UNIVERSITÉ DU BURUNDI
GRENIER DU SAVOIR DU BURUNDI
Dépôt institutionnel officiel
https://repository.ub.edu.bi

Etude sur la surveillance par cameras interconnectés à base d'un réseau informatique cas de la société Gaspas Company

NIMBONA, Bluce; NDIKUMANA, Jean Paul

2009

UB, Institut Technique Supérieur

https://repository.ub.edu.bi/handle/123456789/1096

Document téléchargé depuis le **Grenier du Savoir du Burundi** — https://repository.ub.edu.bi

UNIVERSITE DU BURUNDI
INSTITUT TECHNIQUE SUPERIEUR
DEPARTEMENT DU GENIE
ELECTROMECANIQUE

ETUDE SUR LA SURVEILLANCE PAR CAMERAS INTERCONNECTEES A BASE D'UN RESEAU INFORMATIQUE CAS DE LA SOCIETE GASPAS COMPANY

Projet de fin d'études présenté et défendu publiquement en vue de l'obtention du grade d'Ingénieur Industriel en Génie Electromécanique

par

NIMBONA Bruce et
NDIKUMANA Jean Paul

Sous la Direction de:
M. Ir GASUNZU Pascal
Ir NDUWAYO Yves

Bujumbura, Septembre 2009

DEDICACE

A mon protecteur Dieu Tout Puissant,
A la Sainte Vierge Marie,
A mes chers parents,
A la famille NDIKUMANA Haruna,
A mes frères et sœurs,
A tous mes amis,

Je dédie ce travail

NIMBONA Bruce

DEDICACE

A Dieu Tout Puissant,
A mes chers regrettés parents,
A mes frères et sœurs,
A mes cousins et cousines,
A mes neveux et nièces,
A toute ma famille, ami(e)s et connaissances,

Je dédie ce travail

NDIKUMANA Jean Paul

REMERCIEMENTS

Au terme de notre travail, il nous est agréable d'exprimer, plus par conviction que par simple formalisme, nos sentiments de reconnaissance envers toute personne qui, de près ou de loin a contribué à sa réalisation.

Certes le succès de mettre à terme ce travail, nous le devons à M.Ir GASUNZU Pascal, Directeur et promoteur de ce projet qui, malgré ses multiples occupations n'a menagé aucun effort pour mener à bout ce travail ; nous lui exprimons notre profonde gratitude.

Nos vifs remerciements sont également adressés à Ir Yves NDUWAYO, Co-directeur de ce mémoire. Ses conseils scientifiques, ses pertinentes remarques et ses suggestions nous ont été d'une importance capitale ; que ce travail lui donne une entière satisfaction.

Nos sincères remerciements s'adressent aux professeurs de l'Université du BURUNDI plus particulièrement les professeurs de l'Institut Technique Supérieur (ITS) pour la formation morale et intellectuelle dont ils nous ont dotés.

Grande est notre reconnaissance à l'égard de l'administration et du personnel des sociétés BRARUDI, INFOCOM, GASPAS COMPANY pour nous avoir accordé des stages de perfectionnement, une documentation, une formation théorique et pratique et les moyens matériels qui nous ont facilité la réalisation de notre travail. Qu'elles trouvent dans ce travail le fruit de la formation qu'elles nous ont donnée.

Enfin, à toutes nos familles, amis et connaissances, nous disons merci.

NDIKUMANA Jean Paul
et
NIMBONA Bruce

LISTES DES SIGLES ET ABREVIATIONS

ADSL : Asymetric Digital Subscriber Line
APC : Asynchronous Procedure Call
ASA : American Standard Association
ASCII : American Standard Code for Information Interchange
BNC : British Naval Connector
CAN : Convertisseur Analogique Numérique
CCD : Charged Coupled Divice
CCTV : Closed Circuit TeleVision
CDROM : Compact Disc Read Only Memory
CMOS : Complementary Metal Oxide Semi-conductor
DCS : Digital Cellular System
DIN : Département d'Imagerie Numérique
DTC : Dispositif à Transfer de Charges
DV : Digital Video
DVR : Digital Video Recorder
ETA/TIA : Electronic Telecommunication Association / Telecommunication Industries Association
ETSI : Electric and Telecommunication Standard Institut
FAI : Fournisseur d'Accés à Internet
FDDI : Fiber Distributed Data Interface
FH : Fréquence Horizontale
FIT : Frame Interline Transfer
FT : Frame Transfer
FTP : File Transfer Protocol
FV : Fréquence Vertical
HTTP : Hyper Text Transfer Protocol
HUB : Hack Un Billow (ou Host Unit Briadcast)
HZ : Hertz
IEEE : Institut of Electrical and Electronic Engineers
IP : Internet Protocol
ISO : International Standard Organisation
IT : Interline Transfer
JPEG : Join Photographi Expert Girond
LAN : Local Area Network
LCD : Liquid Crystal Display(affichage à cristaux liquides)
LLL : Link Logic Control
MAC : Medium Access Control
MAN : Metropolitan Area Network
Mbps : Mégabit par seconde

MJPEG : Montion Joint Picture Experts Group
MMS : Multimedia Messaging Service
MODEM : Modulateur Démodulateur
MPEG : Moving Picture Experts Group
NOS : Network Operating System
NT : New Technologie
NTSC : National Television System Committee
ONATEL : Office Nationale de Télécommunication
OSI : Open System Interconnection
PAL : Phase Alternating Line
PC : Personnal Computer
PTZ : Pan Tilt Zoom
RNIS : Réseau Numérique à Intégration de Services
RPV : Réseau Privé Virtuel
SECAM :Séquentiel Couleur Avec Mémoire
STP : Shielded Twisted Pair
TCP/IP : Transfer Control Protocol / Internet Protocol
USB : Universal Serial Bus
UTP : Unshielded Twisted Pair
VCA : Voltage Controlled Amplifier
VCD : Video Class Device
VPN : Virtual Private Network
WAN : Wide Area Network
WIFI : Wireless Fidelity

TABLE DES MATIERES

DEDICACES.....i & ii
REMERCIEMENTS.....iii
LISTES DES SIGLES ET ABREVIATIONS.....iv
TABLE DES MATIERES.....vi
INTRODUCTION GENERALE.....1

I^{ère} PARTIE : GENERALITES SUR LES CAMERAS.....4

CHAPITRE I STRUCTURES GENERALES DES CAMERAS.....5

I.1 Définition d'une caméra.....5
I.2 Chambre Noire.....5
I.2.1 Instrument optique.....5
I.2.2 Principe de la chambre noire.....6
I.3 Principales parties d'une caméra.....6
I.4 Types de caméra.....8
I.4.1 Camera film.....8
I.4.1.1Différents types de film.....8
I.4.1.2 Principe de fonctionnement de la pellicule photographique.....9
I.4.1.2.1 Pellicule négatif noir et blanc.....9
I.4.1.2.2. Pellicule négative couleur.....10
I.4.1.2.3 Pellicule positive couleur- diapositive.....11
I.4.1.2.2 Sensibilité du film.....12
1.4.1.2.3 Types d'émulsions.....12
1.4.2 Caméra vidéo.....12
1.4.2.1 Notion sur la vidéo.....12
1.4.2.1.1 Théorie de la vidéo.....13
1.4.2.1.2 Capture de l'image.....14
I.4.2.2.4 Résolution de l'image et fréquence de balayage.....14

CHAPITRE II TECHNIQUE DE NUMERISATION.....16

II.1 Introduction.....16
II.2 Acquisition des images.....16
II.2.1 Traitement des signaux.....16
II.2.1.1 Signal analogique.....16
II.2.1.2 Signal numérique.....16

II.2.1.3 Conversion d'un signal analogique en numérique.....16
II.2.1.3.1 Echantillonnage.....16
II.2.1.3 Quantification.....17
II.2.1.3.3 Reconstitution du signal quantifié.....18
II.2.2 Camera numérique.....19
II.2.2.1.1 Capteur CCD.....19
II.2.2.1.1 Comparaison des capteurs CCD aux capteurs CMOS.....19
II.2.2.1.2 Performances des capteurs.....19
II.2.2.2 Capture de l'image.....21
II 2.1.2 Compression de l'image.....22
II 2.2.4 Destination de l'image.....23
II.2.2.5 Port de connexion.....23
II.3 Conclusion.....24

CHAPITRE III SYSTEME DE VIDEO SURVEILLANCE.....25

III.1 Introduction.....25
III.2 Equipements de la vidéosurveillance.....25
III.2.1 Types de caméras.....25
III.2.2 Supports de transmission.....27
III.2.2.1 Câble coaxial.....27
III.2.2.1.1 Rôle des différentes parties du câble coaxial.....28
III.2.2.1.2 Types de câbles coaxiaux.....28
III.2.2.1.3 Connecteurs pour câble coaxial.....29
III.2.2.2 Câble à paire torsadée.....30
III.2.2.2.1 Types de câbles à paire torsadée.....30
III.2.2.2.2 Connecteur pour câble à paire torsadée.....31
III.2.2.3 Fibre optique.....32
III.2.3 Enregistreur Vidéo Numérique ou DVR.....32
III.3 Différents systèmes de connexion de réseaux cameras.....33
III.3.1 Système sur réseau IP.....33
III.3.2 Kit de Vidéosurveillance.....34
III.3.3 Réseau classique de Vidéosurveillance.....35
III.3.4 Système hybride de Vidéosurveillance.....35

II^{ème} PARTIE : INTRODUCTION AU DOMAINE INFORMATIQUE....36

CHAPITRE IV : NOTIONS SUR LES RESEAUX INFORMATIQUES...37

IV.1 Définition d'un réseau informatique.....37
IV.2 Intérêt d'un réseau informatique.....37
IV.3 Classification des réseaux.....38
IV.4 Topologies des réseaux.....39
IV.4.1 Topologie en bus.....40
IV.4.2 Topologie en étoile.....40
IV.4.3 Topologie en anneau.....41
IV.4.4 Comparaison des différentes topologies.....42
IV.5 Architecture de réseau: le modèle OSI.....43
IV.5.1 Les sept couches du modèle ISO.....44
IV.6 Réseaux locaux.....48
IV.6.1 Objectifs des réseaux locaux.....48
IV.6.2Caractéristiques des réseaux locaux.....48
IV.6.3 Constituants matériels d'un réseau local.....50
IV.6.4 Différents types de réseau.....51
IV.6.4.1 Présentation de l'architecture d'égal à égal.....51
IV.6.4.1.1 Inconvénients des réseaux d'égal à égal.....51
IV.6.4.1.2 Avantages de l'architecture d'égal à égal.....52
IV.6.4.1.3 Mise en oeuvre d'un réseau peer to peer.....52
IV.6.4.1.4 Administration d'un réseau poste à poste.....53
IV.6.4.1.5 Notions de sécurité.....53
IV.6.4.2 Présentation de l'architecture client/serveur.....53
IV.6.4.2.1 Avantages.....54
IV.6.4.2.2 Inconvénients.....54
IV.7 Réseau local sans fil.....54
IV.7.1 Définition.....54
IV.7.2 Cas d'utilisation.....55
IV.7.3 Réglementation.....55
IV.7.4 Les équipements nécessaires pour un réseau local sans_fil.....55
IV.7.4.1Carte réseau sans fil.....55
IV.7.4.2 Routeur sans fil.....55
IV.7.5 Exemple d'une installation d un réseau local sans fil.....56
IV.7.5.1 Préparer l'installation.....56
IV.7.5.2 Installation du routeur sans fil.....56
IV.7.5.3 Installation des cartes réseaux sans fil.....57

CHAPITRE V : INTERCONNEXION DES RESEAUX.....58

V.1 Interconnexion des Réseaux locaux.....58
V.1. 1 Introduction.....58
V.1.2 Equipements d'interconnexion.....58
V.1.2.1 Répéteurs.....58
V.1.2.2 Concentrateurs (hubs).....59
V.1.2.3 Ponts.....61
V.1.2.4 Commutateurs.....62
V.1.2.5 Passerelles.....63
V.1.2.5 Routeurs.....63
V.2 Interconnexion des réseaux distants.....65
V.2.1 Internet.....65
V.2.2 Réseau VPN.....66

III[ème] PARTIE : ETUDE DE LA SURVEILLANCE PAR CAMERAS INTERCONNECTEES A BASE D'UN RESEAU INFORMATIQUE « CAS DE LA SOCIETE GASPAS COMPANY ».....68

CHAPITRE VI : PRESENTATION GENERALEDE LA SOCIETE GASPAS COMPANY.....69

VI.1 Historique.....69
VI.2 Organisation générale.....70
VI.4 Réseau informatique existant.....71
VI.4.1 Serveur.....74
VI.1.2 Système d'exploitation réseau.....74
VI.4.3 Internet.....75
VI.4.4 Aspect de sécurité.....75
VI.4.4.1 Sécurité physique.....75
VI.4.4.2 Sécurité des données.....75

CHAPITRE VII : SURVEILLANCE PAR CAMERAS INTERCONNECTEES.....77

VII.1 Pourquoi la vidéosurveillance de la société GASPAS COMPANY.....77
VII.2 Interconnexion des caméras.....77

VII.2.1 Choix de la caméra 77
VII.3 Description de la caméra utilisée.....79
VII.4 Choix du serveur vidéo.....81
VII.5 Nouveau réseau avec caméras de surveillances intégrées.....82
VII.5.1 Câblage.....83
VII.5.2 Fixation.....83
VII.6 Logiciel d'installation.....85
VII.7 Configuration du serveur vidéo.....85
VII.7.1 Configuration via un réseau local.....86
VII.7.2 Configuration via Internet.....86
VII.8 Devis estimatif du projet.....87
VII.8.1 Matériel à commander.....88
VII.8.2 Ressources humaines.....88

CONCLUSION GENERALE.....90
BIBLIOGRAPHIE.....91

INTRODUCTION GENERALE

Le souci d'être sécurisé et de protéger ses biens a été pour l'homme le facteur qui le pousse à chercher des moyens divers pour y faire face ; d'où le proverbe « Là où est ton trésor, là où est ton cœur ». C'est pour cela que dés l'antiquité, l'homme faisait recours à des moyens humains (gardiens, contrôleurs), matériels (clôtures des maisons et des plantations) et animaux (exemple : chiens).
L'infidélité et la corruptibilité de l'un ou l'autre de ces moyens expliquent les résultats moins satisfaisants vis-à-vis de ce besoin vital qui est devenu indispensable face aux guerres perpétuelles ici et là dans le monde créant ainsi un sentiment d'insécurité chez l'homme.

Ainsi, l'être humain, à travers différentes époques, a fourni ses efforts intellectuels afin de découvrir des méthodes de sécurité adéquates. Le fruit de ses efforts a été couronné dans l'histoire de la cinématographie, par l'invention d'un outil pouvant surveiller le mouvement d'un être humain et des objets à ses alentours. C'est « **la caméra** ».
Cette dernière a été inventée par deux frères français LOUIS et AUGUSTE LUMIERE en 1895 à Paris et est destinée à des fins cinématographiques.

La première caméra portative au monde date de 1979. Depuis, la technologie n'a cessé d'évoluer, accélérée encore par les récents développements des puces électroniques liées à l'informatique et à la micro-informatique. On distingue plusieurs catégories de caméras : intérieur/extérieur, fixes/mobiles (PTZ), couleur/noir et blanc.
Par l'utilisation des circuits amplificateurs de lumière ou par traitement infrarouge, certaines caméras sont capables de filmer le jour comme la nuit, selon leur sensibilité.

L'expansion d'INTERNET a conduit de nombreuses entreprises à développer des caméras IP consultables et contrôlables via INTERNET, depuis n'importe où dans le monde. Contrairement aux caméras CCTVC, seuls les caméras IP sont capables de produire des images en haute résolution. En contrepartie, la visualisation ne peut être réalisée que par l'intermédiaire d'un ordinateur.

Les causes de l'installation de systèmes de vidéosurveillance sont diverses. Toutefois, la sécurité publique ainsi que la protection des biens mobiliers ou immobiliers font office d'éléments phares dans la justification de la vidéosurveillance.

Les premières caméras de surveillances destinées à surveiller la population sont apparues dans le commerce et c'est pour prévenir le vol.

Par la suite, le système s'est élargi aux abords des bâtiments importants (ambassades, organisation internationales, banques,....)
Mais tout cela toujours dans un cadre « professionnel ».
Toutefois, la mise en place de la vidéosurveillance ne peut s'expliquer uniquement par l'insécurité grandissante ou la protection des biens. Certaines autres raisons moins connues du grand public existent également. La mise en place de la vidéo surveillance permet une amélioration de la gestion, des incidents ainsi qu'une augmentation de l'efficacité et de la rapidité d'intervention. Par exemple, dans la prévention du suicide ou encore lors des accidents qui pourraient survenir sur la voie publique. La surveillance des axes routiers sert à informer en temps réel les automobiles sur les conditions du trafic.

Ainsi donc, ces nouvelles technologies liées à la sécurité tant humaine que matérielles sont beaucoup appliquées dans les pays développés.
Dans notre pays aussi, des entreprises soucieuses d'acquérir des technologies modernes, ne ratent pas l'occasion offerte par ces nouvelles technologies informatiques pour subvenir à bout des besoins sans cesse croissant de sécurité, ce qui tranquillise un nombre important d'entrepreneurs bénéficiaires. C'est dans ce cadre que la société **GASPAS COMPANY** a songé à l'implantation des cameras de surveillance interconnectés à partir d'un réseau informatique existant pour bénéficier des avantages de ce progrès en matière de surveillance.

Quant à nous, nous nous sommes proposés de contribuer à l'étude de la surveillance pouvant satisfaire aux doléances de l'entreprise, d'où notre projet de fin d'études intitulées :

ETUDE SUR LA SURVEILLANCE PAR CAMERAS INTERCONNECTEES A BASE D'UN RESEAU INFORMATIQUE : « CAS DE LA SOCIETE GASPAS COMPANY »

Notre travail est subdivisé en trois grandes parties à savoir :

1ère Partie : ***Généralité sur les caméras*** où nous présentons brièvement les notions sur les caméras pour mettre en bain le lecteur. Ensuite, nous parlerons un peu du principe de fonctionnement de celles-ci et leur amélioration en système de surveillance qui est la vidéosurveillance.

2ème Partie : ***Introduction au domaine du réseau informatique*** où nous dégagerons les avantages du réseau vis-à-vis de l'interconnexion des équipements qu'héberge celui-ci et ses différentes topologies et structures.

3ème Partie : ***Etudes sur la surveillance par caméras interconnectées à base d'un réseau informatique*** où nous allons décrire quelques généralités sur le réseau informatique existant à la société et ensuite, nous présenterons une application pratique du nouveau réseau (avec des caméras de surveillance intégrées) à implanter.

I^{ère} PARTIE : GENERALITES SUR LES CAMERAS

CHAPITRE I STRUCTURES GENERALES DES CAMERAS

I.1 Définition d'une caméra

La caméra est un appareil de prise de vues animées pour le cinéma, la télévision ou la vidéo. Le terme « ***Camera*** » est issu du latin ***Camera*** et en français veut dire « Chambre ». La ***Camera obscura*** ou Chambre noire en français désignait un dispositif que les peintres (de la Renaissance) utilisaient pour le dessin en perspective conservé dans l'appellation (chambre photographique). En langue anglaise, ***camera*** désigne un appareil photo et ***movie camera*** désigne une caméra.

I.2.1 Chambre Noire

La chambre noire aussi appelée ***camera obscura*** en latin est un instrument optique objectif qui permet d'obtenir une projection de la lumière sur une surface plane c'est-à-dire d'obtenir une vue en deux dimensions très proche de la vision humaine.

I.2.1.1 Instrument optique

Un instrument optique est un instrument formant une image d'un objet.

- Quand il nécessite la présence d'un œil humain pour observer l'image de l'objet ils sont dits subjectif (exemple : télescope, microscope, loupe ...)
- Quand il ne nécessite pas la présence de l'œil humain, ils sont dits objectif (exemple : projecteur, chambre photographique etc)

De manière générale, on désigne par instrument optique tout instrument utilisant l'optique dans son fonctionnement.

I.2.1.2 Principe de la chambre noire

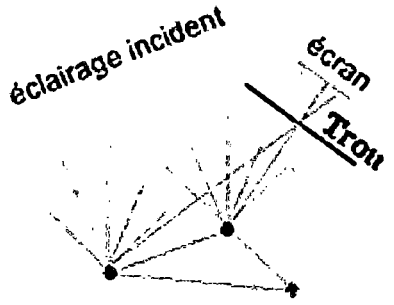


Figure I.1 Principe da la chambre noire

Comme le montre le schéma ci-dessus, les rayons qui passent par le trou proviennent de différentes directions, donc de différents points de l'objet observé. La lumière est réfléchie par les objets dans toutes les directions, suivants leurs qualités propres d'absorption, de réflexion, de diffusion. Chaque point de la surface d'un écran reçoit des rayons lumineux issus de tous les objets alentour ; ces rayons se mélangent et se combinent. L'écran apparaît blanc (ou de teinte majeure éclairant le décor) en restreignant la lumière extérieure de façon à ce que ces rayons lumineux émanant du décor n'entrent que par un seul point dans une chambre obscure, l'écran interceptant cette lumière ne recevant en chacun des points précis de sa surface que les rayons issues en ligne droite d'un seul point du décor placé en face de la paroi comportant le trou. On verra se former l'image inversée (gauche droite) et renversée (haut bas) du décor, extérieure à la chambre obscure, sur l'écran.

I.3 Les principales parties d'une caméra

Les caméras peuvent avoir des apparences différentes, elles fonctionnent toutes sur les mêmes principes. On y retrouve les mêmes organes, et on considère qu'elles sont constituées de 3 parties principales:

- Le Corps caméra
- Le magasin
- L'objectif

1° Le corps

Il comprend donc un compartiment étanche à la lumière extérieure: la chambre d'impression. La lumière ne peut passer que par **l'objectif** qui forme l'image au niveau de la fenêtre. La pellicule est guidée par un couloir et elle est maintenue dans un plan très précis au niveau de la fenêtre par un presseur.

2° Le magasin

La pellicule utilisée pour effectuer les prises de vue est placée dans la caméra dans un compartiment qu'on appelle le magasin.

Débiteur et récepteur

Le magasin comprend 2 axes sur lesquels sont placés des noyaux (sortes de petits cylindres en plastique) autour desquels la pellicule se dévide et s'enroule. La pellicule vierge est placée sur l'axe débiteur, puis la pellicule exposée s'enroule sur l'axe récepteur.

Il y a différents principes dans la conception des magasins:

- le débiteur et le récepteur peuvent être dans des compartiments séparés, ou dans un même compartiment,
- la pellicule du coté débiteur et du coté récepteur peut s'enrouler soit sous forme de deux galettes situées dans le même plan: magasins en ligne, soit sous forme de deux galettes placées sur le même axe: magasins coaxiaux. Ces derniers sont donc deux fois plus larges, mais ils sont plus compacts.

3° L'objectif

L'objectif permet à l'image de se former sur la pellicule derrière la fenêtre ; il permet aussi de régler la quantité de lumière arrivant sur la pellicule.

Un objectif donne d'un objet une image réelle inversée que l'on peut recueillir sur un écran (dans notre cas la pellicule). On peut donc considérer qu'un objectif agit globalement comme une lentille convergente. Si nous considérons une lentille convergente idéale, les rayons parallèles issus d'un objet situé sur l'axe optique à l'infini convergent en un point qu'on appelle le foyer. Il y a également au centre de la lentille, un point appelé centre optique, par lequel les rayons ne sont pas déviés.

La distance focale

La distance focale c'est la distance entre le centre optique et le foyer. Cette distance s'exprime en millimètres. C'est un paramètre important qui caractérise l'objectif, c'est pourquoi on appelle souvent focale l'objectif lui-même. La distance focale définit l'angle de champ de l'objectif, elle a aussi une incidence sur le grossissement de l'image et sur les perspectives.

Quand la focale augmente, l'angle de champ diminue, l'image semble rapprochée car elle est grossie, les perspectives sont écrasées: c'est un téléobjectif, ou longue focale.

Quand la focale diminue, l'angle de champ augmente, l'image semble éloignée car elle est réduite, les perspectives sont fuyantes: c'est un grand-angulaire, ou courte focale.

Il existe des procédés optiques qui permettent de faire varier la focale d'un objectif, ce sont les objectifs à focale variable ou zoom.

I.4 Types de caméra

Il existe deux types de technologies de caméra quelles qu'en soit les applications :

I.4.1 Caméra film

C'est un appareil photo qui expose le film photographique afin de prendre une photo.

- **Film**

C'est un ruban pelliculaire de cellulose, recouvert d'une émulsion photosensible, sur lequel on enregistre des images avec un appareil cinématographique.

I.4.1.1 Différents types de film

Les distinctions peuvent être faites en fonction du format, des perforations, du fait qu'ils sont en noir ou blanc ou tout simplement en couleur.
On les classe selon :

- Les prises de vues : aujourd'hui celle-ci sont toutes professionnelles (films négatifs)
- Films positifs : pour le tirage des copies
- Films intermédiaires employés soit pour obtenir l'internégatif ou pour réaliser des effets spéciaux.
- Films noirs et blancs (haut contraste) .Employés pour la conception des titres ou pour la réalisation de certains effets spéciaux.
- Films noirs et blancs (pouvoir résolvant élevé) pour introduire le son.
- Films spéciaux : généralement utilisés pour capter les rayons infrarouges.

I.4.1.2 Principe de fonctionnement de la pellicule photographique.

La pellicule photographique est un support souple recouvert d'une émulsion contenant des composés sensibles à la lumière, généralement à base d'halogénures d'argent. Leur configuration (taille et forme de cristaux notamment) détermine les caractéristiques du film comme la sensibilité et la définition.
Lorsque l'émulsion est soumise à une exposition à la lumière dans un appareil photographique, il se forme une image visible latente. Il faut pour obtenir une image visible procéder au développement, un procédé chimique en plusieurs phases.

I.4.1.2.1 Pellicule négatif noir et blanc

Le film noir et blanc est constitué, d'une couche de protection, de cristaux d'halogénure d'argent incorporés à la gélatine, de matière plastique transparente, d'une couche anti-halo contre l'auréole crissée qui se produit autour des contours d'un cliché lorsque le sujet présente des contrastes importants.

Pour compenser ces colorations secondaires un masque est ajouté aux deux dernières couches :

*A la couche verte un masque jaune
* A la couche rouge un masque magenta et jaune soit, en soustractif, rouge.

I.4.1.2.3 Pellicule positive couleur- diapositive

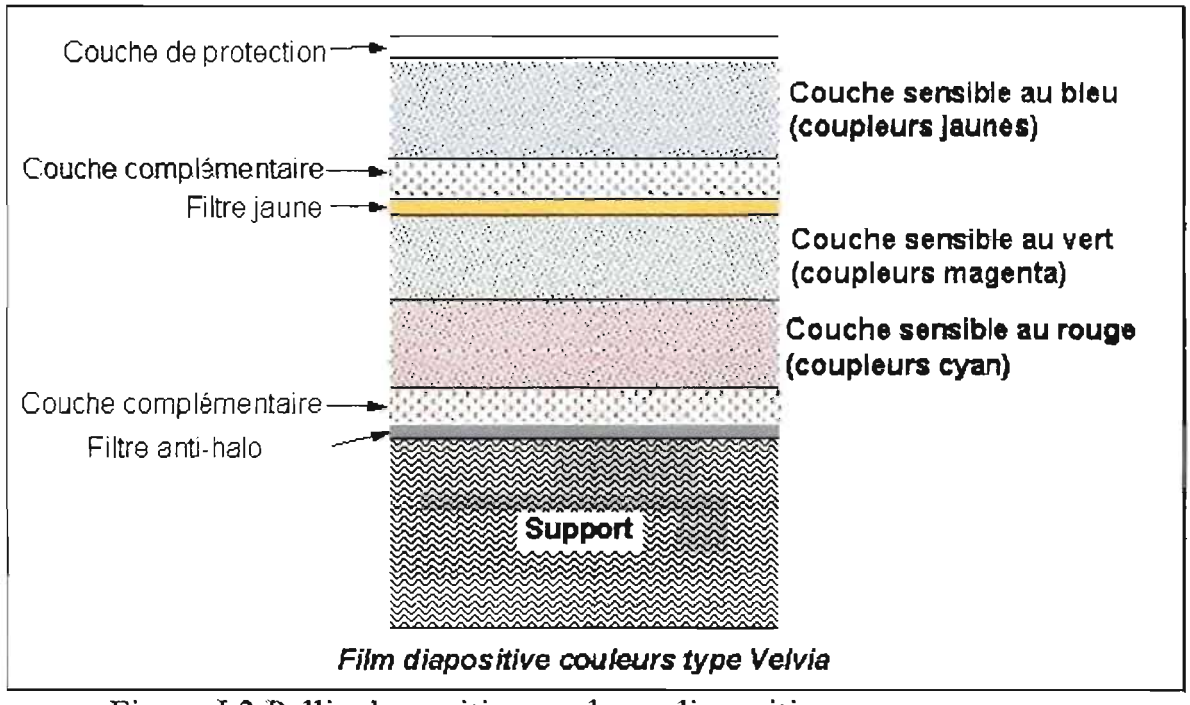


Figure I.3 Pellicule positive couleur- diapositive

Le film positif couleur permet d'obtenir directement une photo observable par transparence ou projection, la diapositive.
Le développement des diapositives se fait suivant les procédés spécifiques aux films inversibles.
Dans le cas général des diapositives ektachrome (traitement E6) l'image négative est inversée vode chimique avant de faire agir les coupleurs qui formeront au cours du développement chromogène :

- La couche sensibilisée au bleu se colore en jaune
- La couche sensibilisée au vert se colore en magenta
- La couche sensibilisée au rouge se colore en cyan.

Lors du développement, les couches filtres et anti-Hals deviennent transparentes.
Dans le cas particulier du kodachrome, le processus est plus complexe avec un traitement couche par couche (inversion puis apport du coupleur).

I.4.1.2.2 Sensibilité du film

La sensibilité du film est sa capacité à être impressionné par une quantité plus ou moins grande de lumière. Plus un film est sensible, plus l'exposition pourra être réduite.
La sensibilité est indiqué par une valeur ISO qui associe les anciennes unités ASA et DIN ASA est encore utilisé dans le langage courant un film de 400 ASA signifie ISO 400. Les valeurs ISO sont proportionnelles à la sensibilité : un film ISO 200 est 2 fois plus sensible qu'un film ISO 100. La valeur de sensibilité ISO des films disponibles varie de 25 à 1000 en couleurs. Les films standards ont une sensibilité entre 100 et 400.

1.4.1.2.3 Types d'émulsions

L'émulsion est la préparation sensible à la lumière qui recouvre les films et les papiers photographiques. Suivant les types d'émulsion, on distingue différents types de films :

- Film monochromatique « noir et blanc »
- Film argentique : on distingue :

  * Film apochromatique : sensible à toute l'étendue visible c'est le type de film par défaut utilisé en photographie
  * Film orthochromatique : très peu sensible au rouge utilisé en reproduction

- Film chromogène : il est fabriqué suivant le principe d'émulsions couleurs donc avec des couleurs ; il se développe d'ailleurs avec le procédé C41.

1.4.2.1.1 Théorie de la vidéo

Un flux vidéo est composé d'une succession d'images, 25 par seconde (25 Hz) en Europe (30 par seconde ou 30 Hz en USA), composant l'illusion du mouvement. Chaque image est décomposée en lignes horizontales, chaque ligne pouvant être considérée comme une succession de points. La lecture et la restitution d'une image s'effectue donc séquentiellement ligne par ligne comme un texte écrit : de gauche à droite puis de haut en bas.

Phénomène de scintillement

Au commencement de la télévision, la qualité des éléments phosphorescents du tube est fort médiocre.
De ce fait quand le faisceau balaye le bas de l'écran, le haut a déjà disparu, d'où un phénomène de scintillement, ressenti fortement par l'œil humain pour 25Hz ou 30 Hz. De même pour les caméras Vidéo.
Dans la première moitié du temps d'une image, une première prise de vue définit toutes les lignes impaires et une moitié d'image plus tard, une seconde prise de vue définit les lignes paires. Ce qu'il faut bien comprendre ici, c'est que les deux prises de vues sont distantes dans le temps (d'une moitié d'image). Et même si ces deux prises de vues sont complémentaires d'un point de vue spatial (les deux balayages se complètent dans le cadre), ces deux prises de vues n'affichent pas le même contenu. Si un sujet se déplace dans le champ, il aura une position différente sur chacune des deux trames. On aura un effet de zigzag sur chaque trame.

Solution du Phénomène : Entrelacement

La solution la plus simple eût été d'accélérer la cadence de balayage pour un téléviseur, mais ceci imposait également d'augmenter la cadence des images. Ce qui était inutile d'un point de vue cinématographique et fort coûteux en matériel et en bande passante. La solution plus astucieuse fut de doubler la cadence de balayage, en omettant une ligne sur deux, afin de garder une quantité d'information constante. Ainsi une première passe affiche toutes les lignes impaires en deux fois moins de temps que pour une image entière et une seconde passe affichent les lignes manquantes paires.

Les caméras qui fonctionnent comme un téléviseur inversé, adoptèrent elles aussi cet entrelacement du balayage par un dispositif de laines cristallines biréfringentes qui étalent les détails en dédoublant les rayons lumineux. Il en découle une perte de définition qui confère aux systèmes PAL et SECAM une résolution verticale multipliée par 0.7 facteur de Kells et qui n'est plus réellement que de 400 lignes environ.

La solution plus astucieuse fut de doubler la cadence de balayage, en omettant une ligne sur deux, afin de garder une quantité d'information constante. Ainsi une première passe affiche toutes les lignes impaires en deux fois moins de temps que pour une image entière et une seconde passe affichent les lignes manquantes paires.

Les caméras qui fonctionnent comme un téléviseur inversé, adoptèrent elles aussi cet entrelacement du balayage par un dispositif de laines cristallines biréfringentes qui étalent les détails en dédoublant les rayons lumineux. Il en découle une perte de définition qui confère aux systèmes PAL et SECAM une résolution verticale multipliée par 0.7 facteur de Kells et qui n'est plus réellement que de 400 lignes environ.

1.4.2.1.2 Capture de l'image

Les premières caméras vidéo fonctionnent sur le même principe que les téléviseurs, analysent l'image formée par l'objectif à l'aide d'un tube cathodique. Depuis la fin des années 1980, elles sont dotées d'un tube de capteurs CCD (Charge Coupled Divice) ou DTC (dispositif à transfert de Charges) en français :
Le transfert de ces charges peut se faire de 3 manières différentes :

-Transfert interligne (capteur IT : Interline transfer)

- Transfert trame (capteur FT : Frame Transfer qui nécessite un obturateur mécanique et est rarement utilisé

- Transfert FIT (frame Interline Transfert)

Au début du 21ème siècle, les fabricants de capteurs ont décidé d'abandonner cette technologie et construisent désormais des capteurs CMOS (Complementary Metal Oxide Semi- Conductor)

I.4.2.2.4 Résolution de l'image et fréquence de balayage

Il existe différents formats d'image vidéo, qui dépendent essentiellement de la fréquence de balayage vertical de l'image.

- 405 lignes 50 Hz (standard anglais abandonné) noir et blanc
- 525 lignes 60 Hz : résolution 4/3 utile = 720 x 480 (standard américain) couleur NTSC et PAL-N
- 625 lignes 50 Hz : résolution 4/3 utile = 720 x 576 (standard européen) couleur PAL, SECAM et NTSC-4.43

- 819 lignes 50 Hz : résolution 4/3 utile = 1024 x 768 (standard français abandonné) noir et blanc

On peut constater à ce point qu'il existe une différence entre le nombre de lignes composant l'image et le nombre de lignes affichées. Ceci représente une différence de 49 lignes en 50 Hz et de 45 lignes en 60 Hz. Ces lignes perdues sont nécessaires, elles représentent le temps nécessaire pour que le faisceau d'électrons balayant le tube cathodique puisse remonter du bas de l'image vers le haut. Ce problème technique n'existe pas avec les panneaux LCD et les dalles plasma, mais il est conservé pour assurer la compatibilité. Les lignes libres sont mises partiellement à profit : on y place les signaux du télétexte, du sous-titrage et aussi le time-code des équipements vidéo professionnels.

Il faut distinguer deux fréquences de balayage de l'image :

- Le balayage vertical, qui s'effectue de haut en bas et sert à composer l'image. Il s'effectue 50 ou 60 fois par seconde.
- Le balayage horizontal, qui s'effectue de droite à gauche pour chaque ligne de l'image. La fréquence de balayage horizontal est donc égale à la fréquence verticale multipliée par le nombre de lignes et divisée par deux à cause de l'entrelacement.

$$F_h = \frac{F_v N}{2}$$

Ceci donne les valeurs suivantes :

- Fh (50Hz) = 50 x 625 / 2 = 15625 Hz
- Fh (60Hz) = 60 x 525 / 2 = 15750 Hz

Ce résultat n'est pas dû au hasard. Si les fréquences horizontales sont presque les mêmes en 50Hz et en 60 Hz, c'est que cela permet d'utiliser la même circuiterie de balayage horizontal, donc de réaliser des économies.

CHAPITRE II TECHNIQUE DE NUMERISATION

II.1 Introduction

Les premières sondes envoyées dans l'espace étaient conçues en mode analogique. Elles étaient incapables d'envoyer des images à la base terrestre. Afin d'améliorer les services que pouvaient ces ondes, ils cherchèrent un mode ou une amélioration pouvant permettre à ces sondes de transmettre les images à la base terrestre. Ils inventèrent donc un capteur permettant la technique de numérisation des images prises par les sondes. Cette technique reste la même pour les cameras.

II.2 Acquisition des images

II.2.1 Traitement des signaux

II.2.1.1 Signal analogique

Un signal analogique est un signal plus complexe ; il peut prendre une infinité de valeurs. Il est représenté par une courbe continue dans le temps (C'est à dire il varie en fonction du temps.)

II.2.1.2 Signal numérique

Un signal numérique est un signal formé d'un nombre fini de valeurs numériques **N** dont chacune est codée sur **n** bits (c'est à dire sous forme d'un nombre entier dont la valeur maximale est limitée).

II.2.1.3 Conversion d'un signal analogique en signal numérique

II.2.1.3.1 Echantillonnage

Les convertisseurs circuits intégrés spécialisés dans les tâches de conversion **A/N** procèdent comme suit :
Ils mesurent à intervalles réguliers, la valeur du signal analogique (sa tension) et transforme aussitôt cette valeur en un nombre binaire. Cette opération s'appelle **« Echantillonnage ».**

Cet échantillonnage est plus ou moins dense en fonction de taux choisi 22000 échantillons par seconde à 22 kHz ou 96000 à 96 kHz par exemple.

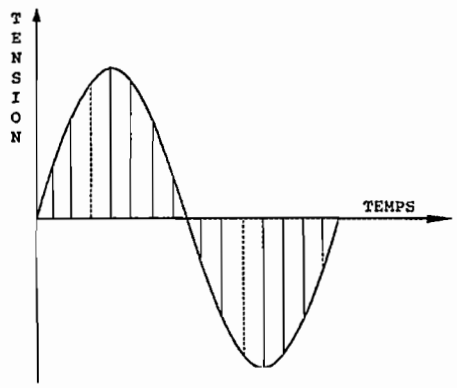


Figure II.1 Echantillonnage

II.2.1.3 Quantification

Apres échantillonnage, la chaîne d'impulsions modulées est quantifiée. Quantifier un signal consiste à placer les amplitudes des échantillons sur une échelle de valeurs à intervalles fixes. En d'autres termes c'est le découpage du signal en un nombre de points précis qui va déterminer la suite des opérations.

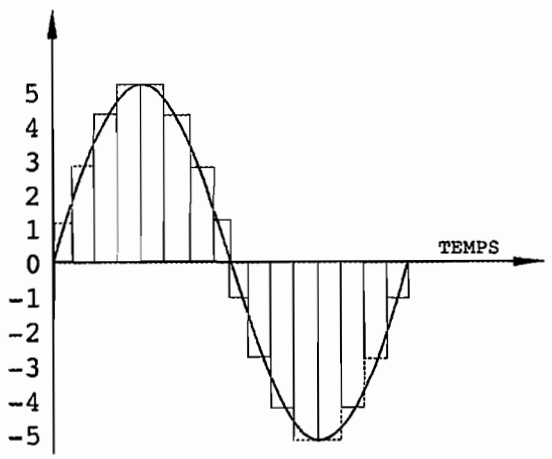
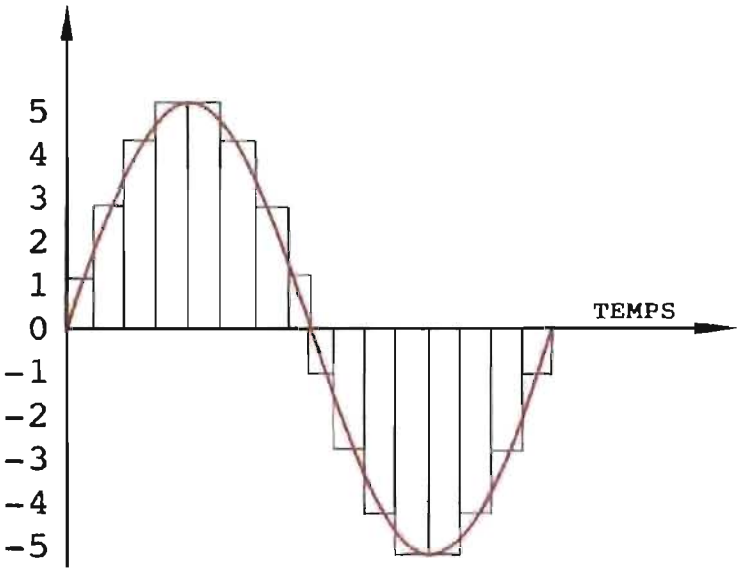


Figure II.2 Quantification

Une fois que le découpage du signal est effectué, on attribue une valeur à chaque signal. C'est là qu'intervient la résolution : en 16 bits. Cette valeur varie entre 0 et 65535(en réalité en audio entre -32768 et + 32767) et en 24 bits entre 0 et 16777215 (en réalité entre-8388608 et + 8388607).
Lorsqu'un signal ne correspond pas à un entier le convertisseur arrondit à l'entier le plus proche. Chaque arrondit induit donc une erreur, ou une déformation, par rapport au signal original. Ce sont ces erreurs que l'on nomme en français **erreur de quantification**.

II.2.1.3.3 Reconstitution du signal quantifié

Une fois les valeurs attribuées, le signal est reconstitué par le biais d'un filtre de reconstruction. Lors de cette reconstruction, le convertisseur applique un filtre passe bas qui va éliminer les plus hautes fréquences, génératrices d'erreurs par excellences. Plus le nombre de valeurs précédemment arrondies est grand, plus on devra éliminer les hautes fréquences.



Figire II.3 Signal reconstruit

Le nombre de valeurs arrondies, et donc <d'erreurs>, est directement lié au taux d'échantillonnage choisi. On comprend que théoriquement, plus on rajoute d'intervalles dans la numérisation, plus le signal reconstituée a sa chance d être fidèle à l'original.

II.2.2 Caméra numérique

II.2.2.1.1 Capteur CCD

Un capteur CCD (dispositif à transfert de charge) est un composant électronique qui sert à convertir un rayonnement électromagnétique en un signal électrique analogique. Ce signal est ensuite amplifié, puis numérisé par un convertisseur analogique et enfin traité pour obtenir une image numérique.
Bien que les capteurs CCD sont les plus populaires, il existe d'autres types de capteurs tels que, les capteurs CMOS, les capteurs FOVEON, etc.

II.2.2.1.1 Comparaison des capteurs CCD aux capteurs CMOS

Les capteurs CCD gardent beaucoup d'avantages :

- Une meilleure linéarité car moins de dispersion dans les convertisseurs Analogique/Numérique **(CAN)** ; les **CMOS** ont un convertisseur par pixel dont la dispersion augmente avec la miniaturisation.
- La surface participante à la capture des images est proportionnellement plus élevée : les capteurs **CMOS** sont encombrés par trois à six transistors ; amplification et logique d'obturation rapide.
- L'inconvénient des capteurs **CCD** est que l'électronique qui leur est associée est plus complexe avec notamment la nécessite d'horloges multiples pour piloter le transfert de charges et de tensions élevées tandis que pour les **CMOS**, l'électronique qui leur est associée est plus simple.

II.2.2.1.2 Performances des capteurs

La résolution maximale d'un capteur est en fonction du nombre de photosites qui permettront d'obtenir autant de pixels grâce à une interpolation astucieuse.

L'efficacité quantique du capteur est définie par le rapport électrons produit et photons incidents. Elle est surtout fonction de la taille de la partie active de chaque photosite(c'est à dire la surface de capture des photons)

La dynamique d'un capteur CCD est évaluée généralement par la formule suivante :

Dynamique = 20 log (Cap/C+B), en dB

où

- Cap : capacité de stockage d'un photosite en électrons ;
- C : courant d'obscurité, en électrons ;
- B : bruit de lecture, en électrons.

II.2.2.2 Capture de l'image

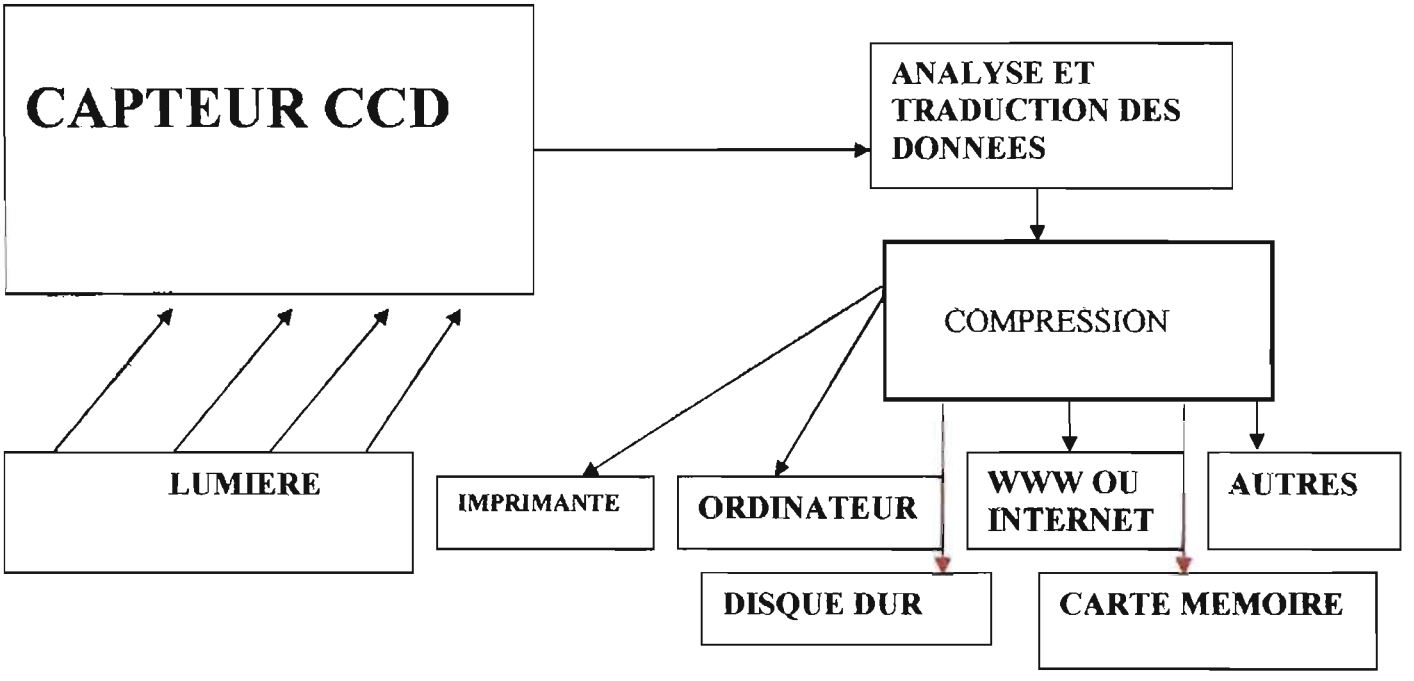


Figure II.4 Schéma de capture de l'image

La capture d'image se fait sous trois étapes :

1° Conversion des ondes lumineuses en charges électriques

Le capteur CCD est frappé par un photon (onde lumineuse). Si l'image déployé par ce photon est suffisante, la matière semi-conductrice qui compose le capteur (Silicium) réagit avec celui-ci de manière proportionnelle à la longueur d'onde de ce photon .La couche de Silicium a donc transformé le photon en une charge électrique (accumulation d'électron) qui varie en fonction de la couleur. Le signal analogique est donc transformé en charge électrique.

2° Accumulation de ces charges

Sur chaque pixel, les électrons s'accumulent, et après le temps d'intégration, on compte les électrons présents sur chacun des pixels. Cette charge a été mesurée, le signal est donc devenu numérique.

3° Transfert et interprétation des charges électriques.

Les informations (nombre d'électron) sont envoyées aux différentes puces qui composent le circuit imprimé de la caméra numérique et elles sont finalement traduites en données numériques.

II 2.1.2 Compression de l'image

La compression est une méthode qui permet de diminuer la place occupée par une image sur un support de stockage. Son principe est de diminuer le nombre de couleurs différentes d'une image.
L'œil humain ayant une perception de 2500 couleurs, alors qu'une image numérique en contient 16.7 million de plus.

Ainsi une compression consiste à examiner chacun des pixels et de changer une couleur spécifique vers une couleur plus commune : C'est la compression JPEG (Join Photographic Expert Girond). Dans certains cas, on procédera à une indexation des couleurs TZW (Temple, Zif et Welsley) noms des inventeurs

Prenons l'exemple de la compression de certaines couleurs proches du rouge. Voici la transformation de quelques couleurs à différents niveaux de compression.

Pas de compression	Compression moyennes	Forte compression
Blanc	Blanc	Blanc
Rouge Clair	Rouge Clair	Rouge
Rose	Rouge clair	Rouge
Rouge	Rouge	Rouge
Rouge foncé	Rouge foncé	Rouge
Couleurs différentes	Total : couleurs différentes	Total : 2 couleurs différentes

Tableau II.1 Compression des couleurs

II 2.2.4 Destination de l'image

Après avoir été converties, les données numérisées sont ensuite transférées vers un périphérique de sortie qui peut être : imprimante, moniteur, support magnétique ou optique, Disque Dur, Carte mémoire, etc.

II.2.2.5 Port de connexion

Pour importer une image de la caméra vers l'ordinateur, il existe deux méthodes. La première consiste à utiliser la connexion IEEE 1394 et la deuxième fait appel à la norme USB 2.0.

1° Connexion IEEE 1394

Une extrémité du câble IEEE 1394 est connectée au port DV de la caméra et l'autre extrémité du câble est branchée dans le port IEEE 1394 de l'ordinateur. Enfin, on peut importer l'image à l'aide d'un logiciel approprié de son choix.

2° Connexion USB

En premier lieu, il peut vérifier si la caméra est une caméra USB vidéo class (VCD) c'est à dire qui prend en charge le flux de données en continu sur USB.
Pour le vérifier, il suffit de brancher la caméra sur l'ordinateur, puis vérifier si dans le gestionnaire du périphérique Windows, la caméra figure en tant que « périphérique vidéo USB »

N.B : Pour déterminer le type de connexion à utiliser et savoir comment connecter votre caméra, il faut toujours consulter la documentation de la caméra.

II.3 Conclusion

La technique de numérisation d'une caméra peut être résumée par le schéma suivant :

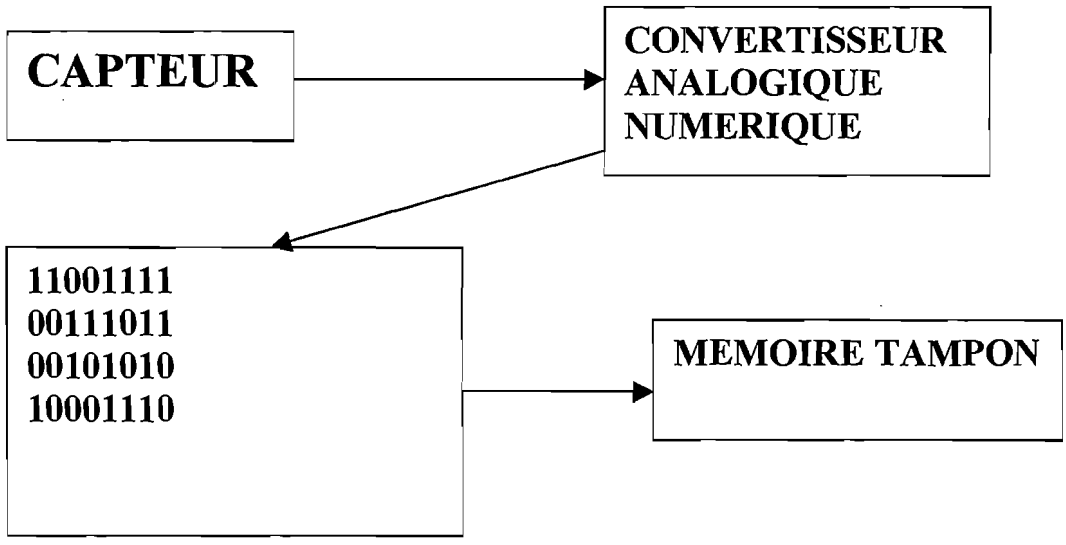


Figure II.5 Schéma de numérisation d'une camera

En résumé, deux petits schémas montrent les ressemblances et différences entre les appareils analogiques et numériques :

Appareil Analogique **Appareil Numérique**

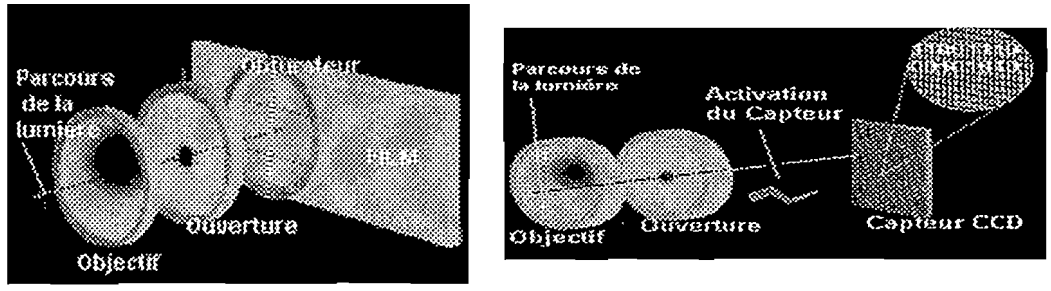


Figure II.6 Ressemblances et différences entre les appareils analogiques et numériques

CHAPITRE III SYSTEME DE VIDEO SURVEILLANCE

III.1 Introduction

La première caméra vidéo portative au monde date de 1978. Depuis ce jour, la technologie n'a cessé d'évoluer, accélérée encore par les récents développements des puces électroniques liées à l'informatique et à la micro-informatique.
Par l'utilisation des circuits amplificateurs de lumière ou par traitement infrarouge, certaines caméras sont capables aujourd'hui de filmer de jour comme de nuit, selon leur sensibilité.
La généralisation d'Internet a conduit de nombreuses entreprises à développer des Camera IP, c est à dire consultables et contrôlables via Internet, depuis n'importe où dans le monde. Contrairement aux caméras CCTV, seul les cameras IP sont capables de produire des images en haute résolution. En contre partie, la visualisation ne peut être réalisée que par l'intermédiaire d'un ordinateur ou un décodeur.

III.2 Equipements de la Vidéosurveillance

III.2.1 Type de caméras

La vidéosurveillance est généralement un système de caméras disposées dans un espace public ou privé pour le surveiller. En effet, les caméras utilisés dans ce système sont appelés caméras réseaux ou caméra IP par le fait qu'elles travaillent en réseau. On distingue :

1° Caméras réseaux fixes

Les caméras réseaux fixes, avec boîtier et objectif représentent le type de caméra réseau traditionnel. Pour certaines applications, il est important que la caméra soit visible. Dans ce cas, une caméra réseau fixe constituera un meilleur choix. Parfaitement visible, elle indique tout aussi clairement la direction dans laquelle elle pointe. Autre avantage, les caméras réseaux fixes sont équipées d'objectifs interchangeables. Pour une raison de protection renforcée, ces caméras réseaux fixes peuvent être placées dans les caissons spécialement conçus pour des installations d'Intérieur ou d'extérieur.

U. B.

Les plus connues et les plus utilisées sont :

- **Caméras réseaux à dôme fixe**

Les caméras à dôme fixe, ou mini-dômes, se composent essentiellement d'une caméra fixe préinstallée dans un caisson fixe de type dôme. Elles peuvent être orientées facilement dans n'importe quelle direction. Leur principal atout tient à leur conception discrète et à leur capacité de passer inaperçue, ainsi qu'à la difficulté de déterminer la direction dans laquelle elles pointent. Les caméras à dôme fixe sont rarement équipées d'objectifs interchangeables et même lorsque plusieurs objectifs sont possibles, leur remplacement est limité par l'espace disponible à l'intérieur du dôme.

- **Caméras réseaux PTZ**

Les avantages des caméras PTZ tiennent précisément à leurs fonctionnalités PTZ, c'est à dire à leurs options de contrôle **panoramique/inclinaison/zoom**. Dans le cas d'utilisation manuelle, les caméras PTZ s'utilisent essentiellement en intérieur et lorsqu' il importe de rendre visible la direction dans laquelle elles pointent. La plupart des caméras PTZ n'offrent pas de fonctions panoramiques à 360 degrés et ne sont pas conçues pour fonctionner en mode automatique, ou tours de garde. Le zoom optique va de 18x à 26x.

2° Caméras dôme réseau

Les caméras dôme réseau possèdent tous les avantages des caméras à dôme fixe : relativement discrètes, leurs observations ne permettent pas de déterminer la direction dans laquelle elles pointent. Contrairement aux caméras PTZ, les caméras dôme réseaux sont pourvues de fonctions panoramiques à 360 degrés. Elles possèdent également toute la robustesse nécessaire pour un fonctionnement en continu en mode tour de garde, la caméra bouge alors en continu suivant par exemple 10 présélections, de jour comme de nuit. Grâce à la fonction tour de garde, une même camera permet de couvrir une zone pour laquelle dix caméras fixes seraient nécessaires. Le principal inconvénient est qu'un seul lieu peut être surveillé à la fois, laissant ainsi les neuf autres positions sans surveillance. Le zoom optique va normalement de 18x à 30x. Dans le cas d'installation en extérieur, des zooms supérieurs à 20x s'avèrent en principe impraticables du fait des vibrations et des mouvements dus aux vents. La plus connu et la plus utilisée de ces caméras s'appelle camera réseau PTZ non mécanique.

- **Caméras réseaux PTZ non mécanique**

Les caméras PTZ dites non mécanique sont équipées d'un capteur méga pixel, elles sont capables de couvrir des angles allant de140 à 360 degrés. L'opération peut en outre réaliser des vues panoramiques, en inclinaison ou en zoom dans toutes les directions, sans aucun mouvement mécanique. Son principal avantage tient à l'absence d'usure inhérente aux parties mobiles et motorisées. Elles permettent aussi le recadrage immédiat dans une nouvelle position, une opération qui, dans le cas des caméras PTZ traditionnelles, prennent parfois une seconde. Les meilleures caméras PTZ actuelles utilisent des capteurs de trois méga pixels. Pour garantir une bonne qualité d'image, les fonctions de panoramique et d'inclinaison doivent être limitées à 140 degrés, et le zoom à 3x. Une couverture plus large ou un zoom plus élevé ont pour effet de nuire à la qualité d'image.

III.2.2 Câbles

Pour relier les divers cameras en réseau, plusieurs supports physiques de transmissions de données peuvent être utilisés. Une de ces possibilités est l'utilisation des câbles. Les câbles utilisés sont les mêmes que pour le réseau informatique. Il existe de nombreux types de câbles, mais on distingue généralement :

- Le câble de type coaxial
- La double paire torsadée
- La fibre optique

III.2.2.1 Câble coaxial

Le câble coaxial (en anglais coaxial câble) a longtemps été le câblage de prédilection, pour la simple raison qu'il est peu coûteux et facilement manipulable (poids, flexibilité,...).

Un câble coaxial est constitué d'une partie centrale (appelée âme) c'est à dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.



Figure III.1 Constitution du câble coaxial

III.2.2.1.1 Rôle des différentes parties du câble coaxial

- La gaine permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en chlorure de polyvinyle : PVC ; éventuellement en téflon).
- Le blindage (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support contre les parasites (autrement appelé bruit) pouvant causer une distorsion des données.
- L'âme accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.

Grâce à son blindage, le câble coaxial peut être utilisé sur de longues distances et à haut débit (contrairement à un câble de type paire torsadée), on le réserve toutefois pour des installations de base. A noter qu'il existe des câbles coaxiaux possédant un blindage double (une couche isolante, une couche blindage) ainsi que des câbles coaxiaux à quadruple blindage (deux couches isolantes, deux couches de blindage)

III.2.2.1.2 Types de câbles coaxiaux

On distingue habituellement deux types de câbles coaxiaux :

1° Le 10 Base 2

C'est un câble appelé ***Thinnet*** en anglais qui signifie ***réseau fin*** ou ***cheapernet*** qui signifie ***réseau plus économique***. Il a un diamètre de 6mm de couleur blanche (ou grisâtre) par convention. Il permet de transporter un signal sur une distance de 185m sans affaiblissement.

2° Le 10 Base 5

C'est un câble coaxial épais appelé ***thicknet*** ou ***thick ethernet*** en anglais et également appelé Yellow cable, en raison de sa couleur jaune. C'est un câble blinde de plus gros diamètre (12mm) et de 50 ohms d'impédance. Il a longtemps été utilisé dans les réseaux Ethernet, ce qui lui a valu l'appellation de « câble Ethernet Standard ». Etant donné que son âme a un plus gros diamètre, la distance susceptible d'être parcourue par les signaux est grande, cela lui permet de transmettre sans affaiblissement des signaux sur une distance atteignant 500m (sans réamplification du signal). Sa bande passante est de 10 Mb/s. Toutefois, étant donné son diamètre, il est moins flexible que le ***Thinnet***.

III.2.2.1.3 Connecteurs pour câble coaxial

Thinnet et ***Thicket*** utilisent tous deux des connecteurs BNC (Bayonet-Neill-Concelman ou British Naval Connector) servant à relier les câbles aux caméras ou les câbles aux ordinateurs.
Dans la famille BNC, on trouve :

- Connecteur de câble BNC : il est soudé ou serti à l'extrémité du câble.
- Connecteur BNC en T : il relie la carte réseau des ordinateurs au câble du réseau.
- Prolongateur BNC : il relie deux segments de câble coaxial afin d'obtenir un câble plus long.
- Bouchon de terminaison BNC : il est placé à chaque extrémité d'un réseau en bus pour absorber les signaux parasites. Il est relié à la masse. Sans le bouchon de terminaison BNC, le réseau en Bus ne peut pas fonctionner.

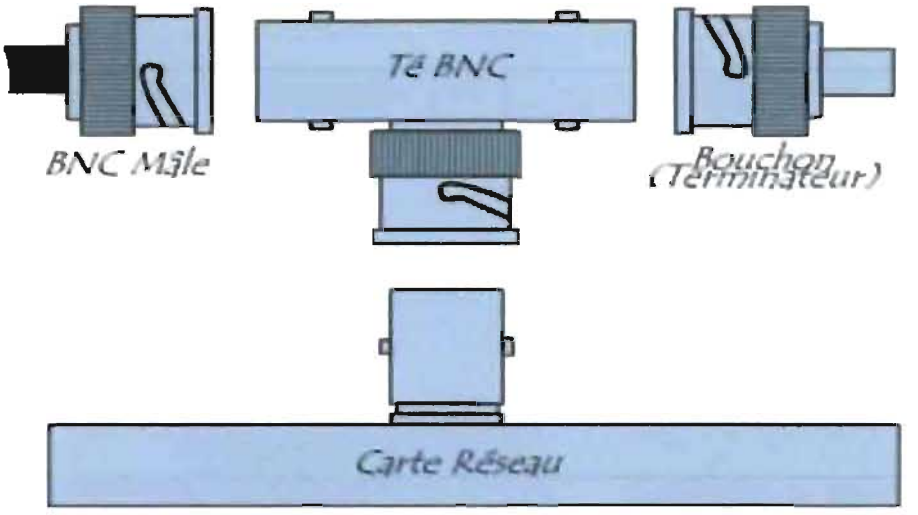


Figure III.2 Connecteur du câble coaxial

III.2.2.2 Câble à paire torsadée

Dans sa forme la plus simple, le câble paire torsadée est constitué de deux brins de cuivre entrelacés en torsade et recouvert d'isolant. Ce câble est souvent fabriqué à partir de plusieurs paires torsadées regroupées et placées à l'intérieur de la gaine protectrice. L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou autres sources (moteur, relais, transformateur). La paire torsadée est donc adaptée à la mise en réseau local d'un faible parc avec un budget limité, et une connectique simple. Toutefois, sur de longues distances avec des débits élevés elle ne permet pas de garantis, l'intégrité des données (c'est-à-dire la transmission sens perte des données)

III.2.2.2.1 Types de câbles à paire torsadée

On distingue généralement deux types de câble à paire torsadée :

- Câble à paire torsadée blindée (STP)
- Câble à paire torsadée non blindée(UTP)

1° Câble à paire torsadée blindée (STP)

Le câble STP (Schielded Twisted Pair) utilise une des cuivres de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP.

1° Câble à paire torsadée blindée (STP)

Le câble STP (Schielded Twisted Pair) utilise une des cuivres de meilleure qualité et plus protectrice que la gaine utilisée par le câble UTP.
Il contient une enveloppe de protection entre les paires et autour de paire. Dans les câbles STP, les fils de cuivre d'une paire sont eux mêmes torsadés, ce qui fournit au câble STP un excellent blindage (c'est-à-dire une meilleure protection contre les interférences). D'autres parts il permet une transmission plus rapide et sur une plus longue distance.

2° Câble à paire torsadée non blindée(UTP)

Le câble UTP obéit à la spécification 10 base T. C'est le type de paire torsadée le plus utilisé et le plus répandu. Voici quelques caractéristiques :

- Longueur maximale d'un segment : 10 mètres
- Composition : 2 fils de cuivres recouverts d'isolant
- Normes UTP : conditionnent le nombre de torsion par pied (33 cm) de câble en fonction de l'utilisation prévue

U T P : Répertorié dans la norme commercial Building Wiring Standard 568 de l'EIA/TIA (Electronic Industries Association/ Telrcommunication Industries Association). La raison EIA/ TIA 568 a utilisé U T P pour créer des normes applicables à toutes sortes de taux et de contextes de câblage qui garantissent au public l'homogénéité des produits. Ces normes incluent cinq catégories de câble U T P :

- Catégorie 1 : câble téléphonique traditionnel (transfert de voix mais pas de données)

- Catégorie 2 : transmission des données à 4Mbit/s maximum (RNIS). Ce type de câble est composé de 4 paires torsadées.
- Catégorie 3 : 10Mbit/s maximum. Ce type de câble est composé de 4 paires et 3 torsions par pied.
- Catégorie 4 : 16Mbits/S maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.
- Catégorie 5 : 100% Mbits/S maximum. Ce type de câble est composé de 4 paires torsadées en cuivre.

III.2.2.2.2 Connecteur pour le câble à paire torsadée

La paire torsadée se branche à l'aide d'un connecteur RJ-45. Ce connecteur est similaire au RJ-11 utilisé dans la téléphonie mais différent sur certains points : le RJ-45 est légèrement plus grand et ne peut être inséré dans une prise de téléphone RJ-11. De plus, le RJ-45 se compose de 8 broches alors que le RJ -11 n'en possède que six, voire quatre également.

N.B : Pour que ce câble soit utilisé sur une caméra, cette dernière doit avoir un port RJ-45.

III.2.2.3 Fibre optique

La fibre optique est un câble possédant de nombreux avantages :

- Légèreté
- Immunité
- Faible atténuation
- Tolère des débits de l ordre de 10Mbps
- Largeur de bande de quelques dizaines de mégahertz (fibre monomode)

Le câblage optique est particulièrement adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments, appelée ***backbone***, ou épisse dorsale) car elle permet des connexions sur des longues distances (de quelques kilomètres à 60 km dans le cas des fibres monomodes) sans nécessiter de mise à la masse. De plus, ce type de câble est très sûr car il est extrêmement difficile de mettre un tel câble sur écoute. Toutefois, malgré sa flexibilité mécanique, ce type de câble ne convient pas pour des connexions dans un petit réseau ou réseau local, car son installation est problématique et son coût est élevé. C'est la raison pour laquelle on préférera la paire torsadée ou le câble coaxial pour des petites liaisons.

III.2.3 Enregistreur Vidéo Numérique ou DVR

Un enregistreur vidéo numérique est un magnétoscope de vidéosurveillance, connecté avec une ou plusieurs caméras CCTV. Il est muni d'un périphérique de stockage à l'intérieur (disque dur). Avec ces fonctionnalités évoluées d'enregistrement sur détections des mouvements, disparition d'objet, faire de comptage, etc, il devient un central de vidéosurveillance.

III.3 Différents systèmes de connexion de réseaux cameras

III.3.1 Système sur réseau IP

1° connexion avec un réseau local (LAN)

Les caméras prennent des images en cas d'intrusion et les envoient par le réseau sur n'importe quel PC du réseau et visualisées en temps réel .

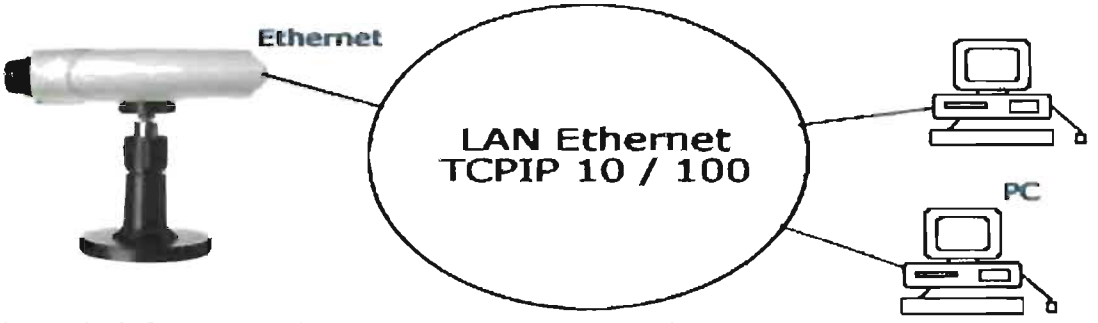


Figure III.3 Connexion d'une camera avec un réseau local

2° Connexion directe avec la carte réseau du PC

La caméra prend des images en cas d'intrusion et les envoient par le réseau sur le serveur FTP installé sur votre PC. On peut se connecter en direct sur la camera et regarder en temps réel ce qui se passe.

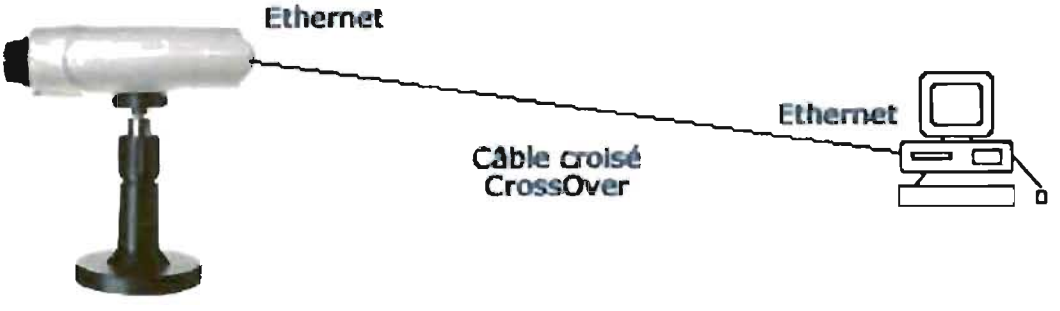


Figure III.4 Connexion directe avec la carte réseau

3° Connexion permanente avec un routeur à Internet

Les caméras prennent des photos en cas d'intrusion et les envoient sur un serveur FTP. On peut se connecter avec n'importe quel PC dans le monde sur la caméra et regarder en temps réel ce qui se passa. Par exemple, l'animation des sites Internet ; les cameras sont visibles en direct par les internautes du monde entier.



Figure III.5 Connexion permanente avec un routeur à l'internet

III.3.2 Kit de Vidéosurveillance

On entend par KIT le genre de cameras utilisées dans les petits magasins par exemple. Il regroupe en général une ou deux cameras et un moniteur. Ces systèmes sont plutôt utilisés à titre de prévention et n'enregistrent pas ce qu'ils voient. C'est en quelque sorte de la Vidéosurveillance bon marché qui est proposé comme une solution de sécurité peu couteuse.

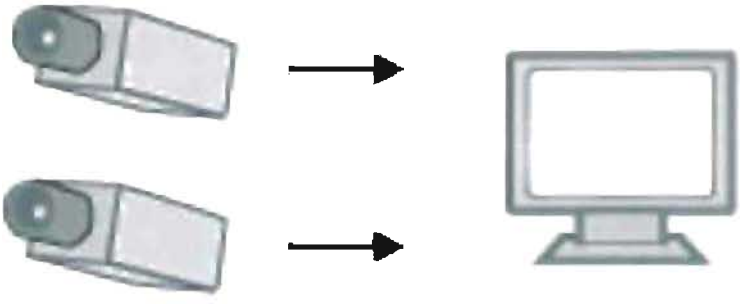


Figure III.6 Caméra avec accessoires de visualisation

III.3.3 Réseau classique de vidéosurveillance

Le réseau classique est encore base sur un système analogique, avec dans la plupart des cas un enregistrement limité dans la durée. Il s'agit d'une des méthodes les plus anciennes, également les plus répandues dans un grand nombre d'établissements.

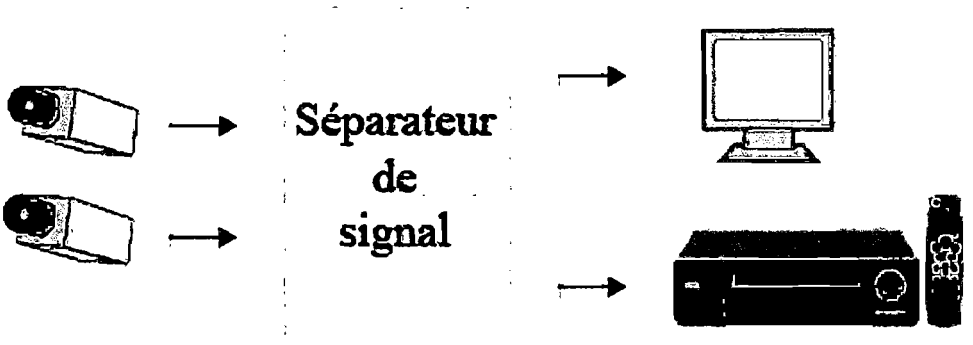


Figure III.7 Réseau classique de la vidéosurveillance

III.3.4 Système hybride de vidéosurveillance

Le système hybride intègre les systèmes classiques de vidéosurveillances basés sur les caméras analogiques et les caméras en réseaux. Il permet d'intégrer aisément les deux types de systèmes en place sur un seul serveur ou faciliter l'évolution d'un système de vidéosurveillance analogique vers le numérique, sans remettre en cause l'existant, et introduire de nouvelles fonctions comme la détection, disparition, apparition de l'objet, le comptage d'objet ou de personne.

III.3.3 Réseau classique de vidéosurveillance

Le réseau classique est encore base sur un système analogique, avec dans la plupart des cas un enregistrement limité dans la durée. Il s'agit d'une des méthodes les plus anciennes, également les plus répandues dans un grand nombre d'établissements.

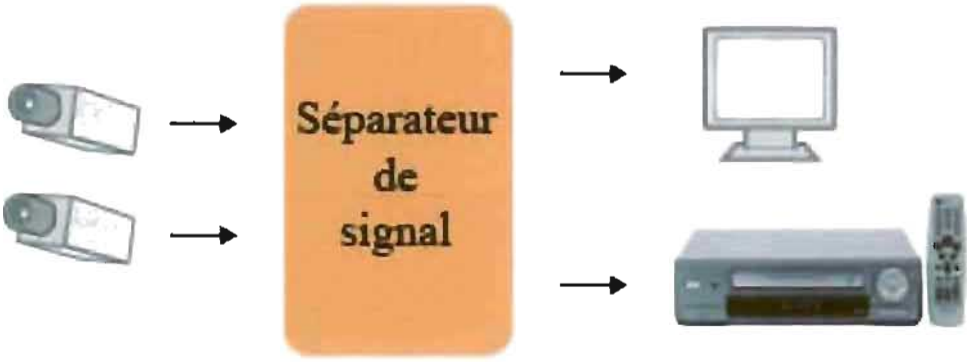


Figure III.7 Réseau classique de la vidéosurveillance

III.3.4 Système hybride de vidéosurveillance

Le système hybride intègre les systèmes classiques de vidéosurveillances basés sur les caméras analogiques et les caméras en réseaux. Il permet d'intégrer aisément les deux types de systèmes en place sur un seul serveur ou faciliter l'évolution d'un système de vidéosurveillance analogique vers le numérique, sans remettre en cause l'existant, et introduire de nouvelles fonctions comme la détection, disparition, apparition de l'objet, le comptage d'objet ou de personne.

II^{ème} PARTIE: INTRODUCTION AU DOMAINE DU RESEAU INFORMATIQUE

CHAPITRE IV : NOTION SUR LES RESEAUX INFORMATIQUES

IV.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations. Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet), on appelle nœud (node) l'extrémité d'une connexion qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur)

Indépendamment de la technologie sous-jacente, on porte généralement une vue matricielle sur ce qu'est un réseau. De façon **horizontale**, un réseau est une strate de trois couches : les infrastructures, les fonctions de contrôle et de commande, les services rendus à l'utilisateur. De façon verticale, on utilise souvent un découpage géographique : réseau local, réseau d'accès et réseau d'interconnexion.

IV.2 Intérêt d'un réseau informatique

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à Internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Le jeu vidéo multi joueurs

Les réseaux permettent aussi de standardiser les applications, on parle généralement de ***groupware*** pour qualifier les outils permettant à plusieurs personnes de travailler en réseau.

Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement. Voici un aperçu des avantages qu'offrent de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques,
- Standardisation des applications,
- Accès aux données en temps utile,
- Communication et organisation plus efficace.

IV.3 Classification des réseaux

On distingue différents types de réseaux (privés) selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux :

1° **LAN** signifie Local Area Network (**en français Réseau Local**). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs. En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'égal à égal (**en anglais Peer to Peer**), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire
- dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseau aux utilisateurs

2° **MAN** (Metropolitan Area Network) interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux noeuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

3°WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LAN à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un noeud du réseau. Le plus connu des WAN est Internet.

	WAN	MAN	LAN
Taille géographique	quelques milliers de kilomètres	de 1 à 100 km	de 1 à 2km
Nombre d'abonnés	plusieurs milliers	de 2 à 1000	de 2 à 200
Opérateur	différents utilisateurs	regroupement d'utilisateurs	l'intéressé lui - même
Facturation	volume et durée	forfait	gratuit
Débit	de 50 bits à 2 Mbits/s	de 1 à 100 Mbit/s	de 1 à1000 Mbit/s
Taux d'erreurs	de 10^{-3} à 10^{-6}	$>10^{-9}$	$> 10^{-9}$
Délais	< 0.5 s	de 1 ms à 100 ms	de 1 à 100 ms

Tableau IV.1: Caractéristiques de différents réseaux

IV.4 Topologie des réseaux

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).

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

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes :

IV.4.1 Topologie en bus

Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

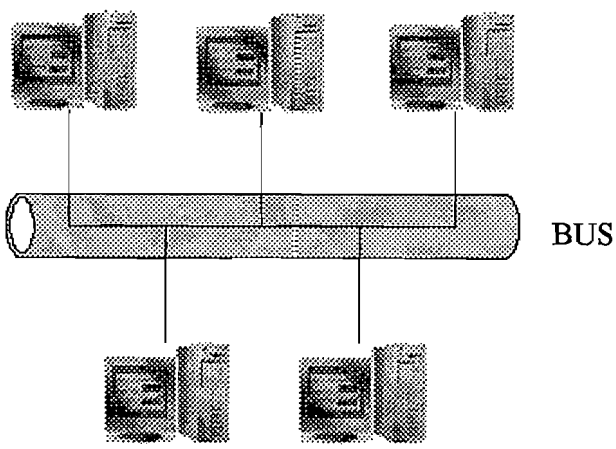


Figure IV.1 : Topologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

IV.4.2 Topologie en étoile

Dans une topologie en étoile, les ordinateurs sont reliés par des segments de câble à un composant central appelé concentrateur (***hub***). Par l'intermédiaire du concentrateur, les signaux sont transmis depuis l'ordinateur émetteur vers tous les ordinateurs du réseau. Les réseaux en étoile apportent une administration et des ressources centralisées. Cependant, comme chaque ordinateur est relié à un point central, cette topologie exige davantage de câblage dans le cas d'un grand réseau. De plus, si le point central tombe en panne, le réseau tout entier est mis hors service.

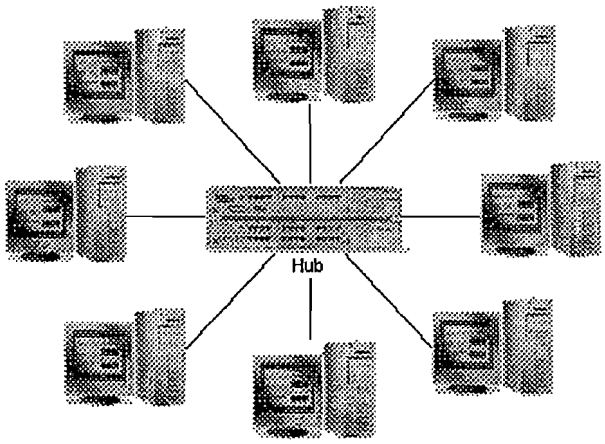


Figure IV.2 : Topologie en étoiles

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

IV.4.3 Topologie en anneau

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

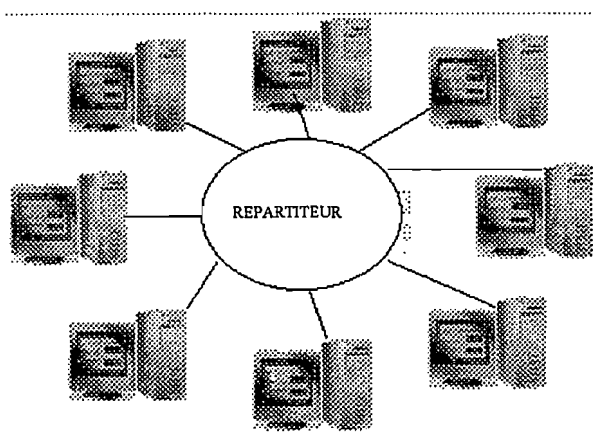


Figure IV.3 Topologie en anneau

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-deux un temps de parole.

Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI.

IV.4.4 Comparaison des différentes topologies

A chaque topologie correspondent des méthodes d'accès au support physique différentes et chaque topologie a ses faiblesses et ses avantages

Topologie	Avantages	Inconvénient
Bus	Economise la longueur de câble. Support peu coûteux. Simple et fiable. Facile à étendre.	Ralentissement possible du réseau lorsque le trafic est important. Problèmes difficiles à isoler. La coupure du câble peut affecter de nombreuses stations.
Anneau	Accès égal pour tous les ordinateurs. Performances régulières même si les utilisateurs sont nombreux.	La panne d'un seul ordinateur peut affecter le reste du réseau. Problèmes difficiles à isoler.
Etoile	Il est facile d'ajouter de nouveaux ordinateurs et de procéder à des modifications. Contrôle et administration centralisés. La panne d'un seul ordinateur n'a pas d'incidence sur le reste du réseau.	La reconfiguration du réseau interrompt le fonctionnement de celui-ci. Si le point central tombe en panne, le réseau est mis hors service.

Tableau IV.2 : Comparaison des différentes topologies

IV.5 Architecture de réseau: le modèle OSI

L'agencement d'un système en couches permet de réduire sa complexité. Le modèle OSI (Open Systems Interconnexion) ou ISO en français, définit une structure de référence en 7 couches individualisées pour les systèmes de communication de données.

Deux normes sont définies pour chaque couche:

- une norme qui spécifie l'interface pour accéder aux services de la couche depuis la couche supérieure;
- une norme qui définit le protocole par lequel les services sont fournis.

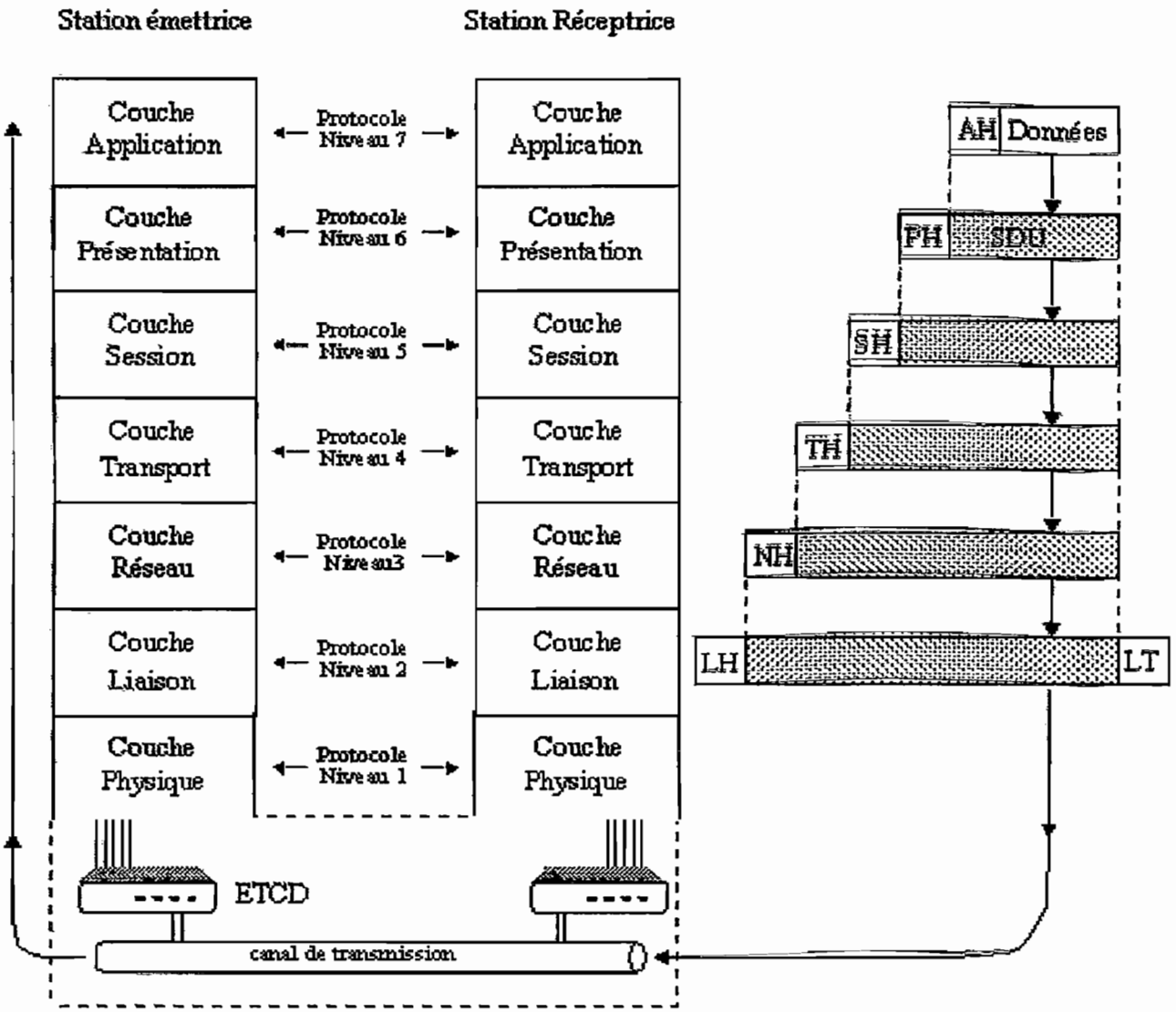
La normalisation des interfaces de service libère l'utilisateur du besoin de connaître les protocoles utilisés. Ceci permet de prédire et contrôler les conséquences des changements effectués dans un réseau, notamment lors d'une réorganisation des couches inférieures qui se fait ainsi de manière transparente pour les couches supérieures (par exemple.. changement de site d'un serveur, changement de la technologie du réseau, ...).

Le modèle OSI permet également de fournir un langage et un cadre facilitant la description et l'interconnexion des systèmes hétérogènes.

Ce modèle est contraignant et souvent plus coûteux dans les traitements spécialisés, mais il a l'énorme avantage de diminuer la tendance "spécifique constructeur" et donc de permettre une meilleure compatibilité et interopérabilité des systèmes.

Les protocoles des systèmes actuels tendent à converger vers le modèle OSI, mais pour des raisons historiques ils recouvrent parfois plusieurs couches et sont donc dans ce cas incomplètement décrits par le modèle.

Exemple de normalisation: communication interprocessus par socket sous UNIX est remplacé par le service de transport ISO 8072 indépendant du système et du réseau.



AH: Application Header
PH: Presentation Header
SH: Session Header
TH: Transport Header
NH: Network Header
LH: Link Header
LT: Link Trailer
SDU: Service Data Unit

ETCD: Equipement Terminal de Circuit de Données (DCE en anglais)

Figure IV.4 Schéma du modèle OSI à 7 niveaux

Figure IV.4 Schéma du modèle OSI à 7 niveaux

IV.5.1 Les sept couches du modèle OSI

Le modèle ISO (Interconnexion des Systèmes Ouverts) d'architecture des réseaux informatiques définit les 7 couches suivantes:

1. **Physique**

   Cette couche définit les caractéristiques physiques des signaux et des supports utilisés pour l'interconnexion des systèmes. Elle est également responsable de l'activation, du maintien, et de la désactivation des circuits de l'ETCD, ainsi que des signaux d'horloge.
   Il existe une myriade de normes pour ce niveau (par exemple EIA-232, V22bis et IEEE 802.3 sont des protocoles au niveau physique).

1. **Liaison de données**

   Cette couche est responsable de l'échange de blocs d'information sur une ligne (détection, correction d'erreurs, adressage). Elle est subdivisée en deux sous-couches dans la norme IEEE 802 (sous-couches MAC et LLC).

2. **Réseau**

   Cette couche réalise l'interface utilisateur avec le réseau, et gère l'adressage et le transfert des données vers la machine destinataire à travers le ou les réseaux connectés.

3. **Transport**

   Ce niveau est responsable du contrôle du transport de bout en bout (réordonnancer des paquets, demande de réémission,...). Elle fournit l'interface permettant à l'utilisateur de paramétrer la qualité (et donc le coût) de l'acheminement des données. C'est le premier niveau permettant de gérer les erreurs dues au passage à travers plusieurs liens (réseaux). Elle fournit 2 principaux types de service: avec connexion (circuit virtuel) ou sans connexion (paquets indépendants).

4. **Session**

   Cette couche fournit une interface permettant de gérer la synchronisation de la communication entre processus distants (rendez-vous, point de reprise, resynchronisation de l'échange de données).

5. **Présentation**

   Ce niveau est responsable de la présentation des données sous un format (une syntaxe) lisible par l'application. Par exemple:
   - passage du code ASCII au code EBCDIC ou VIDEOTEXTE,
   - passage de la représentation binaire BIG ENDIAN à LITTLE ENDIAN,
   - mappage d'un format de commande terminal virtuel à celui du terminal,
   - compression, décompression de données.

6. **Application**

   Cette couche comprend les programmes d'application avec leurs conventions d'échange et de coopération. C'est la seule couche qui s'occupe de la sémantique des données transférées. On y trouvera des protocoles spécifiques à certains types d'applications (par exemple: applications bancaires, réservation de places, messagerie électronique, terminal virtuel, prises de commande, ...).

Dans le modèle OSI, la numérotation des couches commence par le bas, c'est à dire par le matériel. La présentation adoptée dans le tableau ci-dessous respecte l'usage général (matériel en bas, logiciel d'application en haut). Le modèle OSI comporte 7 couches.

Le modèle OSI		
Couche	**Fonction**	**Exemple**
Couche n° 7 : application (couche sémantique)	Gère l'échange des données entre deux ordinateurs	Couches supérieures du navigateur
Couche n° 6 : présentation (couche syntaxique)	Assure l'intégrité des données quelle que soit la plate-forme	
Couche n° 5 : session	Gère les communications entre les deux systèmes	HTTP (protocole du World Wide Web)
Couche n° 4 : transport	Assure le transport et l'intégrité des données	TCP (mise en paquets selon le protocole d'Internet)
Couche n° 3 : réseau	Assure le routage des données sur le réseau	IP (adressage des paquets selon le protocole d'Internet)
Couche n° 2 : liaison des données	Contrôle le flux des informations	Ethernet : mise en "frames", gestion des collisions
Couche n° 1 : couche physique	Spécifie le matériel du réseau et son fonctionnement	Ethernet : matériel & signaux, codage des bits, etc.

Tableau IV.3 : Fonction des différentes couches du modèle

Dans le tableau ci-dessus, nous avons pris l'exemple d'un ordinateur client, relié à Internet grâce au réseau local de l'entreprise. Lorsque l'internaute interroge le web, le programme d'application qu'il utilise est un navigateur : Internet Explorer de Microsoft ou Communicator (ex-Navigator) de Netscape. La demande d'information qu'il formule (par exemple : télécharger une page web donnée) est mise en forme selon le protocole HTTP du web. Les données ainsi générées sont mises en paquets en accord avec le protocole TCP d'Internet. Chaque paquet reçoit une adresse conforme au protocole IP d'Internet. Il est ensuite introduit dans un "frame" Ethernet, puis expédié sur le réseau de l'entreprise. Tout se passe comme si nous parcourions le modèle OSI en descendant. Lorsque la réponse arrive du serveur web, les mêmes opérations se déroulent en sens inverse : tout se passe comme si nous parcourions le modèle OSI en montant Comme nous le constatons, le modèle OSI permet de décomposer en étapes successives les opérations qu'effectue le système informatique, lorsqu'il envoie ou reçoit l'information.

IV.6 Réseaux locaux

IV.6.1 Objectifs des réseaux locaux

Les réseaux locaux diffèrent des réseaux MAN et WAN par leurs objectifs et caractéristiques. Un réseau local d'entreprise RLE représente un système de communication locale reliant plusieurs ordinateurs (serveur, stations de travail et périphérique) permettant de transféré des données à des vitesses élevées sur des courtes distances et dans les limites d'une enceinte privée.
Le réseau local a les objectifs suivants :

- la mise en commun des données communes à plusieurs utilisateurs
- le partage d'un accès à l'Internet
- le partage des périphériques (FAX, MODEM, IMPRIMANTE, LECTEUR DE CD ROM,...etc.)
- le partage des applications (exemple : partage d'un progiciel d'application)
- l'accès à un site Internet

IV.6.2 Caractéristiques des réseaux locaux

Les caractéristiques suivantes sont communes à tous les réseaux locaux et permettent d'atteindre les objectifs fixés par les utilisateurs.

Liaisons multipoints symétriques : multipoints est en opposition avec les liaisons point à point qui permettent de relier uniquement deux équipements comme deux ponts reliant deux LAN d'une entreprise qui possède plusieurs bâtiments par exemple. Multipoints signifie qu'il y a plusieurs entrées sur la liaison. Symétrique signifie que l'on veut que tous les équipements reliés puissent discuter directement entre eux et non comme dans les réseaux où il y a un poste principal dit contrôleur où un poste désirant communiquer avec un autre s'adresse au contrôleur qui passe le message au destinataire.

Distance limité : pour obtenir des débits élevés, les réseaux locaux limitent leurs tailles de quelques dizaines de mètres à une dizaine de kilomètres. L'objectif étant de partager des équipements, cette distance est suffisante.
Haut débit global : les WAN ont souvent des débits bas. Par contre, un LAN s'efforce d'obtenir des débits élevés. Par exemple, Ethernet a un débit de 10Mbps à 1Gbps

Faible taux d'erreurs : le taux d'erreur correspond au nombre de bits qui s'inversent sur le nombre de bits transmis. Pour le LAN le taux d'erreur est 10^{-9}, souvent 10^{-12}
Un taux de 10^{-9} signifie qu'un bit sur un milliard inverse. Ce chiffre paraît impressionnant mais sur Ethernet 10Mbps, cela correspond à plus d'une erreur toutes les minutes. Pour obtenir de hauts débits, on ne peut pas se permettre d'émettre et de demander un accusé de réception, il faut émettre en continu, en supposant que la réception est bonne. C'est pour cela qu'il est important d'avoir des taux d'erreurs aux alentours de 10^{-12} ce qui correspond à moins d'une erreur toutes les 27 heures.

Diffusion : elle signifie dans notre cas que lorsqu'un poste d'un réseau local émet, tous les autres l'entendent. Et si un poste entend un message qui n'est pas pour lui il ignore le message.

Faible délais d'accès au disque : ce partage des fichiers nécessite des accès aux disques distants rapides, sinon l'utilisateur transfère sur son disque le fichier et le renvoie sur le disque partagé. Ceci pose un problème de cohérence lorsque plusieurs utilisateurs veulent accéder à un ficher. Avec un LAN, le temps d'accès à un disque local est faible.

Privé : les réseaux locaux doivent être administrés par leurs propriétaires : on ne passe pas par un opérateur.

Grand nombre d'utilisateurs : les réseaux locaux sont évidemment conçus pour accueillir un grand nombre de postes.

IV.6.3 Constituants matériels d'un réseau local

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants :

- **La carte réseau** (parfois appelé coupleur): il s'agit d'une carte connectée
- **Le transceiver** (appelé aussi adapteur): il permet d'assurer la transformation des signaux
- **La prise**: il s'agit de l'élément permettant de réaliser la jonction mécanique
- **Le support physique d'interconnexion**:

  - Le câble coaxial

  - La paire torsadée

  - La fibre optique

Voici reprises, de manière synthétique dans le tableau ci-dessous, les principales caractéristiques des câbles déterminantes quant au choix à effectuer.

	Paire torsadée	**Câble coaxial**	**Fibre optique**
Coût	Faible	Moyen	Assez élevé
Bande passante	Moyenne	Large	Très large
Longueur maximale	Moyenne	Elevée	Elevée
Immunité aux interférences	Basse (UTP) Moyenne (STP)	Moyenne à élevée	Très élevée
Facilité de connexion	Simple	Variable	Difficile
Facilité d'installation	Variable	Variable	Difficile
Fiabilité	Bonne	Bonne	Très bonne

Tableau IV.4 : Principales caractéristique des câbles

IV.6.4 Différents types de réseaux locaux

On distingue généralement les deux types de réseaux suivants :

- Les réseaux poste à poste (Peer to Peer / égal à égal)
- Réseaux organisés autour de serveurs (Client/Serveur)

Ces deux types de réseau ont des capacités différentes. Le type de réseau à installer dépend des critères suivants :

- Taille de l'entreprise
- Niveau de sécurité nécessaire
- Type d'activité
- Niveau de compétence d'administration disponible
- Volume du trafic sur le réseau
- Besoins des utilisateurs du réseau
- Budget alloué au fonctionnement du réseau (pas seulement l'achat mais aussi l'entretien et la maintenance)

IV.6.4.1 Présentation de l'architecture d'égal à égal

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

IV.6.4.1.1 Inconvénients des réseaux d'égal à égal

Les réseaux d'égal à égal ont énormément d'inconvénients :

- ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer
- la sécurité est très peu présente
- aucun maillon du système n'est fiable

Ainsi, les réseaux d'égal à égal ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

IV.6.4.1.2 Avantages de l'architecture d'égal à égal

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance)
- une simplicité à toute épreuve!

IV.6.4.1.3 Mise en œuvre d'un réseau d'égal à égal

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés. On peut donc utiliser Windows NT Workstation, Windows pour Workgroups ou Windows 95 car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

La mise en œuvre d'une telle architecture réseau repose sur des solutions standard :

- Placer les ordinateurs sur le bureau des utilisateurs
- Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité
- Pour les connexions, on utilise un système de câblage simple et apparent

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- Moins de 10 utilisateurs
- Tous les utilisateurs sont situés dans une même zone géographique
- La sécurité n'est pas un problème crucial
- Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir

IV.6.4.1.4 Administration d'un réseau poste à poste

Le réseau poste à poste répond aux besoins d'une petite entreprise mais peut s'avérer inadéquat dans certains environnements. On désigne par le terme "Administration" :

- Gestion des utilisateurs et de la sécurité
- Mise à disposition des ressources
- Maintenance des applications et des données
- Installation et mise à niveau des logiciels utilisateurs

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, etc.).

IV.6.4.1.5 Notions de sécurité

La politique de sécurité minimale consiste à mettre un mot de passe à une ressource. Les utilisateurs d'un réseau poste à poste définissent leur propre sécurité et comme tous les partages peuvent exister sur tous les ordinateurs, il est difficile de mettre en œuvre un contrôle centralisé. Ceci pose également un problème de sécurité globale du réseau car certains utilisateurs ne sécurisent pas du tout leurs ressources. .

IV.6.4.2 Présentation de l'architecture client/serveur

L'architecture **client/serveur** désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs postes clients du serveur : chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique.

Caractéristiques d'un serveur :

- il est initialement passif (ou esclave, en attente d'une requête) ;
- il est à l'écoute, prêt à répondre aux requêtes envoyées par des clients ;
- dès qu'une requête lui parvient, il la traite et envoie une réponse.

Caractéristiques d'un client :

- il est actif le premier (ou maître) ;
- il envoie des requêtes au serveur ;
- il attend et reçoit les réponses du serveur.

Le client et le serveur doivent bien sûr utiliser le même protocole de communication.

IV.6.4.2.1 Avantages

- toutes les données sont centralisées sur un seul serveur, ce qui simplifie les contrôles de sécurité et la mise à jour des données et des logiciels ;
- les technologies supportant l'architecture client/serveur sont plus organisées que les autres.

IV.6.4.2.2 Inconvénients

- si trop de clients veulent communiquer avec le serveur au même moment, ce dernier risque de ne pas supporter la charge (alors que les réseaux pair à pair fonctionnent mieux en ajoutant de nouveaux participants) ;
- si le serveur n'est plus disponible, plus aucun des clients ne marche (le réseau pair à pair continu à fonctionner, même si plusieurs participants quittent le réseau). Les coûts sont élevés.

IV.7 Réseau local sans fil

IV.7.1 Définition

Un réseau sans fil est un réseau informatique qui connecte différents postes ou systèmes entre eux non pas par liaison filaire mais plutôt par ondes radio. Les réseaux sans fils constituent avant tout une alternative aux réseaux câblés. Leur compatibilité avec les réseaux câblés permet également de les y ajouter comme extensions. Grâce aux réseaux sans fil un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour la quelle on entend parler de mobilité. La norme la plus utilise est la norme IEE802.11mieux connue sous le nom de WI-FI.

IV.7.2 Cas d'utilisation

Ils sont généralement utilisés dans les cas suivants ;
- Pour réaliser des réseaux temporaires très rapidement (conférence, réunion)
- Pour permettre d'éviter de gros travaux de câblages dans des endroits où c'est difficile, même prohibé
- Pour donner la possibilité de transmettre des données dans le cas d'application mobile.

IV.7.3 Réglementation

Deux organismes gèrent la normalisation des bandes de fréquences attribués aux réseaux sans fil ; le centre américain IEEE et le centre européen ETSI. Une fois les normes établies, des commissions distribuent ces fréquences aux utilisateurs selon la taille du réseau créée.

IV.7.4 Equipements nécessaires pour un réseau local sans_fil

IV.7.4.1Carte réseau sans fil.

Une carte réseau sans fil est un adaptateur ou une carte d'extension installée dans un ordinateur portable ou de bureau permettant a l ordinateur de se connecter a un réseau sans fil.

IV.7.4.2 Routeur sans fil.

Un routeur est un équipement assurant la gestion des accès à Internet sans qu'il soit nécessaire d'établir une connexion téléphonique. Les routeurs peuvent connecter simultanément plusieurs ordinateurs à Internet et combiner les services voix et données.

IV.7.5 Exemple d'une installation d'un réseau local sans fil.

IV.7.5.1 Préparation de l'installation

Certaines informations sont probablement utiles pour installer convenablement le routeur. Pour les obtenir, ouvrir le **Panneau de configuration**, cliquer deux fois sur **connexion réseau** puis cliquer avec le bouton droit de la souris sur l'icône **connexion au réseau local**. Choisir **Propriété, Protocole Internet (TCP/IP), Propriété**. Si la case **utiliser l'adresse IP suivante** est active, l'accès à Internet utilise une adresse statique. Noter alors l'adresse IP, **le masque de sous réseau** et **la passerelle par défaut**. Cliquer ensuite sur, **Obtenir une adresse IP automatiquement**,. Cliquer sur **OK** pour appliquer les modifications, puis de nouveau sur **OK** pour fermer la boite de dialogue.

Si on bénéficie d'une connexion **ADSL**, on aura probablement besoin du nom d'utilisateur et du mot de passe nécessaire à la connexion du prestataire de service. Si on ne connaît pas ces informations, on les recherche dans le logiciel ou dans les documents fournis lors de votre abonnement. Veiller collecter les adresses **MAC** des adaptateurs de réseau sans fil qu'on va installer. Elles sont normalement imprimées sur chaque carte **PC WI-FI** ou **adaptateur PCI**.

Remarque : On trouvera peut être des instructions spécifiques de configuration du routeur dans le support technique du site du prestataire de service ou du fabricant du routeur, notamment si on utilise **ADSL**.

IV.7.5.2 Installation du routeur sans fil

Avant d'installer le routeur, éteindre le PC et le modem ; déconnecter le câble Ethernet du PC et relier au port WAN du routeur de telle sorte que ce câble unisse modem et routeur. A l'aide d'un second câble Ethernet, raccorder ensuite le port Ethernet de votre PC à l'un des ports Ethernet du routeur.

Mettre le modem sous tension et attendre qu'il se connecte. Mettre alors le routeur ainsi que le PC sous tension. Apres démarrage du système, activer le navigateur et parcourir quelques sites web afin de tester la connexion Internet.

IV.7.5.3 Installation d'une carte réseau sans fil.

Installer une carte réseau sans fil dans chacun des ordinateurs de bureau qu'on souhaite connecter au réseau sans fil. Si on utilise un adaptateur **D-Link** sur un PC, installer d'abord le logiciel correspondant, à partir du CD fourni, avant de mettre la carte en place. Arrêter ensuite l'ordinateur, installer l'adaptateur et relancer le système. Apres initialisation de Windows, **l'assistant Ajout de matériel** devrait s'afficher et initialiser automatiquement l'installation du pilote. Si un message vous avertit que le pilote ne dispose pas de la **certification Windows Logo**, on l'ignore et on clique sur **Continuer**.

Remarque : si l'ordinateur portable inclut une connexion Wi-Fi intégré, on n'a pas besoin de carte PC additionnelle.

A ce stade, l'installation physique est terminée. La suite de procédure consiste à sécuriser le réseau sans fil que le routeur va administrer et à autoriser la connexion sans fil des ordinateurs.

CHAPITRE V : INTERCONNEXION DES RESEAUX

V.1 Interconnexion des Réseaux locaux

V.1. 1 Introduction

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires. Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

V.1.2 Equipements d'interconnexion

- Les répéteurs
- Les concentrateurs (hub)
- Les ponts (bridges)
- Les commutateurs (switch)
- Les passerelles (gateway)
- Les routeurs
- Les B-routeurs

V.1.2.1 Répéteurs

Le répéteur est un dispositif permettant d'étendre la distance de câblage d'un réseau local. Son rôle consiste à amplifier et à répéter les signaux qui lui parviennent. Il existe également des répéteurs qui régénèrent les signaux. Ceci réduit le bruit et la distorsion. Le répéteur intervient au niveau 1 du modèle OSI. Sur une ligne de transmission, le signal subit des distorsions et un affaiblissement d'autant plus importants que la distance qui sépare deux éléments actifs est longue. Généralement, deux nœuds d'un réseau local ne peuvent pas être distants de plus de quelques centaines de mètres, c'est la raison pour laquelle un équipement supplémentaire est nécessaire au-delà de cette distance.

III.3 Différents systèmes de connexion de réseaux cameras

III.3.1 Système sur réseau IP

1° connexion avec un réseau local (LAN)

Les caméras prennent des images en cas d'intrusion et les envoient par le réseau sur n'importe quel PC du réseau et visualisées en temps réel .

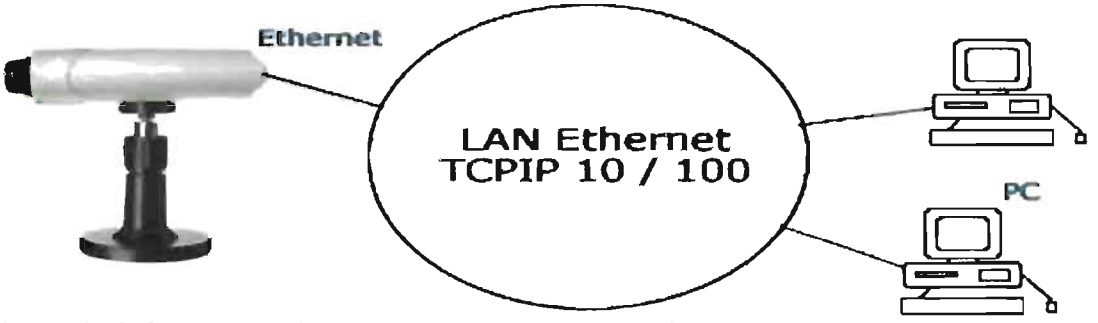


Figure III.3 Connexion d'une camera avec un réseau local

2° Connexion directe avec la carte réseau du PC

La caméra prend des images en cas d'intrusion et les envoient par le réseau sur le serveur FTP installé sur votre PC. On peut se connecter en direct sur la camera et regarder en temps réel ce qui se passe.

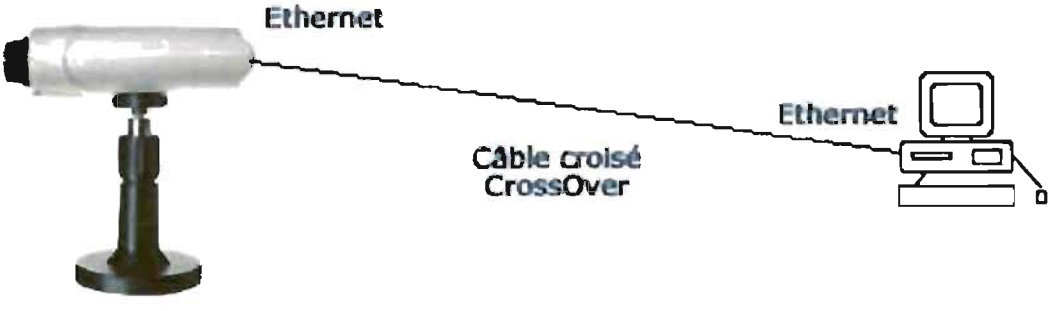


Figure III.4 Connexion directe avec la carte réseau

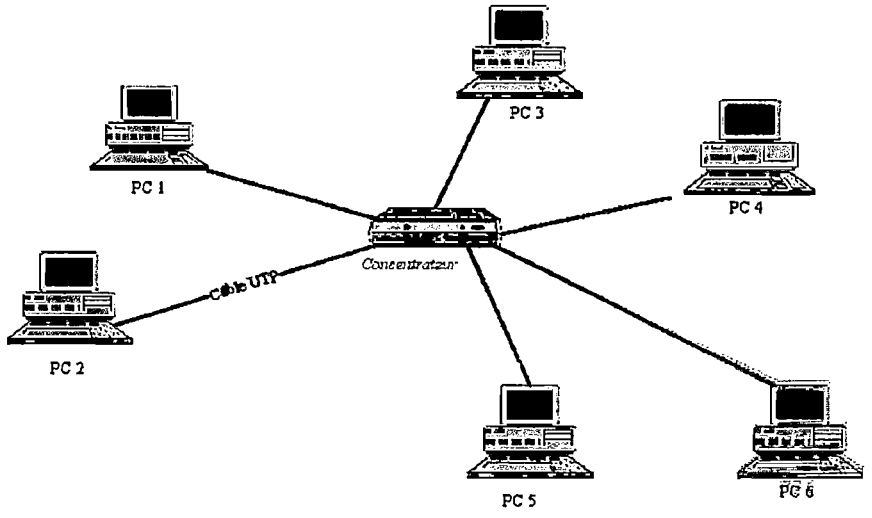


Figure V.3 Concentrateur comme HUB

Il est possible de connecter plusieurs **hub** entre eux afin de concentrer un plus grand nombre de machines, on parle alors de connexion en cascade (parfois appelé ***daisy chains*** en anglais). Pour ce faire, il suffit de connecter les hub à l'aide d'un câble croisé, c'est-à-dire un câble reliant les connecteurs de réception d'une extrémité aux connecteurs de réception de l'autre. Il est possible de chaîner jusqu'à trois concentrateurs. Les concentrateurs sont en général dotés d'un port spécial appelé "**uplink**" permettant d'utiliser un câble droit pour connecter deux **hub** entre eux. Il existe également des **hub** capables de croiser ou de décroiser automatiquement leurs ports selon qu'il est relié à un hôte ou à un **hub**. Le nombre de réseaux importe peu, il convient malgré tout de respecter certaines règles dont les principales sont que chaque câble (d'un concentrateur à un autre concentrateur, ou d'un concentrateur à un PC) ne peut pas dépasser 100m et qu'un PC, pour communiquer avec un autre, ne peut pas rencontrer plus de quatre concentrateurs.

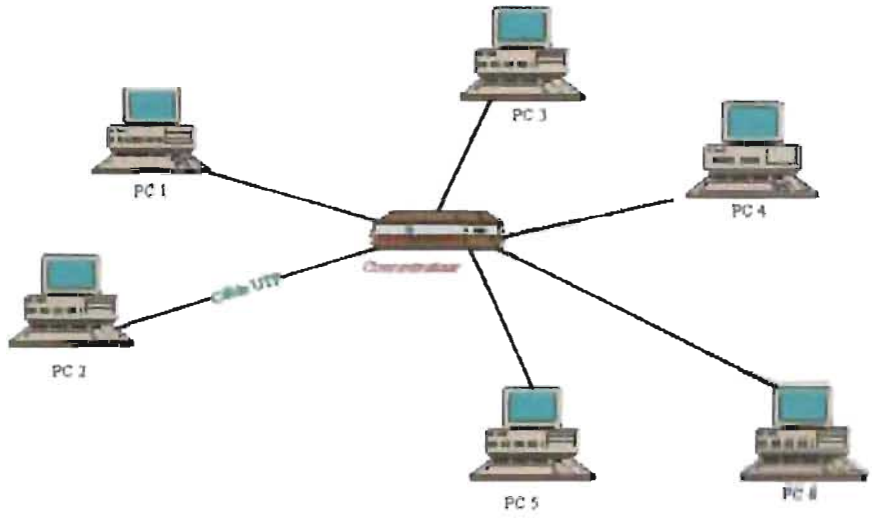


Figure V.3 Concentrateur comme HUB

Il est possible de connecter plusieurs **hub** entre eux afin de concentrer un plus grand nombre de machines, on parle alors de connexion en cascade (parfois appelé ***daisy chains*** en anglais). Pour ce faire, il suffit de connecter les hub à l'aide d'un câble croisé, c'est-à-dire un câble reliant les connecteurs de réception d'une extrémité aux connecteurs de réception de l'autre. Il est possible de chaîner jusqu'à trois concentrateurs. Les concentrateurs sont en général dotés d'un port spécial appelé "**uplink**" permettant d'utiliser un câble droit pour connecter deux **hub** entre eux. Il existe également des **hub** capables de croiser ou de décroiser automatiquement leurs ports selon qu'il est relié à un hôte ou à un **hub**. Le nombre de réseaux importe peu, il convient malgré tout de respecter certaines règles dont les principales sont que chaque câble (d'un concentrateur à un autre concentrateur, ou d'un concentrateur à un PC) ne peut pas dépasser 100m et qu'un PC, pour communiquer avec un autre, ne peut pas rencontrer plus de quatre concentrateurs.

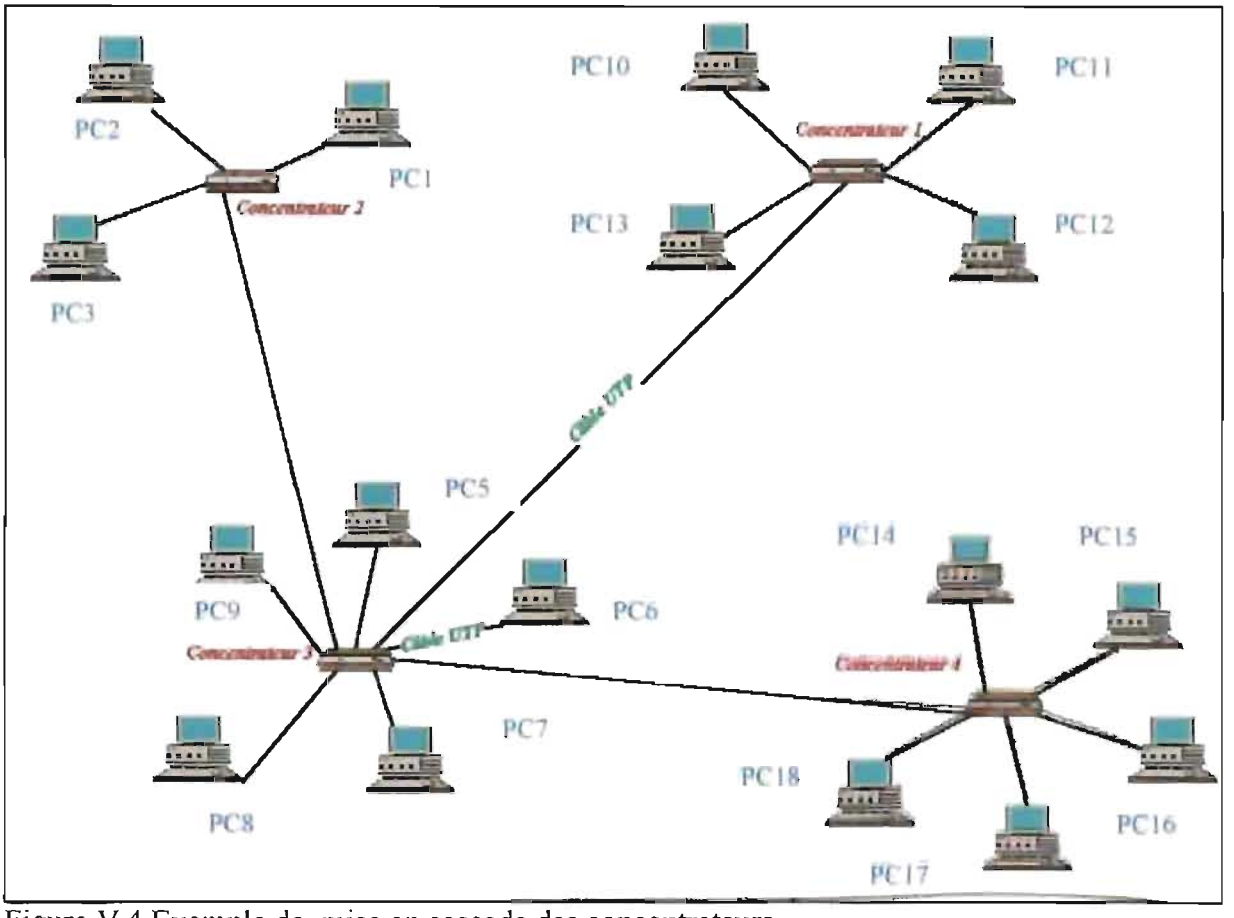


Figure V.4 Exemple de mise en cascade des concentrateurs

V.1.2.3 Ponts

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin.

En contrepartie, l'opération de filtrage réalisée par le pont peut conduire à un léger ralentissement lors du passage d'un réseau à l'autre, c'est la raison pour laquelle les ponts doivent être judicieusement placés dans un réseau.

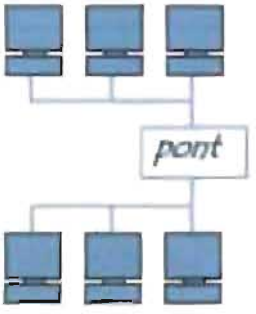


Figure V.5 Concentrateur comme pont

V.1.2.4 Commutateurs.

Un commutateur (en anglais switch) est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de commutation ou de réseaux commutés). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

Connaissant le port du destinataire, le commutateur ne transmettra le message que sur le port adéquat, les autres ports restants dès lors libres pour d'autres transmissions pouvant se produire simultanément. Il en résulte que chaque échange peut s'effectuer à débit nominal (plus de partage de la bande passante), sans collisions, avec pour conséquence une augmentation très sensible de la bande passante du réseau (à vitesse nominale égale). Le câblage reste le même que le hub, et il est aussi possible de relier plusieurs commutateurs afin de relier plusieurs réseaux locaux.

V.1.2.5 Passerelles

Une passerelle applicative (en anglais «**gateway** ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents. La passerelle est généralement un ordinateur complet avec plusieurs cartes réseau. Les passerelles recouvrent les sept couches du modèle OSI. Elles sont nécessaires pour passer d'un type de réseau à un autre, les deux étant complètement différents sur les 7 couches OSI.

Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.

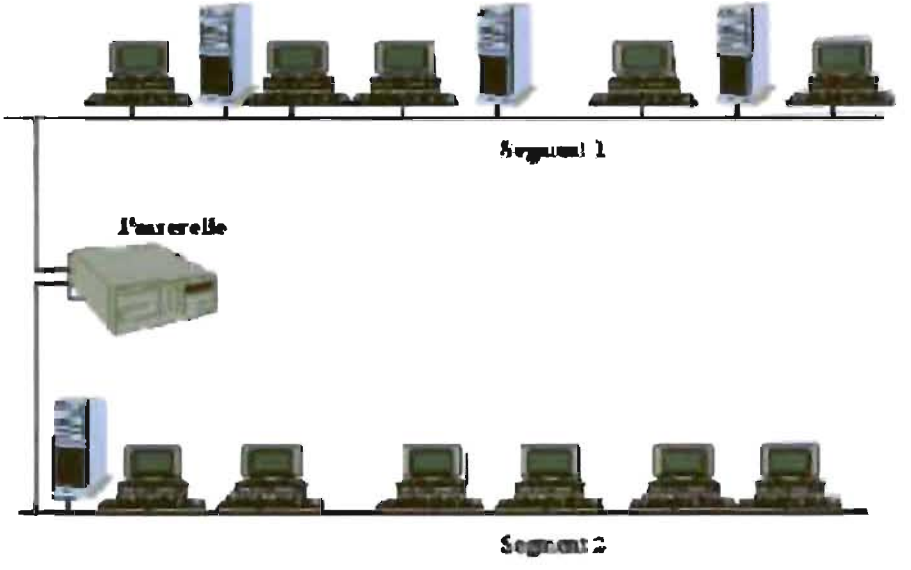


Figure V.6 Liaison de deux réseaux par une passerelle

V.1.2.5 Routeurs

Contrairement aux ponts ou aux commutateurs, les routeurs travaillent sur la couche 3 du modèle OSI, ils sont donc capable de déchiffrer complètement les deux couches les plus basses, et donc de connecter deux réseaux de type très différent comme Ethernet ou Token Ring. Pour cela il est très souvent utilisé pour connecter un **LAN** à un **WAN** (réseau étendu comme **X25** ou **RNIS**). En fait un routeur n'est vraiment nécessaire que lors des communications entre stations de réseaux différents.

V.1.2.5 Routeurs

Contrairement aux ponts ou aux commutateurs, les routeurs travaillent sur la couche 3 du modèle OSI, ils sont donc capable de déchiffrer complètement les deux couches les plus basses, et donc de connecter deux réseaux de type très différent comme Ethernet ou Token Ring. Pour cela il est très souvent utilisé pour connecter un **LAN** à un **WAN** (réseau étendu comme **X25** ou **RNIS**). En fait un routeur n'est vraiment nécessaire que lors des communications entre stations de réseaux différents.

Le routeur doit donc être capable de traduire des trames d'un certain type de réseau pour un autre type de réseau, il doit donc transformer complètement les paquets qui transitent sans bien sûr toucher fondamentalement au contenu des données. Outre cette fonction de traduction, le fait de travailler au niveau de la couche réseau, lui permet de connaître l'adresse IP de l'expéditeur et du destinataire. Comme le pont il est capable au moyen d'une table interne qui s'enrichit continuellement de déterminer sur quel brin de réseau se trouve un poste particulier (sauf qu'à la différence du pont, le routeur travaille sur les adresses IP) cette table est appelé table de routage. Les routeurs ne sont pas utilisés uniquement pour connecter un LAN et un WAN, de par la richesse des possibilités de configuration, on peut s'en servir au sein d'un réseau local pour des raisons de sécurité pour limiter la communication vers certains segments ou nœuds du réseau. Physiquement les routeurs sont des ordinateurs à part entière, avec CPU, mémoire, système d'exploitation, interface, etc. Les routeurs sont également disponibles comme cartes enfichables ou comme boîtiers rackables. Il existe aussi des routeurs complètements logicielles, une station avec plusieurs cartes réseaux peut jouer le rôle de routeur.

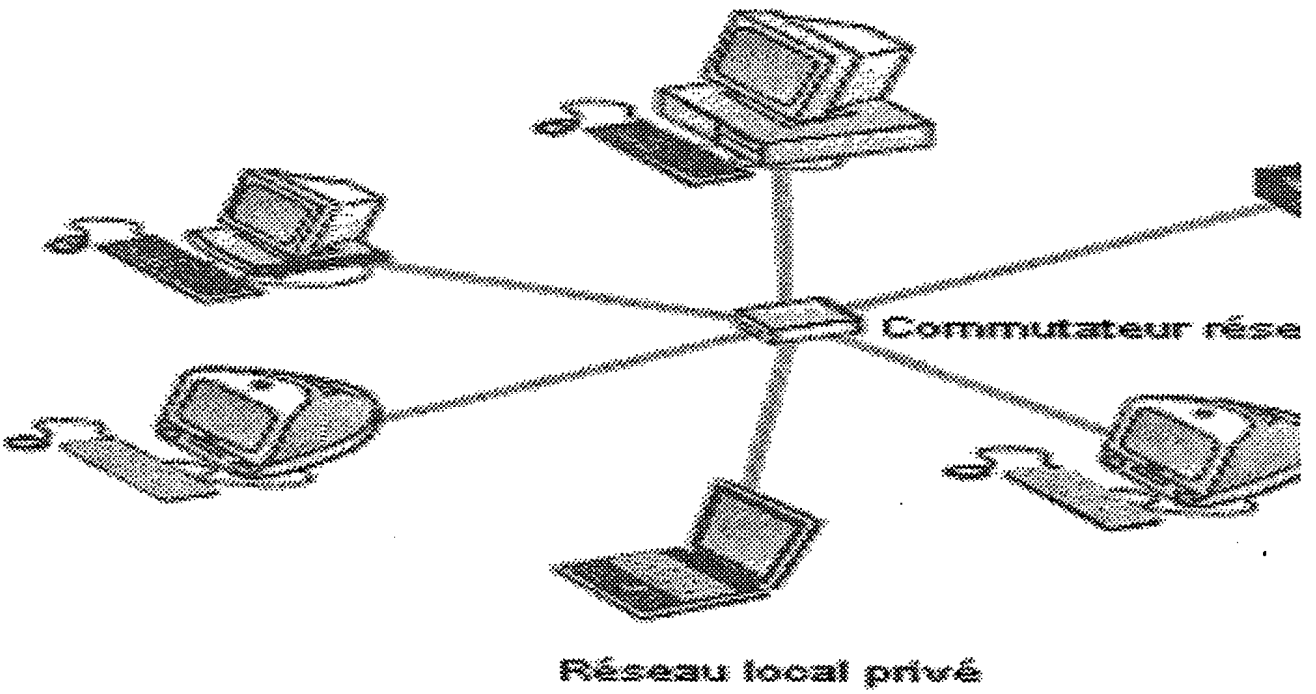


Figure V.7 routeur comme équipement d'interconnexion

N.B : Il faut enfin noter qu'il existe un autre équipement appelé B-Routeur ; qui est un élément hybride associant les fonctionnalités d'un routeur et celles d'un pont. Ainsi, ce type de matériel permet de transférer d'un réseau à un autre les protocoles non routables et de router les autres. Plus exactement, le B-routeur agit en priorité comme un pont et route les paquets si cela n'est pas possible.
Un B-routeur peut donc dans certaines architectures être plus économique et plus compact qu'un routeur et un pont.

V.2 Interconnexion des réseaux distants

Pour les réseaux filaires, seul la fibre optique est utilisée pour l'interconnexion des réseaux à grande distance. La solution sans fil (Wireless) est requise pour interconnecter les réseaux informatiques distants lorsqu'il n'existe pas de possibilité de creuser les tranchées pour câble. Ainsi, on se sert du faisceau Hertzien qui permet une connexion à haut débit entre deux ou plusieurs réseaux d'entreprises par l'intermédiaire des antennes appropriés. Enfin une autre méthode consiste à utiliser l'Internet comme support de transmission d'interconnexion des réseaux en utilisant un support d'encapsulation (en anglais **tunneling**).

Ce type de réseaux est appelé réseaux Privé Virtuel (noté **RPV** ou **VPN**). Il est dit virtuel car il relie deux réseaux physiques (réseaux locaux) par une liaison non filaire (Internet) et privé car seuls les ordinateurs des réseaux locaux de part d'autre du VPN peuvent voir les données.

V.2.1 Internet

L'Internet est un réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs. L'ambition d'Internet s'exprime en une phrase : relier entre eux tous les ordinateurs du monde. A l'image du téléphone qui permet de converser avec toute personne dont on connaît le numéro, Internet est un système mondial d'échange de documents électroniques : textes, fichiers, images, sons et séquences audiovisuelles. C'est l'alliance de l'informatique et des télécommunications : la télématique au véritable sens du terme. Les utilisateurs d'Internet sont désignés par le terme d'internautes, synonyme de cybernaute, de surfer ou de net surfer. Quant aux informations du réseau, elles sont accessibles à partir de "lieux" que l'on appelle les sites Internet. Internet ayant été popularisé par l'apparition du **World Wide Web**, les deux sont parfois confondus par le public non averti. Le Web est une des applications d'Internet, comme le sont le courrier électronique, la messagerie instantanée et les systèmes de partage des fichiers poste à poste. L'accès à Internet peut être réalisé auprès d'un fournisseur d'accès via divers moyens de télécommunication : soit filaire (réseau téléphonique à bas débit, ADSL ou XDSL, câble coaxial, fibre optique, courant électrique porteur CPL), soit sans fil (Wi-Fi, Wimax, Internet par satellite...).

V.2.2 Réseau VPN

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison suscite des discussions (Internet), comme s'ils étaient sur le même réseau local.
Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombre d'applications possibles :

- Accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades
- Accès au réseau caméra IP (d'entreprise) à distance
- Partage de fichiers sécurisés
- Jeu en réseau local avec des machines distantes
- Etc.

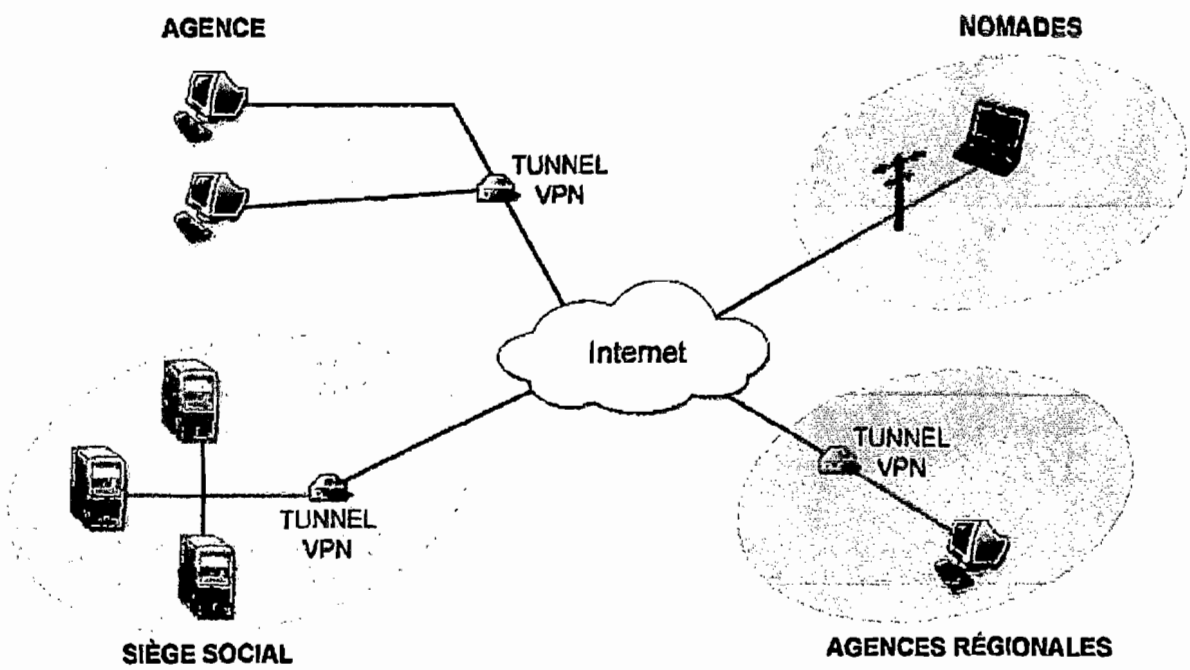


Figure V.8 Exemple d'un réseau VPN

III^{ème} PARTIE : ETUDE DE LA SURVEILLANCE PAR CAMERAS INTERCONNECTEES A BASE D'UN RESEAU INFORMATIQUE «CAS DE LA SOCIETE GASPAS COMPANY »

CHAPITRE VI : PRESENTATION GENERALEDE LA SOCIETE GASPAS COMPANY

VI.1 Historique

Le Burundi n'a pas une culture de regarder, d'interpréter ou de transmettre des messages visuels plus précisément des messages qu'on trouve sur des affiches ou panneaux publicitaires. La société **GASPAS COMPANY** est venue dans le but de faire partager la joie de regarder, apprécier ou encore de transmettre des messages à travers des supports visuels tels que : affiches, pancartes, panneaux publicitaires etc. **GASPAS COMPANY** est le résultat d'une grande expertise dont fait preuve son fondateur ingénieur en communication visuelle spécialisé en **Design** appliquée à l'informatique.

Un fondateur dont le rêve est devenu réalité en 1997, faisant de **GASPAS COMPANY** la première entreprise en informatique graphique au Burundi.
GASPAS COMPANY rempli d'un amour professionnel a avec ses jeunes apprentis encore adolescents à l'époque, innové le system des cybers au Burundi et du graphique **Design**. GASPAS COMPANY fut aussi la première entreprise burundaise à initier la création des sites web, a même dispensé des formations dans ce sens. Elle installa aussi le Studio IJAMBO et la Radio ISANGANIRO à base d'équipements numériques. Avec ses connaissances approfondies dans les domaines de la communication et informatique, GASPAS COMPANY ouvra d'autres horizons extraordinaires d'impressions. Impressions de diverses formes : sur des gobelets, assiette et sur d'autres matières variées, impressions indoor outdoor très grand format, grand format et moyen format.

VI.2 Organisation générale

La société **GASPAS COMPANY** a une structure bien organisée ce qui se manifeste par la décentralisation des services comme le montre l'organigramme suivant :

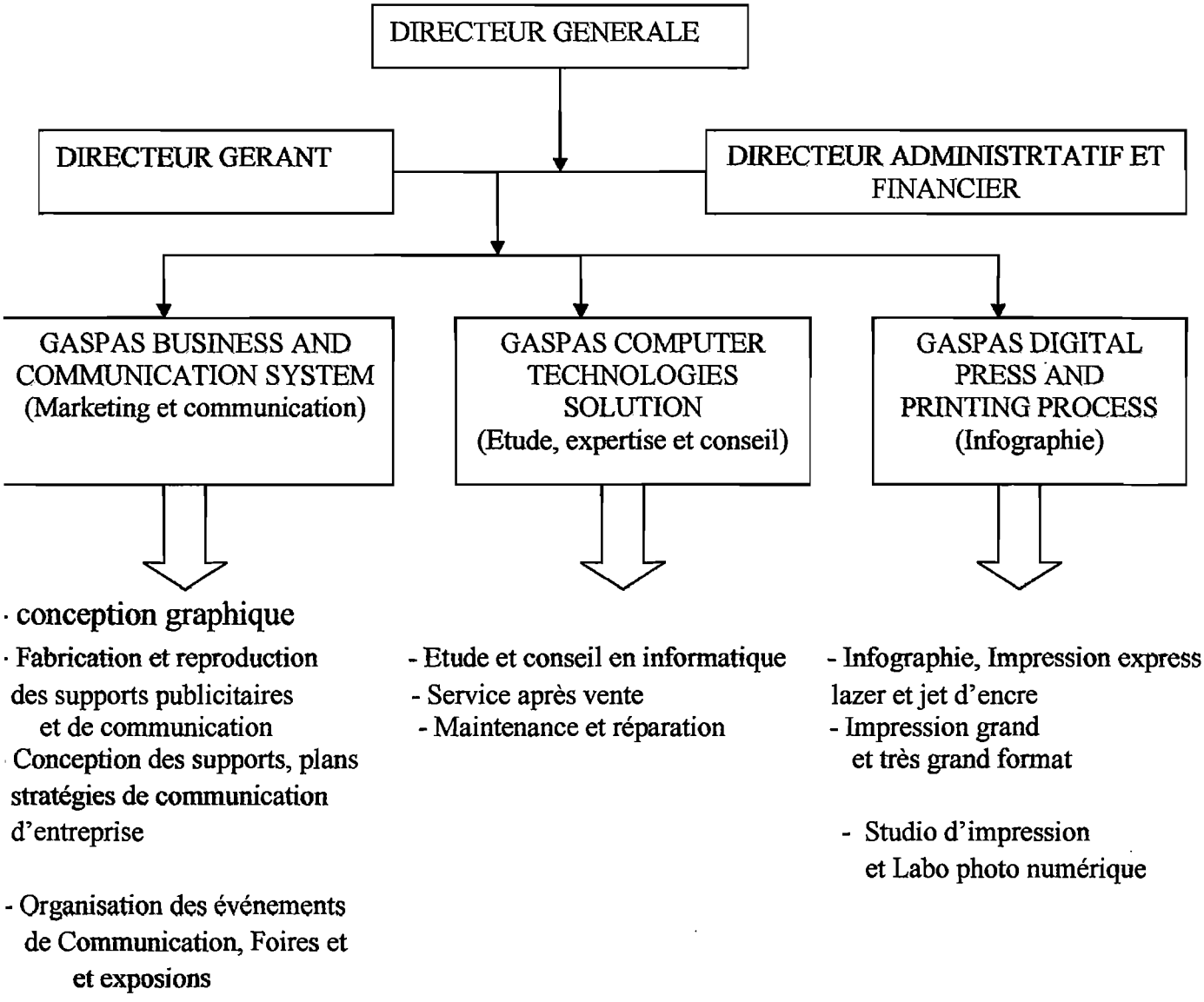


Figure VI.1 Structure de la société GASPAS COMPANY

En ce qui concerne l'équipement informatique, la société GASPAS COMPANY utilise des micro-ordinateurs de types Compac et Dell. Le serveur est aussi du type Compac de grande capacité fonctionnel sous Windows Server 2003 ; permettant la gestion des bases de données.

Les caractéristiques de ce serveur sont les suivantes :

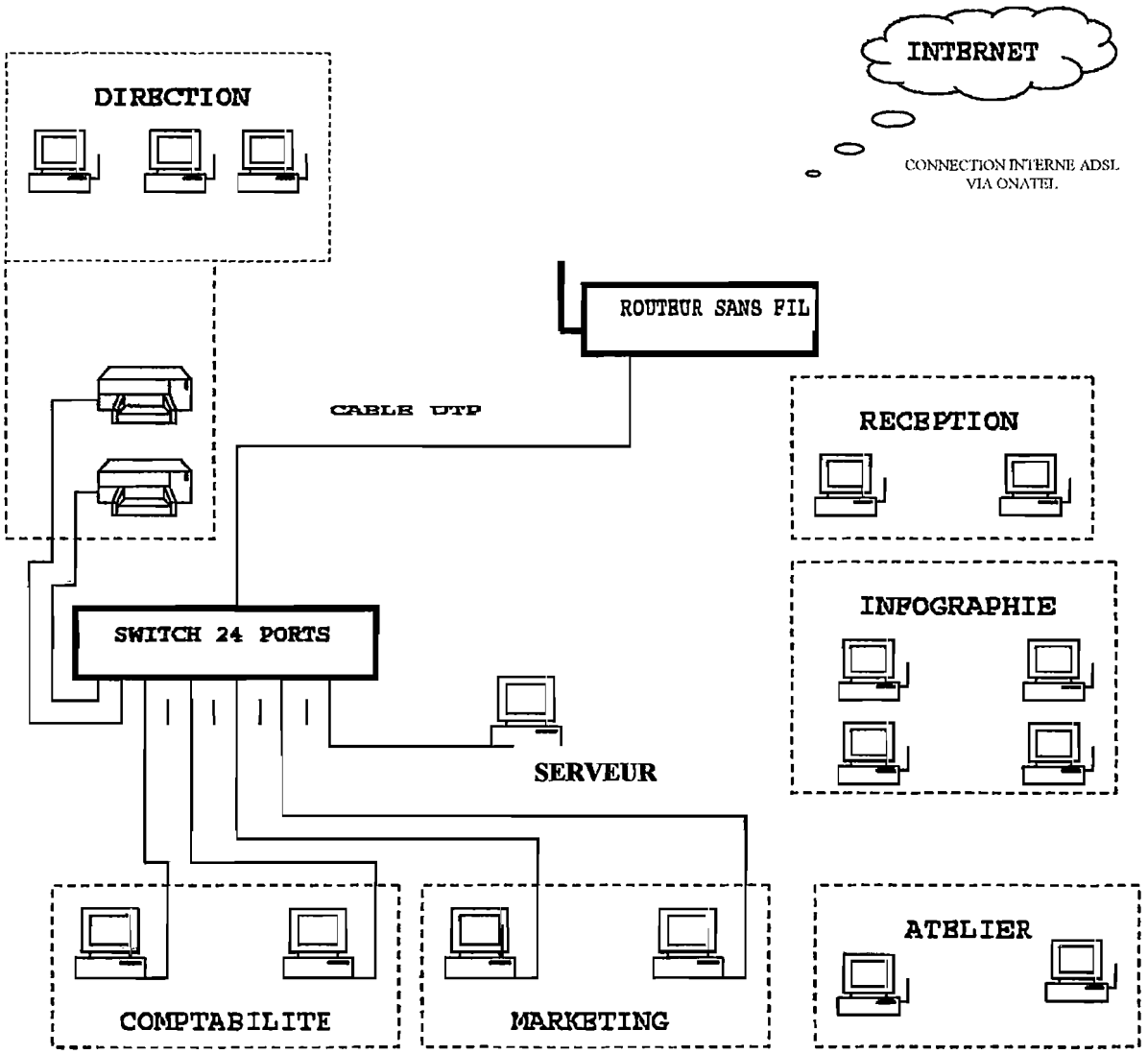
- mémoire vive suffisante : 2 Go
- contrôleur de disques de très bonne qualité basé sur la technologie SCSI
- disques dur de grande capacité (3 disques durs, chacun de 80 Go ce qui fait 240 Go)
- bus d'extension IDE

Comme périphérique d'impression, on trouve

- des imprimantes petit format allant jusqu'au format A3. Ces dernières sont :
  * Une imprimante HP Laser 4700 (format A4, recto verso)
  * Une imprimante Konica Minolta 7400 (33cm* 120cm)
- des imprimantes ploters grand format (largeur maximale de 3,20m) ; elles sont utilisées pour les impressions des affiches publicitaires, banderoles, et décor intérieur et extérieur d'architectures.

VI.4 Réseau informatique existant

Le réseau informatique installé dans la société GASPAS COMPANY est un réseau fast Ethernet (version Ethernet au débit de 100 Mbps).



LEGENDE

: PC avec carte réseau sans fil

: PC avec carte réseau de port RJ 45

: Imprimante réseau

| | | : Signalisation de l'existence d'autres PC et imprimantes non montrés sur le schéma

Figure VI.2 Réseau informatique de GASPAS COMPANY

C'est une topologie étoile. Il a trois principales fonctions :

- une fonction bureautique classique : partage d'imprimante et échange de fichiers
- une fonction de base des données de gestion (utilisation en mode multi utilisateurs de la base des données de gestion : comptabilité, gestion commercial, immobilisation et paie)
- une fonction de partage de connexion Internet

Les équipements d'interconnexion qu'utilise ce réseau sont le Switch et le routeur.

Suivant le mode d'interconnexion, on distingue deux réseaux :

- réseau filaire assuré par le Switch
- réseau non filaire (réseau sans fil) assuré par le routeur (Access point)
- cartes réseaux

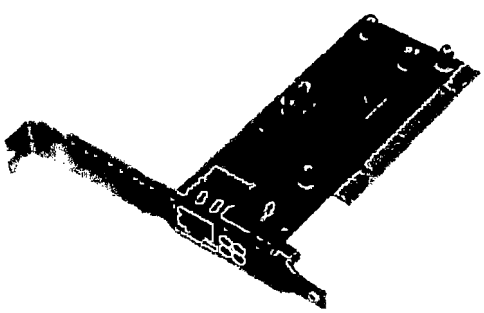


Figure VI.3 Carte réseau avec port RJ 45

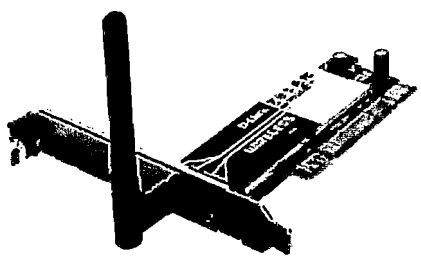


Figure VI.4 Carte réseau sans fil

Le réseau filaire est fait par les câbles de paires torsadés catégorie 5 avec des connecteurs RJ 45 ainsi que des prises RJ 45

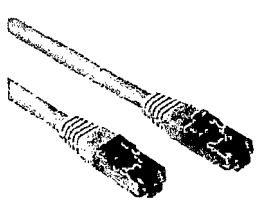


Figure VI.5 Câble RJ45

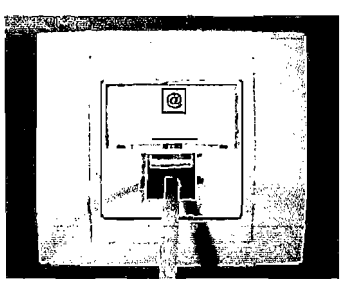


Figure VI.6 Prise murale

Le réseau non filaire ou réseau sans fil est assuré par le routeur.

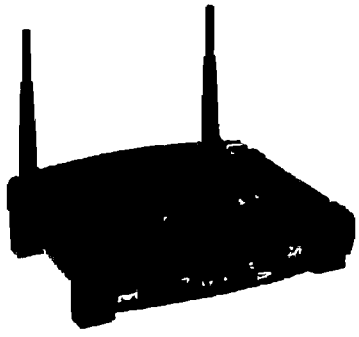


Figure VI.7 Routeur sans fil (Access point)

Ce routeur a trois principaux rôles :

- rôle du modem (assure interconnexion entre le réseau local et le réseau externe pour le fournisseur d'accès Internet en ADSL)
- rôle de switch pour le réseau interne ; pour servir de partage de connexion Internet sur le réseau câblé
- rôle d'Acces point pour partager la connexion Internet sur le réseau sans fil

VI.4.1 Serveur

Pour faciliter la fonction de partage de base de données, la société a mis en place un serveur de fichiers en même temps d'application. :

- Serveur de fichiers : s'occupe de la gestion de fichiers
- Serveur d'application : contient les applications de gestion et de comptabilité.

VI.4.2 Système d'exploitation réseau

Le système d'exploitation des réseaux locaux dits également NOS (Network Operating System) a pour fonction des gestions du réseau. Le NOS est donc une interface entre les applications des utilisateurs et les fonctions du réseau local auxquelles il fait appel par des demandes à travers la carte réseau.

Pour le cas de la société GASPAS COMPANY, le système d'exploitation utilisé est Windows server 2003. Celui-ci est développé par Microsoft et est considéré comme l'un des produits serveurs professionnels.

VI.4.3 Internet

La connexion Internet qu'utilise la société **GASPAS COMPANY** est fournie par ONATEL. C'est une connexion ADSL (Asymetric Digital Subscriber Line ou liaison numérique à débit asymétrique)
L'ADSL est une technique de communication qui permet d'utiliser une ligne téléphonique d'abonné (ou RNIS) pour transmettre et recevoir des signaux numériques à des débits élevés, de manière indépendante du service téléphonique proprement dit (contrairement à celle des modems analogiques)

VI.4.4 Aspect de sécurité

VI.4.4.1 Sécurité physique

Pour protéger les ordinateurs contre les surtensions, chaque ordinateur est connecté à un onduleur APC 1000VA. Et pour sécuriser les câbles réseau ; on les a mis dans des glottes.

VI.4.4.2 Sécurité des données

Un antivirus (Norton 2009) de qualité, mono utilisateur avec « option mise à jour » est installé dans chacune de ces machines.

Conclusion

Comme il est bien décrit aux pages précédentes de ce chapitre, la mise en place du réseau informatique (fast Ethernet) dans la société GASPAS COMPANY est plus bénéfique en termes de satisfaction des activités collectives se déroulant dans cette entreprise.

Après l'analyse des avantages qu'offre ce réseau informatique abritant des équipements informatiques partageables (imprimantes, les lecteurs de disque etc.) les défaillances s'observent sur la sécurité du personnel et du matériel en particulier.

Explicitement parlant, la sécurité ainsi évoquée va lutter contre les actes perturbateurs comme le vol, le cambriolage, etc.

Tout se résout par l'adoption de la technique moderne de vidéosurveillance.

Notre apport en l'implantation des caméras IP comme hôtes intégrés et interconnectés au réseau informatique existant va certainement constituer l'une des meilleures solutions pour l'amélioration de la sécurité par vidéosurveillance en temps réel.

CHAPITRE VII : SURVEILLANCE PAR CAMERAS INTERCONNECTEES

VII.1 Pourquoi la vidéosurveillance dans société GASPAS COMPANY

Souvent ignoré, pourtant nécessaire, l'outil de surveillance pour toute entreprise, constitue l'un des facteurs important pour sa bonne marche, il doit être le plus performant possible et ne doit pas, donc présenter des lacunes. Plus particulièrement, le système de vidéosurveillance, pour une entreprise commerciale, doit être à la hauteur des exigences des nouvelles applications informatiques. Les gestionnaires sont donc dans l'obligation d'instaurer ou d'améliorer leur structure de vidéosurveillance pour la rendre plus efficace.
La mise en place de ce système vient à point nommé pour palier aux problèmes de laisser-aller au lieu de travail, de vol et d'autres incidents. Il fallait une installation des cameras de surveillances sur toutes les pièces de l'entreprise dont le contrôle de situation par capture d'image permettait de minimiser l'irresponsabilité et dommages à l'intérieur.
L'implantation de cette vidéosurveillance dans la société GASPAS COMPANY représente un avantage majeur au chef de l'entreprise de pouvoir surveiller le déroulement des activités étant partout au monde entier grâce à l'utilisation des cameras IP pouvant être consultables et contrôlables à partir d'INTERNET.

VII.2 Interconnexion des caméras

VII.2.1 Choix de la caméra

Pour choisir une caméra de vidéosurveillance, on tient compte de nombreux critères selon les besoins. Les options et fonctionnalités étant nombreuses, il est important de distinguer l'utile et l'accessoire. Pour aboutir à un choix non fantaisiste, plusieurs questions peuvent se poser :

*** Caméra autonome ou connectée à un PC ?**

Dans un premier temps, on détermine si on souhaite une **caméra autonome** ou une caméra qui nécessite un PC pour fonctionner.

*** Caméra fixe ou caméra motorisée ?**

Lors du choix, on doit déterminer si l'on souhaite une **caméra fixe ou motorisée**. La caméra fixe permet de visualiser un seul et unique point de vue du lieu qu'on souhaite diffuser. La caméra motorisée permet en revanche de visualiser plusieurs points de vue, le tout selon 3 axes.

*** Utilisation intérieure ou extérieure ?**

L'utilisation à l'intérieur ou à l'extérieur va définir deux critères supplémentaires : la capacité de la caméra à s'adapter à la luminosité d'une part, et d'autre part, sa capacité à résister aux intempéries, à la chaleur et au froid. L'utilisation de caméras à l'intérieur et à l'extérieur endommage leur capteur. Pour le caisson, on choisi au minimum un caisson chauffé. La ventilation est aussi recommandée dans les zones chaudes et/ou humides. Dans le cas d'une caméra mobile, il est nécessaire de prévoir un caisson adapté sur mesure ou un dôme.

*** Visualisation et diffusion ?**

On peut choisir de diffuser les images pour vous seul (cas de la vidéosurveillance). Dans ce cas, on visualise les images avec n'importe quel navigateur Internet. Si on souhaite diffuser les images à d'autres personnes, on les incorpore au sein des pages d'un site Internet. Dans le cas où on a choisi une caméra mobile, il est nécessaire de déterminer si on souhaite que les internautes contrôlent ou non la caméra. Si tel est le cas, on doit faire le choix d'un serveur vidéo adapté à cette utilisation.

*** Quelle est la taille d'un espace que vous voulez voir à chaque caméra?**

La distance et la largeur de la zone qu'on souhaite à la vue, détermine le type d'objectif dont on a besoin. Il est enfin important d'examiner la méthode de compression utilisée par une caméra IP. La compression réduit la taille de la vidéo tout en contrôlant les fichiers générés. Étant donné que les fichiers vidéo contiennent une énorme quantité de données, la compression est nécessaire pour réduire le stockage et la bande passante. Les techniques de compressions les plus couramment utilisées sont MPEG-4 et MJPEG.

Compte tenu de ces facteurs nous avons choisis une caméra de marque **D-Link** modèle **DCS 6110** appelé caméra réseau ou IP à dôme fixe.



Figure VII 1 Camera D-Link DCS 6110

VII.3 Description de la caméra choisie

La caméra réseau à dôme fixe DCS-6110 est une solution de sécurité économique et idéale, qui offre des rendus vidéo de haute qualité en temps réel en modes compression MPEG-4 et JPEG pour les PME, les bureaux individuels et les particuliers. Ce système de surveillance, doté de la prise en charge vidéo, se branche à votre Ethernet de manière à ce que vous bénéficiiez de la surveillance à distance via Internet. En outre, il prend en charge la sortie double flux pour la surveillance en direct simultanée et l'enregistrement en haute résolution. Le modèle DCS-6110 est une caméra réseau de luxe en forme de dôme. Son apparence professionnelle en fait un choix idéal pour la surveillance en entreprise ou à domicile
. Quant au logiciel Webcam Monitor, également fourni avec les caméras, il vous permet de gérer jusqu'à 32 caméras simultanément depuis votre ordinateur, d'envoyer automatiquement des alertes par e-mail et d'enregistrer des vidéos sur votre disque dur lorsqu'un mouvement est détecté.

Spécifications techniques de cette camera

ALGORITHME VIDÉO PRIS EN CHARGE	JPEG pour les images fixes Compression multiformat MPEG4/MJPEG
FONCTIONS VIDÉO	Taille et qualité d'image réglables Horodatage et superposition de texte 3 fenêtres de détection de mouvement configurables Options Retourner l'image et Miroir
LAN	Respect de la norme IEEE 802.3 Respect de la norme IEEE 802.3u Prise en charge du mode bidirectionnel simultané Prise en charge du contrôle de flux IEEE 802.3x en mode bidirectionnel simultané Prise en charge de la norme IEEE 802.3af (PoE)
INTERFACES RÉSEAU INTÉGRÉES	Port Ethernet 10/100BASE-TX
FONCTIONS LOGICIELLES DE SURVEILLANCE	Gestion/contrôle à distance sur un maximum de 32 caméras Affichage de 32 caméras sur un même écran Prise en charge de toutes les fonctions de gestion fournies dans l'interface Web Détection de mouvement programmée ou options d'enregistrements manuels
PUISSANCE D'ENTRÉE	100-240 VCA, 50/60 Hz
CONSOMMATION ÉLECTRIQUE	Max. 3,6 W
DIMENSIONS	l x L x H = 194 x 180 x 107 mm
POIDS	630 g
SÉCURITÉ	Protection de groupes d'administrateurs et d'utilisateurs Authentification par mot de passe

Tableau VII 1 Spécification de la caméra DCS 6110

VII.4 Choix du serveur Vidéo

Un serveur vidéo se présente comme un simple ordinateur mais doté des caractéristiques techniques appropriées pour pouvoir gérer les logiciels de gestion de ces caméras de surveillances et doit avoir un disque dur de capacité assez importante car les images, malgré leurs compressions en MPEG ou MJPEG, occupent énormément d'espace.

*** Ses caractéristiques minimales :**

Microprocesseur : 1.1 Ghz

Mémoire RAM : 256 Mo

Résolution VGA : 800*600

Disque dur : 40 Go

*** Ses caractéristiques requises :**

Microprocesseur : 3.5 Ghz

Mémoire RAM : 1 Go

Résolution VGA : 1024*768

Disque dur : 160Go

VII.5 Nouveau réseau avec caméras de surveillances intégrées

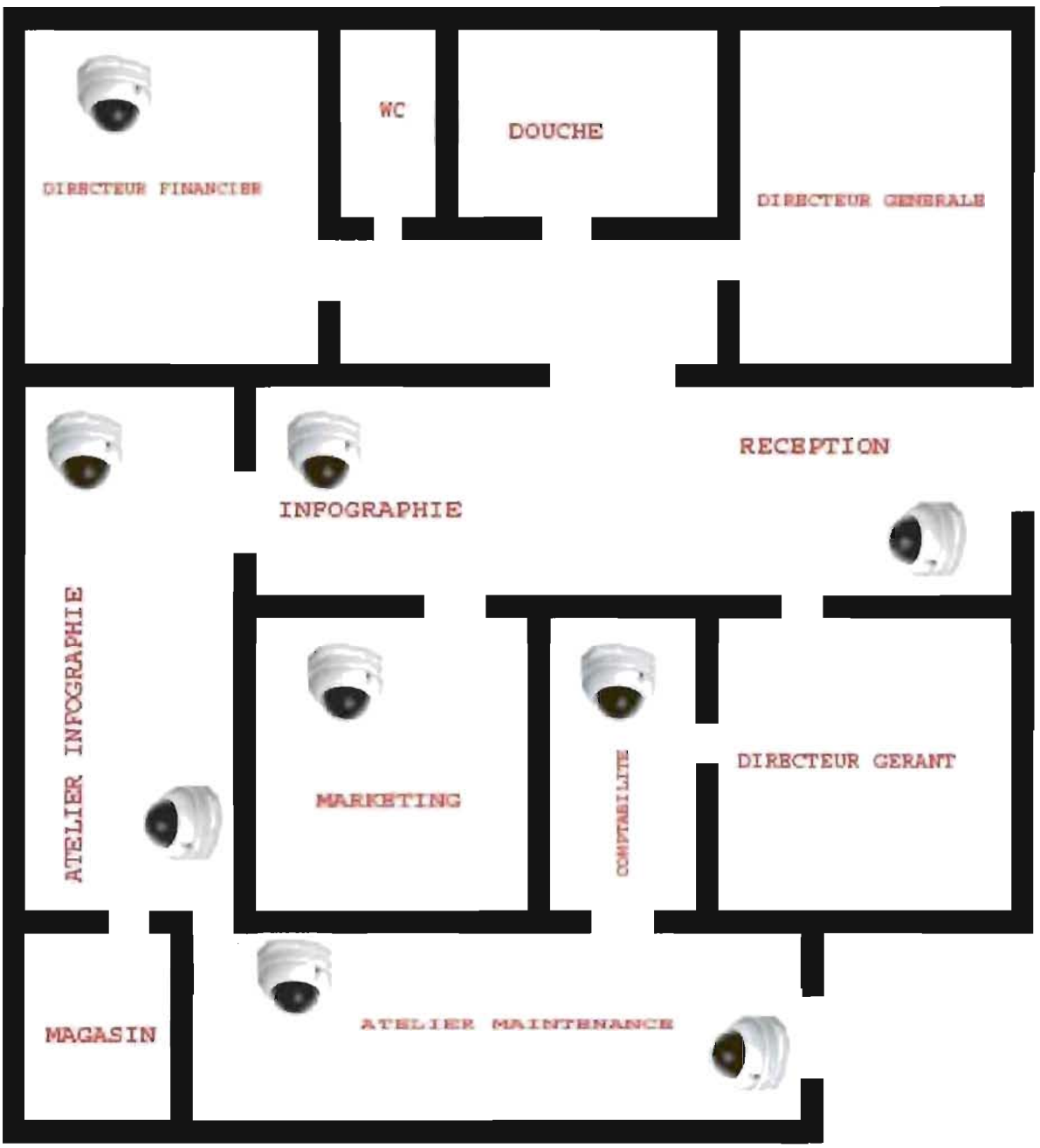


Figure VII 2 Implantation des Caméras

La connaissance des besoins matériels en surveillance et l'identification des points (ou endroit) les plus stratégiques (ou non sécurisé) sont les principales études à mener avant de passer à l'installation proprement dite.

Pour notre cas, compte tenu du plan de l'immeuble de la société, les résultats de l'étude nous ont menés à équiper l'atelier de maintenance et l'atelier d'infographe de deux caméras chacun. Les autres bureaux sont dotés d'une seule caméra chacun à l'exception de ceux du directeur générale et du directeur gérant qui ne sont pas surveillés.

VII.5.1 Câblage

Grâce à son interface réseau intégré, nous avons choisi d'utiliser les câbles UTP catégorie 5 avec des connecteurs Rj 45. Chaque camera du réseau est connecté directement à un switch et agit comme le PC du réseau. Ici ce switch a deux rôles :

- Il remplace la carte DVR et en l'associant avec un ordinateur, ce dernier devient le serveur vidéo.
- Il joue la communication entre le réseau caméra et le réseau informatique.

II.5.2 Fixation

Ces caméras dcs 6110 sont munies d'un module de fixation (ou socle de fixation) se plaçant sur des plafonds ou des murs. Il se présente comme suit :



Figure VII 3 Support de fixation



Figure VII 4 Caméra fixée

Remarque

On peut connecter toutes les caméras sur le même switch auquel les ordinateurs du réseau sont connectés. Mais pour notre cas, le switch qu'on y a trouvé est de 16 port 10/100 Mbps fast Ethernet était saturé, raison pour

Remarque

On peut connecter toutes les caméras sur le même switch auquel les ordinateurs du réseau sont connectés. Mais pour notre cas, le switch qu'on y a trouvé est de 16 port 10/100 Mbps fast Ethernet était saturé, raison pour laquelle les caméras auront leur propre switch et interconnectées par après par un câble UTP au réseau existant

VII.6 Logiciel d'installation

Il existe des multitudes de logiciels de vidéo surveillance qui consistent à gérer de manière centralisé plusieurs caméras IP destinés aux particuliers. Le plus souvent, ils sont distribués avec les caméras lors de son achat. Pour notre cas le logiciel que nous allons utiliser s'appelle WEBCAM MONITOR. Il est conçu :

- pour rendre la configuration des systèmes de surveillance simple et effective, capable de prendre en charge jusqu'à 32 caméras IP, le logiciel WEBCAM MONITOR est compatible avec toutes les caméras IP D-Link actuellement disponibles sur le marché,
- pour offrir des outils de surveillance et d'enregistrement numériques de flux vidéo, audio et d'événements pour différentes applications de sécurité,
- pour fournir aux utilisateurs un grand nombre de fonctionnalités pratiques (notamment l'enregistrement vidéo et la lecture en différée), ce qui en fait une solution de surveillance puissante et facile à utiliser.

VII.7 Configuration du serveur vidéo

Après l'installation physique du matériel, il survient l'installation logique qui consiste à configurer le serveur vidéo qui est le centre de toutes les caméras avant que ces dernières puissent être fonctionnelles. On peut installer ce logiciel en choisissant parmi des dizaines de paramètres, mais l'assistant configuration automatique est plus facile à manipuler. Il démarre dès l'insertion du CD d'installation dans le lecteur. Il ne reste qu'à suivre l'**Assistant de configuration** et à la fin de cliquer sur **terminer.** Pour configurer toutes les caméras on utilise **l'assistant Ajout caméra wizard.** Lors de cette opération le logiciel détecte automatiquement l'adresse IP du caméra. Si cette adresse qui vous a été donné par défaut a été déjà utilisée sur le réseau, le logiciel vous demandera de le changer. Dans ce cas, il faut accepter sinon votre caméra ne sera pas connue. Après l'ajout d'une caméra, il est possible de la supprimer avec l'option **ajout et suppression de la caméra**. La deuxième étape consiste à choisir les scénarios (les scénarios sont des prédéfinis des groupes de paramètres).

En en choisissant une, on configure le programme pour une situation particulière en une seule étape. Les cinq scénarios WebCam Monitor sont :

1° **Lors de l'enregistrement de mouvement où le bruit survient**

Ce scénario est destiné à un type d'alarme de type situation, dans lequel le programme rassemble des éléments de preuve (et éventuellement des alertes et vous tire la sonnette d'alarme), si des intrus sont détectés.

2° **Enregistrement continu des photos JPEG sur mon serveur FTP**

Ce scénario est utilisé lorsqu'on a besoin d'un enregistrement des événements. Le programme prend encore des vidéos et les sauvegardent régulièrement sur un serveur. Il est aussi un bon moyen de transférer des images en continu sur votre site web.

3° **Voir mes caméras à distance depuis un autre PC**

Ce scénario permet à d'autres PC du réseau LAN d'avoir accès aux caméras. Ou si vous utilisez un routeur ou un firewall pour connecter votre réseau à Internet, et vous voulez que les caméras soient accessibles à des ordinateurs en dehors de votre réseau LAN.

4° **E-mail moi quand un mouvement ou un bruit est détecté**

Ce scénario est le même que pour " **Lors de l'enregistrement sonore**, Sauf qu'au lieu de tourner en vidéo / audio d'enregistrement, il envoie automatiquement les e-mails.

4° **Calendrier vidéo de démarrer le contrôle à un moment**

Avec ce scénario, vous pouvez choisir à quel moment vous voulez que ceci ou cela se produise. En général, vous pouvez sélectionner plusieurs scénarios. La seule exception est que les «boutons - pression continuent de télécharger» ne peuvent pas être combiné avec d'autres scénarios. Toutefois, vous pouvez certainement combiner, par exemple, «lors de l'enregistrement de mouvement ou le bruit se produit" par "Voir mes caméras à distance depuis un autre PC» . Vous pouvez même combiner les deux avec "E-mail moi quand un mouvement ou un bruit est détecté." Et vous pouvez certainement utiliser ce scénario avec l'un des quatre autres, ou toute combinaison.

Pour notre cas, le scénario qui nous intéresse et voire même les besoins de la société GASPAS COMPANY,est le troisième « **Voir mes cameras à distance depuis un autre PC** »

VII.7.1 Configuration via un réseau local

Les caméras réseaux se comportent comme les PC en réseau informatique. Lors de la configuration du serveur, dans l'option sécurité, il faut cocher la case « **autoriser l'accès à ce caméra** » par tout les PC du réseau ou en sélectionnant les PC que vous voulez. Chaque PC est identifié dans le serveur vidéo par son IP .Sur le PC client, après avoir installé Webcam Monitor, on ajoute les caméras auxquelles on a le droit d'accéder et ceci à l'aide de **l'assistant ajout wizard** comme pour le serveur.

VII.7.2 Configuration via Internet

Une utilisation commune de Webcam Monitor est de voir ce qui se passe chez vous, ou votre entreprise, quand vous êtes absent. Toutefois, comme la sécurité du réseau devient plus faible, il faut modifier vos paramètres de réseau pour permettre que la vidéo soit visible de l'extérieur de votre réseau local.

Le type le plus commun du réseau informatique utilise aujourd'hui le protocole Internet, presque toujours en abrégé "IP". Il existe deux types d'adresses IP privés et publics. Les numéros qui commencent par 192.168.x .x sont appelés privé ou non routable et ils ne sont utilisés que sur le réseau local. Adresses IP publiques sont attribuées par votre FAI.

Afin de voir un WebCam Monitor diffusion vidéo de l'extérieur de votre réseau, vous avez besoin de configurer le routeur pour permettre certaines requêtes provenant sur le réseau Internet et d'y répondre.
Pour la plupart des routeurs, il y a deux façons de permettre la sortie vidéo de votre réseau: mettre l'ordinateur dans la **zone démilitarisée** et l'utilisation de **Port Forwarding**. Dans le vocabulaire spécifique du réseau des pare-feu, la zone démilitarisée est une zone qui n'a pas de sécurité. Toutes les tentatives de connexion sont autorisées. Si vous mettez votre ordinateur dans la zone démilitarisée, les émissions seront visibles de l'extérieur, mais votre réseau sera sans sécurité. Par conséquent, il est recommandé d'utiliser la redirection de port.
Un aspect de la mise en réseau IP est l'utilisation de différents "ports" pour différents types de service réseau.

Un Port Forwarding vous donnera les instructions de votre routeur et les informations nécessaires dont vous aurez besoin pour ouvrir l'utilitaire de configuration de votre routeur. Bien entendu, les différentes sociétés utilisent des systèmes différents, mais l'une commune est d'ouvrir un navigateur et taper l'adresse souvent 192.168.1.1 dans la barre d'adresse. Vous pouvez trouver la manière de faire cela depuis le manuel de votre routeur ou au site web du fabricant. Maintenant, vous aurez besoin de localiser le Port Forwarding de configuration de votre routeur. Et cela dépend du marque et du modèle du routeur
Ainsi le port par défaut donné par Webcam monitor est 1040 mais on peut ne pas l'utiliser et utiliser un port plus élevé que celui-ci. Pour notre cas la configuration est facile car la connexion Internet qu'utilise la société GASPAS COMPANY est public c'est à dire son routeur laisse certaines requêtes sur des réseaux internet. La seule chose qui reste est de configurer ce port dans le routeur.
Il faut enfin signaler que Webcam monitor vous demande le nombre total des utilisateurs qui peuvent se connecter en même temps.
Pour vous connecter de l'extérieur, il suffit de taper mms: / / au début, et: à la fin : 1040 (en remplaçant votre adresse IP et le port que vous avez choisi). Notre adresse IP est indiquée comme 212.21.63.24. Pour notre cas, il suffit de taper dans le navigateur Web ceci : mms: / /212.21.63.24:1040. D'ici on est déjà dans le serveur vidéo, par la suite on travaille comme si on est dans le réseau sécurisé. Les informations nécessaires qu'on doit disposer pour se connecter au serveur vidéo sont le nom d'utilisateur et le mot de passe fourni par l'administrateur du serveur. Nous avons préféré utiliser ces informations qui sont données par défaut par le concepteur du logiciel Webcam Monitor et elles pourront être modifiées par le nouveau administrateur.

Nom d'utilisateur : admin
Mot de passe : admin
Numéro de port choisi : 1040

NB : mms est un protocole internet généralement utilisé pour les fichiers multimédias.

VII.8 Devis estimatif du coût du projet

Pour bien mener notre projet, il a fallu compléter l'étude technique par une évaluation du coût. Nous avons déterminé les ressources matérielles et humaines à disponibiliser pour le réaliser. Ce qui, compte tenu des moyens dont dispose l'entreprise et de l'utilité de ce projet, détermine sa faisabilité.

Le coût global de ce projet tiendra compte du matériel à commander et de la main d'œuvre pour l'exécution

VII.8.1 Matériel à commander

Matériel	Quantité	Prix Unitaire en FBU	Prix total
Cameras IP D-Link DCS 6110	9	700000	6300000
Switch 16 ports	1	120000	120000
Câble UTP Catégorie 5	100m	700	70000
Connecteurs RJ 45	20	1000	20000
Goulottes	20m	1500	30000
Serveur Vidéo	1	2200000	2200000
Total			8 740 000

Tableau VII 2 Dévis

VII.8.2 Les resources humaines

Les ressources humaines nécessaires pour l'exécution de ce projet se classent en deux catégories:

- une main d'œuvre pour l'installation des câbles dans les différentes pièces de l'entreprise. Le coût de l'installation est déterminé forfaitairement à raison de **10 000 FBU** par pièce ce qui donne au total **90 000 FBU**
- Une main d'œuvre plus spécialisée pour la conception des câbles UTP ainsi que l'installation du logiciel (webcam Monitor) et les configurations connexes. La rémunération de celle-ci est estimé à environ 5% du coût total soit un montant qui s'élève à **437 000 FBU**

En fin, le coût global du projet s'éleve à :

8 740 000 FBU+90 000 FBU+437 000 FBU= 9 267 000 FBU. En tenant compte d'une marge de sécurité de 10% pour les imprévus, le coût total s'élève à **10 193 700 FBU**

CONCLUSION GENERALE

Le but de notre sujet consistait à étudier, à base d'un réseau informatique, la technique de surveillance par caméras, la compatibilité de ces dernières avec le réseau en place et la manière de les consulter ou les contrôler étant partout dans le monde.

Par cette étude, nous avons décelé la technique d'utilisation des caméras réseau ayant des particularités sur leur principe de fonctionnement en réseau comme si c'était des ordinateurs.

Les recherches incessantes nous ont fait découvrir les techniques de conversions qu'utilisent ces caméras en transformant des signaux analogiques en signaux numériques pouvant être visualisées ou enregistrés sous forme d'images par un ordinateur. En outre, ces caméras sont manageables par des logicielles installés dans le serveur vidéo. L'apprentissage d'installation et de la manipulation de ces logicielles nous ont été bénéfiques du fait que nous sommes à jour sur cette technologie moderne beaucoup sollicité dans le monde actuel.

Nous avons ensuite montré, par un cas pratique que son implantation dans une entreprise commerciale ne nécessite pas d'énormes dépenses comme certains le croyaient. Par ailleurs, elles contribuent à l'amélioration de l'efficacité des surveillances.

Nous recommandons donc l'administration et surtout la direction de la société GASPAS COMPANY de faire tout pour que ce projet soit mis en exécution afin de limiter les problèmes liés à la sécurité du personnel et du matériel de l'entreprise.

Enfin, nous ne saurions pas achever notre travail sans toutefois émettre quelques souhaits. Si jamais, la société GASPAS COMPANY se servait de ce nouveau système de surveillance comme nous aurions souhaité, nous recommanderions aux futurs lauréats intéressés par le domaine de la vidéosurveillance de nous devancer en menant une étude sur la surveillance du réseau des caméras interconnectées entre différents agences de la société GASPAS COMPANY.

BIBLIOGRAPHIE

I OUVRAGES GENERAUX

1. GUY PUJOLLE : Les réseaux d'entreprise, réseau locaux et Bureautique
2. TUBBS DB : Histoires des caméras
   Année d'édition : 1980
3. GEORGES SADOUL : De l'autre coté des caméras
   Année d'édition : 1973
4. FAVELAS : Les caméras des Favelas
   Année d'édition 1998

II. PROJETS DE FIN D'ETUDE

1. BUKEYENEZA Désiré

   MWUMVA NEZA Joseph : Analyse technique de la cyber sécurité au Burundi : cas du réseau KAOU-NEW.

2. Lieutenant Donatien KABURA :

   Contribution à la conception d'un réseau Informatique du ministère de la défense nationale : cas d'interconnexion des réseaux locaux EMG, BFA, GMAE et les régions militaires.

3. HABONIMANA Félix

SEBATUNZI Christophe :

Etude des réseaux INTRA-EXTRANET de transmission de données par fibre optique : « cas d'interconnexion de deux réseaux locaux de la BANCOBU par un 100 Base-Fx. »

LES SITES INERNET VISITES.

WWW.DOC-ETUDIANT.FR

WWW.DLINK.FR

WWW.DEVELOPPER.COM

WWW.COMMENTCAMARCHE.NET

WWW.INFOS.DU.NET.COM