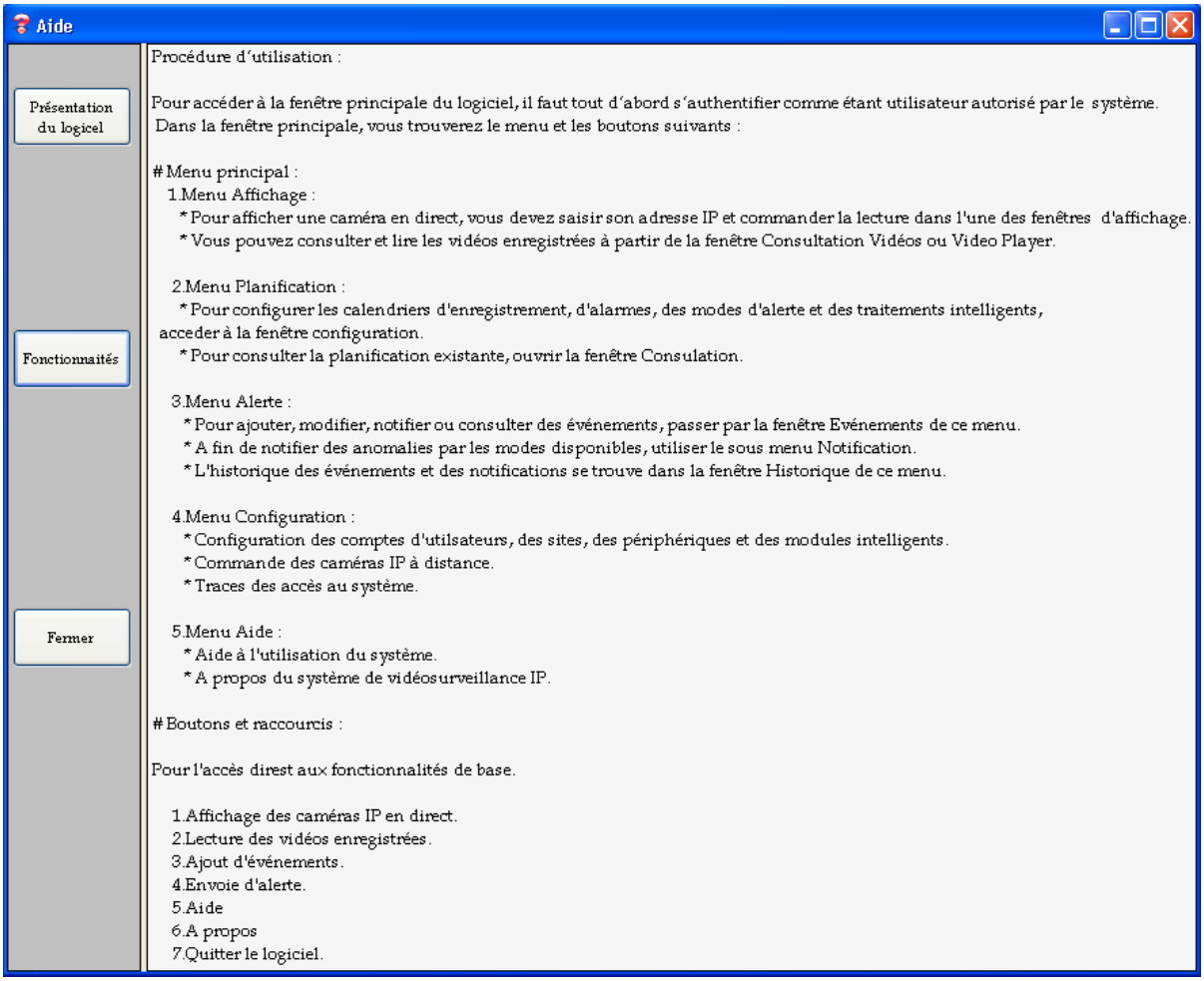

Figure 3.30: Fenêtre « Aide »

3.6. Conclusion

Dans ce chapitre, nous avons, d'abord, présenté l'environnement de la réalisation du logiciel de vidéosurveillance sur IP que nous avons nommé « NetCam Viewer ». Ensuite, nous avons exposé et commenté les principales interfaces relatives aux fonctionnalités d'affichage et d'alerte du système de vidéosurveillance réalisé.

Conclusion générale

Conclusion Générale

Après avoir étudié la vidéo surveillance sur IP de nombreux progrès ont été réalisés dans le monde de la vidéosurveillance. En effet, le passage des technologies analogiques aux numériques dans les installations de vidéosurveillance révolutionne peu à peu le marché des applications vidéo. De ce fait, la solution de vidéosurveillance est devenue une nécessité pour la sécurité des logements, des lieux de travail, de loisirs, des établissements scolaires, des espaces commerciaux, etc.

Dans ce projet, nous avons étudié une solution de vidéosurveillance qui permet la vigilance de plusieurs caméras IP localisées dans des sites distants. Le principe de base de fonctionnement de notre système de vidéosurveillance consiste à : visualiser les images transmises par les caméras réseau disponibles, enregistrer la vidéo reçue selon les modes configurés par l'administrateur (sur alarme, en continu, sur des tranches horaires, etc.), notifier les responsables par Email en cas d'anomalie, mettre à jour les événements déclenchés et plusieurs autres fonctionnalités.

Cette approche de la vidéosurveillance, basée sur l'architecture IP, offre une grande flexibilité d'utilisation vu la facilité et la rapidité de déploiement d'un tel système pour le contrôle simultané de différents sites distants.

Comme perspective de ce travail, nous pouvons envisager l'utilisation des accès mobiles aux données de vidéosurveillance à partir d' d'un téléphone mobile en GPRS/EDGE ou UMTS. Cette orientation répond de manière tellement évidente à certains besoins sécuritaires demandant la mobilité des agents et améliore le champ d'utilisation du système surtout aux utilisateurs sur site. Egalement, nous pouvons aussi, penser à rendre le système de vidéosurveillance accessible à travers le Web, mais le débit exigé par la

procédure de streaming sera très importante à supporter par la connexion disponible si les caméras simultanées sont nombreuses, ce qui traduit une mauvaise qualité d'image, et le problème de retard puisque l'affichage des images à l'écran prendra beaucoup de temps.

Enfin, nous souhaitons que ce travail servira comme documentation de référence pour les promotions à venir.

ANNEXES

Annexe A : Dictionnaire de données

Le dictionnaire est une collection de métadonnées ou de données de référence nécessaires à la conception de la base de données relationnelle. Il contient les différents codes (clés primaires, clés étrangères et les attributs) des différentes tables de la base de données.

Numéro Code Description

Les clés étrangères		
12	NomGroupe_Utilisateur	Le groupe auquel appartient l'utilisateur en cours
13	Utilisateur_Site	Identifiant de l'utilisateur qui gère un site donné
14	Site_Peripherique	Code du site du périphérique courant
15	Utilisateur_Notif	Identifiant de l'utilisateur qui a effectué la notification courante
16	Evenement_Notif	Identifiant de l'événement qui a provoqué la notification courante
17	Peripherique_Enreg	Identifiant de la caméra source de la vidéo enregistrée
18	Utilisateur_Enreg	Identifiant de l'utilisateur qui a effectué cet enregistrement
19	Peripherique_Evenement	Code du périphérique qui a détecté l'événement
20	Utilisateur_Evenement	Identifiant de l'utilisateur qui a observé l'événement
21	Cam_Planification	Code de la caméra au quelle la planification courante est affectée

Numéro	**Code**	**Description**
Les clés primaires		
01	ID_Utilisateur	Identifiant unique d'un utilisateur
02	ID_Site	Identifiant unique d'un site
03	ID_Peripherique	Identifiant unique d'un périphérique
04	ID_Notif	Identifiant unique d'une notification
05	ID_Auth	Identifiant unique d'une authentification
06	ID_Enreg	Identifiant unique d'un enregistrement
07	ID_Evenement	Identifiant unique d'un événement
08	ID_GroupeUtilisateurs	Identifiant unique d'un groupe d'utilisateurs
09	ID_Module	Identifiant unique d'un module intelligent
10	ID_Planification	Identifiant unique d'une planification
11	TypeUtilisateur	Identifiant unique d'un droit d'utilisateur

Les attributs		
22	Nom_Utilisateur	Nom de l'utilisateur
23	Prenom_Utilisateur	Prénom de l'utilisateur
24	Login_Utilisateur	Login de l'utilisateur, utilisée lors de l'authentification
25	MDP_Utilisateur	Mot de passe de l'utilisateur, utilisée lors de l'authentification
26	Email_Utilisateur	Email de l'utilisateur
27	Tel_Utilisateur	Téléphone de l'utilisateur
28	Type_Utilisateur	Type de l'utilisateur : Administrateur, Exploitant ou Observateur
29	Nom_Site	Nom du site surveillé
30	Adresse_Site	Adresse du site surveillé
31	Type_Peripherique	Type du périphérique : caméra, capteur, sirène, etc.
32	AdresseIP_Peripherique	Adresse IP du périphérique s'il s'agit d'une caméra
33	AdresseMAC_Peripherique	Adresse MAC du périphérique
34	Login_Peripherique	Login utilisé pour accéder au périphérique (caméra) si l'accès est protégé
35	MDP_Peripherique	Mot de passe utilisé pour accéder au périphérique (caméra) si l'accès est protégé
36	Contenu_Notif	Le message de notification
37	Image_Notif	Capture d'écran attaché au message d'alerte par email ou par MMS
38	DateHeure_Notif	Date et heure d'envoie de la notification
39	Moyen_Notif	Moyen de notification : SMS, MMS ou email.
40	Acq_Notif	Acquittement de la notification
41	Login	Login saisis lors de l'authentification
42	LogOn	Date et Heure d'accès au système
43	LogOut	Date et heure de sortie du système
44	URL_Enreg	Nom du fichier vidéo enregistré

45	Mots_clés	Description de la séquence enregistrée
46	Temps_debut	Heure d'enregistrement
47	Type_Evenement	Quel est l'événement détecté ?
48	Declench_Evenement	Mode de déclenchement de l'événement
49	Categorie_Evenement	Degré de danger de l'événement
50	DateHeure_Evenement	Date et heure de déclenchement de l'événement
51	Nom_GroupeUtilisateurs	Nom du groupe de l'utilisateur
52	Detection_Mouvement	Module de détection de mouvement
53	Reconnaissance_Visage	Module de reconnaissance de visage
54	Calendrier_Planification	Type de calendrier : journalier, hebdomadaire, mensuel, annuel
55	Enreg_Planification	Mode d'enregistrement : sur alarme, manuel, sur intervalle de temps
56	Notif_Planification	Mode de notification : SMS, MMS, email
57	Fonction_Planification	Planification du module intelligent activé
58	AnDebut_Planification	Année de début du calendrier de planification
59	MoisDebut_Planification	Mois de début du calendrier de planification
60	JourDebut_Planification	Jour de début du calendrier de planification
61	HrDebut_Planification	Heure de début du calendrier de planification
62	MnDebut_Planification	Minute de début du calendrier de planification
63	AnFin_Planification	Année de fin du calendrier de planification
64	MoisFin_Planification	Mois de fin du calendrier de planification
65	JourFin_Planification	Jour de fin du calendrier de planification

66	HrFin_Planification	Heure de fin du calendrier de planification
67	MnFin_Planification	Minute de fin du calendrier de planification
68	Jours_Planification	Jour de configuration de la planification
69	Mois_Planification	Mois de configuration de la planification
70	Gest_Utilisateurs	Droit de Gestion des comptes d'utilisateurs
71	Gest_Sites	Droit de gestion des sites
72	Gest_Peripheriques	Droit de gestion des périphériques
73	Traces	Droit de gestion des traces d'accès au système
74	Gest_Enreg	Droit de gestion des enregistrements
75	Cfg_Plan	Droit de planification
76	Consult_Plan	Droit de consultation des planifications faites
77	Evenement	Droit de gestion des évènements
78	Notification	Droit de notification
79	Historique	Droit de consultation des historiques d'alerte
80	Modules_Intelligents	Droit de configuration des modules intelligents
81	Cmd_Camera	Droit de la commande des caméras
82	Cfg_Camera	Droit de la configuration des caméras
83	Visualisation	Droit de visualisation live des caméras

Annexe B : Description des objets de la base de données

Dans le tableau suivant, nous exposerons les tables constitutives de la base de données du système de vidéosurveillance sur IP. Chaque table est décrite par ses identifiants clés les champs propriétés.

Notifications	**04**	ID_Notif	**36**	Contenu_Notif
	15	Utilisateur_Notif	**37**	Image_Notif
	16	Evenement_Notif	**38**	DateHeure_Notif
			39	Moyen_Notif
			40	Acq_Notif
Authentification	**05**	ID_Auth	**41**	Login
			42	LogOn
			43	LogOut
Enregistrement	**06**	ID_Enreg	**44**	URL_Enreg
	17	Peripherique_Enreg	**45**	Mots_clés
	18	Utilisateur_Enreg	**46**	Temps_debut
Evénements	**07**	ID_Evenement	**47**	Type_Evenement
	19	Peripherique_Evenement	**48**	Declench_Evenement
	20	Utilisateur_Evenement	**49**	Categorie_Evenement
			50	DateHeure_Evenement
Groupe_Utilisateur	**08**	ID_GroupeUtilisateurs	**51**	Nom_GroupeUtilisateurs
Modules Intelligents	**09**	ID_Module	**52**	Detection_Mouvement
			53	Reconnaissance_Visage

Planification	**10**	ID_Planification	**54**	Calendrier_Planification
	21	Cam_Planification	**55**	Enreg_Planification
			56	Notif_Planification
			57	Fonction_Planification
			58	AnDebut_Planification
			59	MoisDebut_Planification
			60	JourDebut_Planification
			61	HrDebut_Planification
			62	MnDebut_Planification
			63	AnFin_Planification
			64	MoisFin_Planification
			65	JourFin_Planification
			66	HrFin_Planification
			67	MnFin_Planification
			68	Jours_Planification
			69	Mois_Planification
Types_Utilsateurs	**11**	TypeUtilisateur	**70**	Gest_Utilisateurs
			71	Gest_Sites
			72	Gest_Peripheriques
			73	Traces
			74	Gest_Enreg
			75	Cfg_Plan
			76	Consult_Plan
			77	Evenement
			78	Notification
			79	Historique
			80	Modules_Intelligents
			81	Cmd_Camera
			82	Cfg_Camera
			83	Visualisation

Bibliographie

[1] :<< Guide technique de la vidéo sur IP >>, page 7, guide disponible sur le site : www.axis.com.

[2] : << réseau de télésurveillance par caméra IP >>, Rapport de fin d'études, réalisé par Mohamed Moncef BEN AMOR, page 20.

[3] : PHILIPPE Bellaiche, << les secret de l image vidéo>> 4 eme édition, page 236,237.

[4] :<< guide technique de la vidéo sur IP>> page 21, le guide disponible sur le site : www.axis .com.

[5] : << catalogue vidéosurveillance –IP-2011>> catalogue disponible sur le site : www.securite 01.com.

[6] :philipe gasser << MPEG-4>>, créative commons , 17 septembre 2005 , article disponible sur le site http:// plate –forme-ast.mshparismonde.org/.

[7] : le guide technique de la vidéo sur IP >>, page 45 ,46, www.axis.com.

[8] : <<techguide AXIS de la vidéo sur IP >> - technologies réseau (chapitre 9,page 80,81) ,www.axis.co m.

[9] : Nico VanHaute, Julien Barascud et Jean-Roland Conca, « Les Protocoles RTP et RTCP », document disponible sur : www.commentcamarche.net

[10] : Guillaume Rincé, « Le principe du streaming », Créative Commons, 20 février 2001, article disponible sur : http://www.rince.fr/

[11] : « RTSP », document disponible sur : www-rp.lip6.fr

[12] : André Aoun, « Le protocole RTSP », Université Paul Sabatier (Toulouse III), 2001, disponible sur : http://www.httr.ups-tlse.fr/

[13] : Mohamed Moncef BEN AMOR, « Réseau de télésurveillance par caméras IP », Rapport de fin d'études, SUP'COM, pages : 28-33, 2004/2005.

[14] : www.commentcamarche.net/forum/affich-1384859-differences-entre-merise-et-uml

[15] : www.commentcamarche.net/uml/uml-use-cases.php3

[16] : http://www.microsoft.com/sql/default.mspx

[17] : https://dpt-info.u-strasbg.fr/~frey/L3PF_BD/TP8/L3PF_BD_TP8.pdf

[18] : John Sharp et Jon Jagger, « Microsoft VISUAL C#.NET étape par étape », Dunod, 2002.