Habib Al-muhanna

WIRELESS LOCAL AREA NETWORKS; SAVINGS IN COST, TIME, AND ENERGY

Degree Programme in Information Technology
Master's Degree
2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

WIRELESS LOCAL AREA NETWORKS; SAVINGS IN COST, TIME, AND ENERGY.

Al-muhanna, Habib
Satakunta University of Applied Sciences
Degree Programme in Information Technology Master's Degree
December 2017
Supervisors: Trast, Ismo and Aromaa, Juha
Number of pages: 73
Appendices: None

Keywords: Wireless, video, network.

The purpose of this thesis is to prove that by using wireless local area networks (WLANs), it is possible to save cost, time, and energy. The focus was on network video. Small offices and users in houses could earn the benefits of using WLANs and / or network video; however, such benefits or at least some of them can surely be earned by companies and organizations.

The solution(s) offered by wireless local area networks and the solution(s) offered by network (IP) video systems were compared to the solution(s) offered by using IT devices with no network connections and the solution(s) offered by analog video systems respectively.

Introduction and theoretical information related to wireless local area networks were presented.

Introduction and theoretical information related to network video were presented.

The Case Study methodology was used to achieve the objectives of the thesis, a hypothetical case was presented, a case that has many similarities in real world.

Problems and / or drawbacks which are related to the thesis objectives were tackled and the solutions were presented by using WLANs and network video.

It was proven that it is more cost, time, and energy effective to use a wireless local area network (WLAN) and the same for using IP cameras (network video) rather than analog CCTV cameras.

Also it was mentioned how to convert a CCTV analog video system to a network video system.

A WLAN and a network video were implemented, and there was a comparison between images of an analog video system and a network video system.

CONTENTS

1 INTRODUCTION 5
2 WIRELESS LOCAL AREA NETWORKS (WLANS) 6
2.1 Benefits of WLANs 6
2.2 Applicatins of WLANs 8
2.3 Wireless LAN Technologies 10
2.4 Wireless LAN Implications 11
2.5 Wireless LANs: Historical Perspective 14
2.6 Wireless LAN Configuration 14
2.7 Wireless LAN Components and Systems 16
2.8 Peer-t-Peer Wireless LANs 17
2.9 Multiple Cell Wireless LAN 18
3 IEEE STANDARDS USED FOR IP CAMERAS 19
3.1 IEEE 802.3af 19
3.2 IEEE 802.3at 21
4 DEPLOYING WIRELESS LANS 23
5 NETWORK VIDEO 24
5.1 Overview 24
5.2 Benefits 24
5.3 Applications 27
5.4 Network cameras 29
5.5 Video Encoders 39
6 A HYPOTHETICAL CASE 48
6.1 Description 48
6.2 Problems and Analysis 50
6.3 Solutions 52
6.4 Conclusions 57
7 IMPLEMENTATION OF A WIRELESS LOCAL AREA NETWORK 58
7.1 Description 58
7.2 Procedure 58
7.3 Results 59
8 IMPLEMENTATION OF A NETWORK VIDEO 60
8.1 Description 60
8.2 Procedure 60
8.3 Results 61
9 SHOWING DIFFERNECE IN IMAGE QUALITY BETWEEN AN ANALOG CAMERA AND AN IP CAMERA 63

9.1 Using an IP camera and an anlog camera 63
9.2 Picture quality 65
10 ACCESSING A WLAN FROM THE INTERNET 70
10.1 WAN and LAN 70
10.2 Dynamic Domain Network Sevices (DDNS) 71
10.3 Port forwarding 71
11 CONCLUSIONS 73
REFERENCES 74

1 INTRODUCTION

Wireless LANs became an important part of computer science; it provided solutions for many problems in variety of fields including monitoring and security.
The work done on the IEEE 802.11 wireless LAN standard played a key role in the current status of wireless local area networks (Geier 2002, 1).

In this thesis an attempt will be made to prove advantages of wireless local area networks (WLANs.) in the aspects of cost, time, and energy.

Network video can be operated either via wired or wireless IP (Internet Protocol) networks. There are some advantages associated with network video that are not available when using traditional CCTV (closed-circuit television) systems (Axis Communications, 7).

In this thesis, an attempt will made to prove the advantages of network video related to cost, time, and energy.

2 WIRELES LOCAL AREA NETWORKS (WLANS)

2.1 Benefits of WLANs

Probably the main reason behind the growth of the use of wireless LANs is the need for mobility in a various fields of business and organizations and to have that with lower cost of network infrastructure. The following shed light on mobility and cost-saving benefits of wireless LANs (Geier 2002, 8).

2.1.1 Portability

Mobility enables users to move physically while using an appliance, mobility for some jobs is very important and feasible, like in inventory control and police stations.

If we take an example of an employee who works as an inventory control officer, if he has some items to check for new entries or updates for the inventory list, he will have to check those items in their physical locations, write down the needed information, then return to his office and finally connect (by wire) to the network to connect to the server of the organization to update the inventory list. But in the case of having a wireless local area network, all that can be made on site, needless to say how much time and effort will be saved.

So, wireless LANs can prove to be very efficient to those who need to have wireless access to data stored in centralized databases (see Figure 1) (Geier 2002, 8).

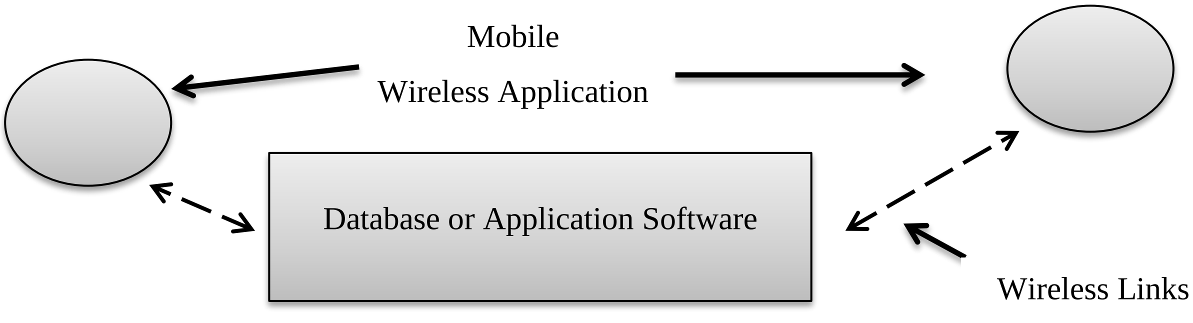

Figure 1. A wireless network supports mobile applications by providing wireless access data (Geier 2002, 8)

2.1.2 Installation in areas where wiring is difficult

In the case of areas where networking is needed but it is not cost effective to use wire-based connection, like in the case of the need to connect two building that are located on two sides of a river or a main road , the use of wireless LAN can be a solution to such a problem. Like shown in figure 2 (Geier 2002, 9).

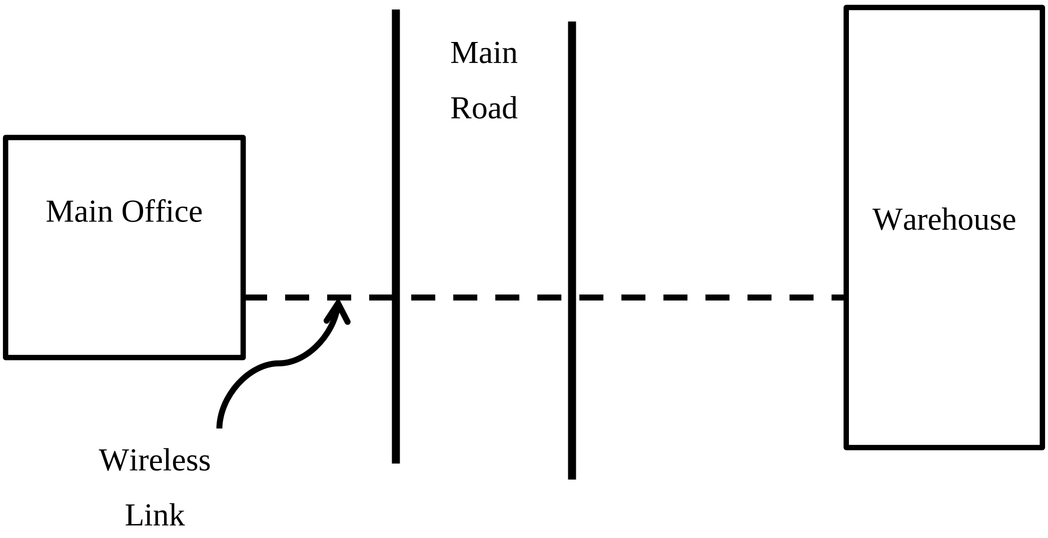

Figure 2. Wireless networks make it cost effective to provide network connectivity in situations where it is expensive and difficult to use wires (Geier 2002, 9)

2.1.3 Higher reliability, in some cases

One of the main problems that occur in wired networks are faults in cables, such faults can be caused by a number of reasons including corrosion and damage by mechanical load. It is obvious that such problems may cause the network to be off for a considerable time, hence potential loss of time, money, and information.

Since wireless networking uses no or less cabling, cabling problems is very seldom (Geier 2002, 12).

2.1.4 Less installation time

Wiring work requires time, cables are required to be extended and fixed in a way that does not or almost does not affect the aesthetic and the practical use of offices and facilities , that said, wired networks installation require more time than wireless networks which need much less cable installation (Geier 2002, 12).

2.1.5 Savings in cost

Many organizations and facilities are subject to change in locations, in case of wire-based networks, this means removing the cables from the original location, transform them to the new location, and then do the recabling process. All that cost money.
In case of wireless networks, moving a network from one location to another is mostly moving the devices which may cost nothing extra (Geier 2002, 13).

2.2 Applications of WLANs

There are many applications of Wireless Local Area Networks, in houses, offices, industries, and almost all facilities which are in need of connecting computers and other IT devices, especially when cables are not available or not feasible to use (Geier 2002, 13).
Below are some of those applications:

2.2.1 Retail business

As an example of the application of Wireless LANs in retail business; in large stores, prices may change on weekly basis, hence, the staff responsible for tagging the prices on merchandise need to have updated information, and they need that while roaming around in the store, wireless connection between their laptops and a centralized server can provide them with such updates (Geier 2002, 14).

2.2.2 In Warehouses

In warehouses, in many cases, inventory staff need to have a list of the items stored, and then they are required to update that list with the incoming and the outgoing items, and finally make that list available for management.

To do such tasks in the conventional way, a lot of paper work is needed, and a delay may occur to make the updated list available for management.

A wireless LAN enables staff to do all the above tasks from the warehouse without using any paper and with less time. And that is an example of the application of Wireless LANs in warehouses (Geier 2002, 14).

2.2.3 Healthcare sector

In the healthcare sector, there are many uses of wireless networking, including updating the patient status sheet by the doctor, informing the pharmacy of the medicine needed, viewing images of X-ray, and all that can be done from the patient room (Geier 2002, 15).

2.2.4 Hoteling business

In hoteling business, information related to reservations and services may vary on daily basis especially during certain seasons, therefore, there is a need to update such information so that staff involved can conduct their duties efficiently.

This can be done with the help of a wireless LAN.

For example, the staff responsible to make reservations need to know the updated information of the status of rooms, like how many are available, consequently he / she can provide accurate information to customers, on the other hand, this same staff will update the information accordingly so that other concerned staff (like management) can have access to updated information (Geier 2002, 17).

2.2.5 Small offices and houses

Many things can come to mind when thinking of the applications of wireless LANs in homes and small offices like using mobile devices while connected to the Internet, sharing IT devices like printers, using wireless security cameras, and other applications (Geier 2002, 17).

2.3 Wireless LAN Technologies

IEEE (Institute for Electrical and Electronic Engineers) 802.11 is a group of media access control (MAC) and physical layer (PHY) specifications for implementing wireless LAN (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. Those standards are created and maintained by IEEE LAN/MAN Standards Committee (IEEE802). The base version of the standard has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. The 802.11 family consists of a series of half-duplex over-the-air modulation techniques which use the same basic protocol. Although 802.11 was the first wireless networking standard in the family, 802.11b was the first to be widely accepted, followed by 802.11a, 802.11g, 802.11n, and 802.11ac (Website of Wikipedia).

There are a number of wireless LAN solutions with varying levels of standardization and interoperability, one of those solutions is the Wi-Fi (IEEE 802.11b).

802.11 technologies are widely used in homes, offices, and enterprises, the IEEE finalized the initial standards for wireless LANs, IEEE 802.11 in 1997, this standard specified a 2.4 GHz operating frequency (data rate 1 and 2 Mbps). Because of low data rates compared to Ethernet, products based on that initial standard didn’t achieve the selling rates that many hoped.

In 1999, IEEE published two supplements to 802.11 which are 802.11 a and 802.11 b (Wi-Fi).

Bluetooth wireless technology is an industry specification for short-range RF-based connectivity. Bluetooth sends out very weak signals, that low power limits the range of a Bluetooth device to about 10 meters.

There are two categories of Wireless LANs: ad hoc WLANs and Wireless LANs with infrastructure, in ad hoc WLANs, number of nodes are connected wirelessly together to make a peer-to-peer communication, in that type of networks, only devices within transmission range of each other can communicate with each other.
In wireless LANs with infrastructure, a wireless or wired backbone of high speed is used; wireless devices or nodes access the backbone via access points which allow the nodes to share the network resources in an efficient manner (Website of the University of Texas at Arlington).

2.4 Wireless LAN Implications

The following are considered as implications of wireless Local Area Networks:

2.4.1 Multipath Propagation

It is the combination of transmitted signals and those reflected (for example from walls) causing corruption of received signals. Figure 3 illustrates. As the delay time (compared to primary signal) of the reflected signal increase the distortion of the received signal at the receiver increases, and it is possible that the signal will not be detectable (Geier 2002, 21).

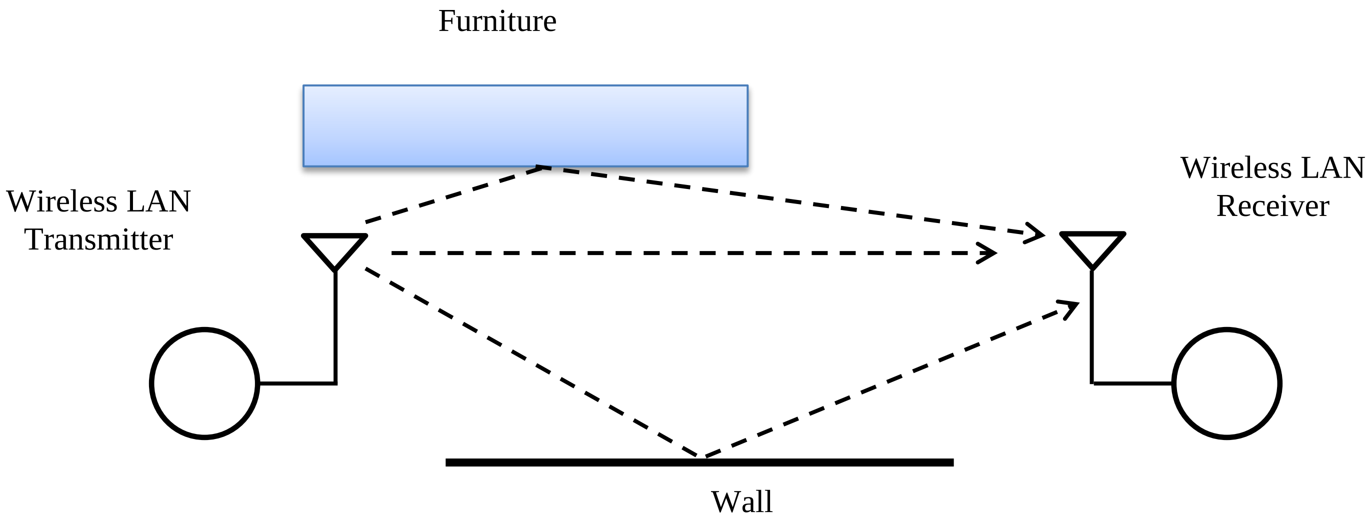

Figure 3. Multipath Propagation decreases quality of the signal at the receiver (Geier 2002, 21)

Equalization and antenna diversity are methods used to reduce the problems caused by multiple propagation (Geier 2002, 22).

2.4.2 Loss of Path

One of the important things that should be considered when designing a wireless LAN solution is path loss between the transmitter and receiver, range between transmitter and receiver can provide expectation for path loss and hence provide important information for the designer pertaining requirements for transmission power levels, the sensitivity of the receiver and signal-to-noise ratio (SNR) (Geier 2002, 22).

2.4.3 Interference of radio signals

Wireless LAN transmission and receiving of signals are vulnerable to atmospheric noise and transmissions from other systems; also, wireless LANs can interfere with each other (Geier 2002, 22).

2.4.4 Limitations of operation times of batteries

Portable devices (like laptops) are usually most of the devices used in wireless LANs; the time of using such devices depend mainly on their batteries.
When the laptop battery of a warehouse staff (for example) needs to be charged, this staff needs to stop his mobile part of the job to charge his laptop, so mobile operating time of staff could be reduced for hours daily due to time needed for charging the batteries of their mobile devices (Geier 2002, 25).

2.4.5 Security

The following are examples of security threats that wireless LANs may encounter:

- Service denial

  In this case, the wireless LAN is flooded with messages by an intruder, which will affect (and may be even stop) the availability of the network resources (Website of SANS Information Security Training | Cyber Certifications | Research 20003).

- Spoofing and Hijacking

  In this case, the intruder (using the identity of a valid user) can gain access to data and resources in the network (Website of SANS Information Security Training | Cyber Certifications | Research 2003).

- Eavesdropping

  In this case, the intruder intercept information transmitted by the wireless LAN, this can be done from within the building where the wireless LAN devices are located or from outside the building (Website of SANS Information Security Training | Cyber Certifications | Research 2003).

2.4.6 Issues related to installation

Unlike wired networks, the installation of wireless LANs is not predictable; the design of the building (including walls and ceilings), the furniture within, and the movement of objects can all affect the propagation of signals by attenuation and even changing of transmission paths. Hence the actual pattern of the radiation will be distorted taking the shape of a jagged appearance, as shown in Figure 4.

In order to avoid or reduce installation problems, propagation tests should be performed as part of the design process of the wireless LAN (Geier 2002, 29).

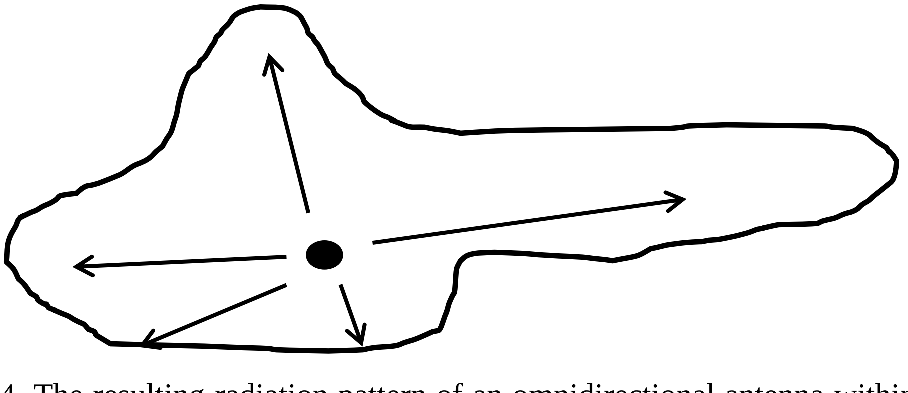

Figure 4. The resulting radiation pattern of an omnidirectional antenna within an office building is irregular and unpredictable (Geier 2002, 30)

2.4.7 Risks to health

One of the main common concerns is whether wireless networks pose any form of health risk. Thus far, there has been no conclusive answer (Geier 2002, 30).

2.5 Wireless LANs: A Historical Perspective

In 1971, network technologies and radio communications were brought together for the first time as a research project called ALOHANET when computer sites at 7 campuses located in 4 islands communicated with a central computer without using phone lines.

By the authorization provided by the Federal Communications Commission (FCC) in 1985 of the public use of the Industrial, Scientific, and Medical (ISM) band, by that, the radio-based LAN developed commercially (Geier 2002, 31).

Institute of Electrical and Electronic Engineers (IEEE) 802 Working Group began in the 1980s development of standards of wireless LANs.

The Wireless LAN medium Access Control and physical layer specifications were developed by the IEEE 802.11 Working Group.

The supplements (802.11a and 802.11b) to the 802.11 standard were released by IEEE to increase data rate in wireless LANs up to 54Mbps (Geier 2002, 32).

2.6 Wireless LAN Configuration

2.6.1 The architecture of wireless LAN

There are three modes of wireless LANs

- Infrastructure mode

  Any kind of devices that can be connected with every type of work station of WLAN with the use of access points is called infrastructure network mode.

- Ad hoc network mode

  In this mode, all workstations are connected with other workstations with no obstacles.

- Mixed network mode

  It is a mix of infrastructure mode and ad hoc mode, the work stations can work simultaneously.

Computer architecture is the process of assembling parts of computer hardware in computer networking, if this is used in wireless LAN; it is called a Wireless LAN Architecture. It is a technique of the design and arrangement of components in a wireless LAN device. Transceiver is a combination of transmitter and receiver; it is an essential part of the WLAN architectures called Access Points (Website of WIFI NOTES 2015).

Networks perform the following functions (like Ethernet and token-ring counter-parts) in order to establish information transference from source to destination

1. Providing a path for data transmission by the medium.
2. Providing sharing of a common medium by media access technique (Geier 2002, 34).
3. Ensuring that each link transfers the data intact by synchronization and error control mechanisms.
4. Moving data from origin to destination via routing mechanisms.
5. Interfacing appliances such as a pen-based computer to application software hosted on a server by connectivity software.

(Geier 2002, 35).

2.6.2 Medium Access Control

A MAC (Medium Access Control) sublayer, as shown in figure 5, is a function in radio-based wireless LAN for Data Link, it enables the sharing of a common transmission medium by appliances by means of carrier sense protocol like in Ethernet (Geier 2002, 35).

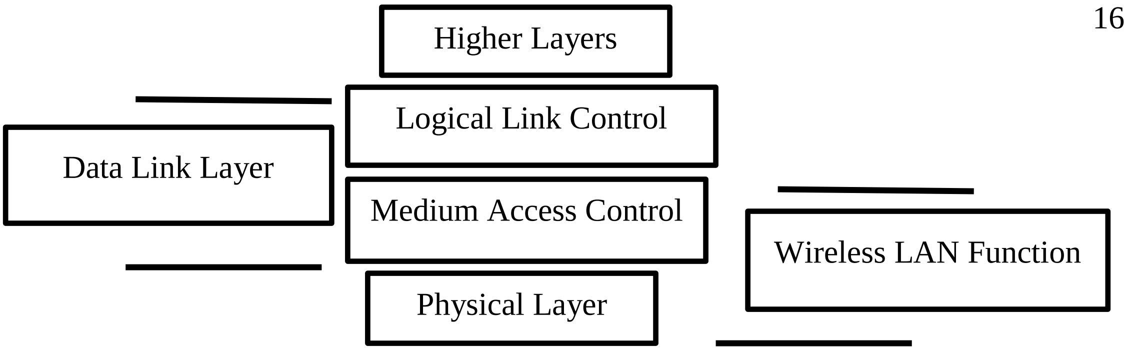

Figure 5. Functions related to Medium Access Control (MAC) and Physical layers are provided by a Wireless LAN (Geier 2002, 35)

2.6.3 Physical Layer

This layer defines electrical, mechanical, and procedural specifications to provide transmission of data through a communication channel (Geier 2002, 36).

2.7 Wireless LAN Components and Systems

Major components:

- Wireless (NIC) Network Interface Card.
- Wireless local bridge (usually referred to as Access Point).

The wireless NIC does the interfacing between an appliance (like a laptop) with the wireless network while the Access point interfaces the latter with the wired network (Geier 2002, 46).

2.7.1 End User Appliances

By end user appliances, users interface with the network, such appliances include: computers, tablets, smart phone, and many other devices (Geier 2002, 46).

2.7.2 Software of network

The network software resides on different parts of the network, in most cases, appliances interface with a network operation system (NOS) via TCP/IP (Transmission Control Protocol / Internet Protocol) (Geier 2002, 47).

2.7.3 Antenna

Radiation of the modulated signal through air is done by the antenna; there are many shapes and sizes of antennas (Geier 2002, 51).

2.7.4 Channel of communications

Communications channel is used by wireless LANs; they use air as a medium for information to flow from source to destination.

At the surface of earth, where the majority of wireless LANs operates, gases like nitrogen and oxygen are contained in pure air. This atmosphere is an effective medium for wireless LANs operation.

When there is rain, fog, and snow, the amount of water in the air is increased, hence causing a significant attenuation to the propagation of modulated wireless signals.

Other example of things that cause attenuation (which is a decrease in the amplitude of the signal) is smog (Geier 2002, 53).

2.8 Peer to Peer Wireless LANs

A peer to peer wireless LAN (like the one in figure 6) is probably sufficient for small single-floor offices and houses. Such a LAN requires NICs only in the devices connected to it. An access point isn't required unless there is a need to connect to resources based on wired network like servers (Geier 2002, 54).

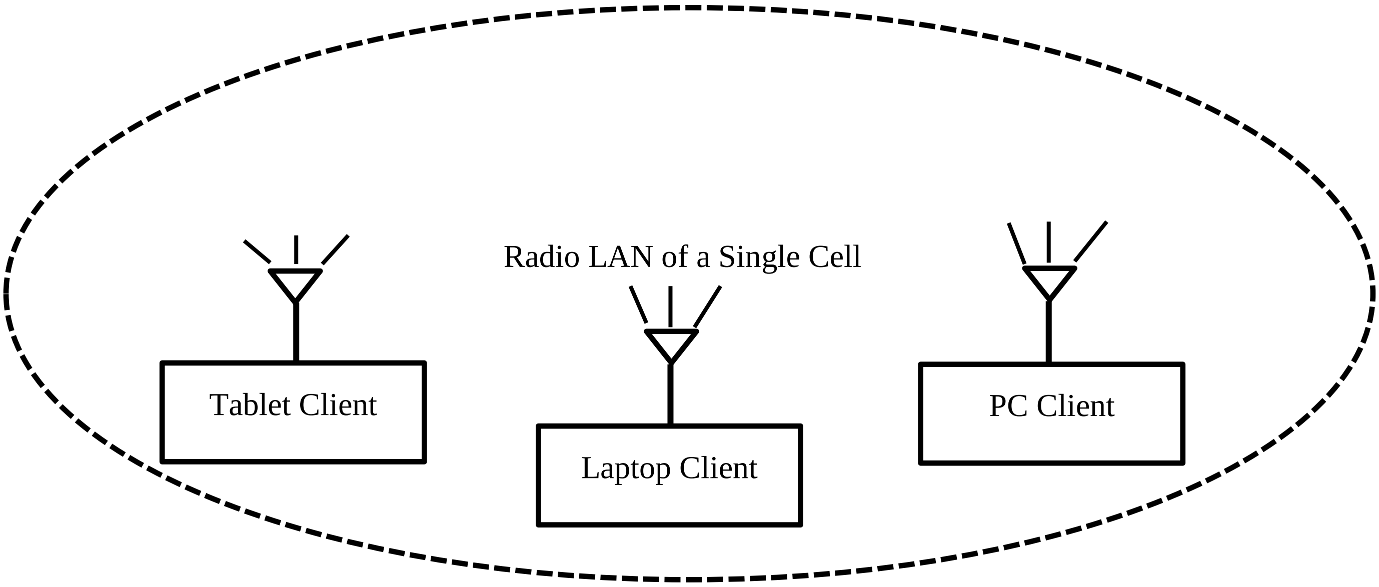

Figure 6. Peer-to-Peer Wireless LAN (Geier 2002, 54

2.9 Multiple Cell Wireless LAN

In case there is a need for greater range than the limitations of a single cell wireless LAN, a set of access points and a wired network backbone can be used to make a multiple-cell wireless LAN. As shown in figure 7, this can be used, for instance, in multiple floor buildings (Geier 2002, 55).

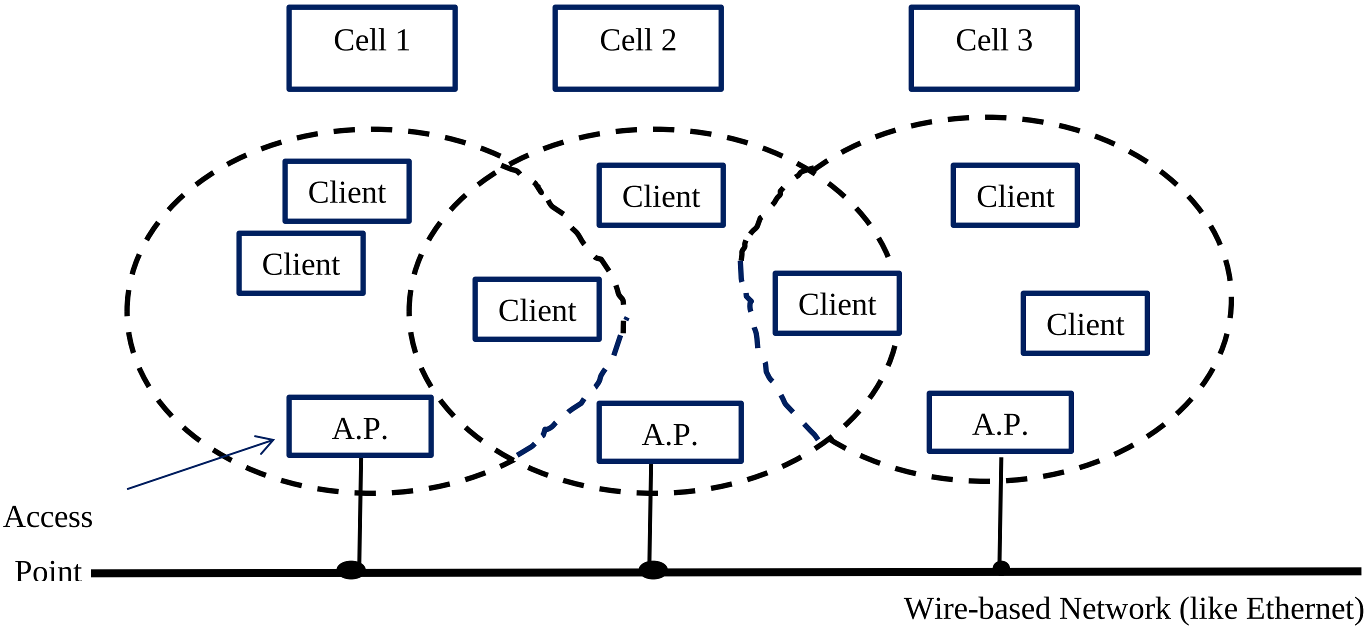

Figure 7. A multiple cell LAN (Geier 2002, 56)

3 IEEE STANDARDS USED FOR IP CAMERAS

3.1 IEEE 802.3af

IEEE 802.3af is one of the IEEE standards that can be used in video networking; it gained universal adoption because PoE (Power over Ethernet) technology became popular, hence to achieve compatibility between modern PoE equipment (website of Veracity global 2016, a).

3.1.1 (PoE) Power over Ethernet

PoE is a technology that allows network cables to supply electrical power.
As shown in figure 8. A network camera normally needs two cables connected to it, one is the network connection; which is used to carry data, and the other is called the power connection; which used to carry electrical current needed to operate the camera (website of Veracity global 2016, b).
But when using PoE technology, the network connection will be sufficient; it will do the two functions.
The benefits of using PoE are savings in time, savings in cost, flexibility, safety, reliability, and scalability (website of Veracity global 2016, b).

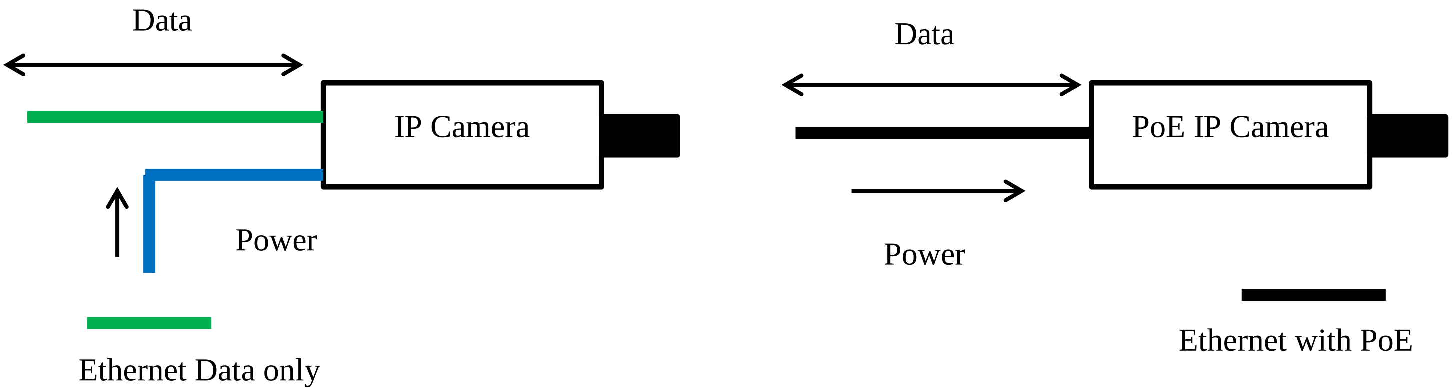

Figure 8. Using PoE (website of Veracity global 2016, b)

3.1.2 Upgrading to PoE

It is an easy task to add PoE to the network; there are ways to do that:

1. **A PoE switch**

   This is a network switch that has PoE injection built in, as shown in figure 9, other network devices can be connected to the switch in a normal way, the switch will detect if they are PoE-compatible and will power them automatically (website of Veracity global 2016, b).

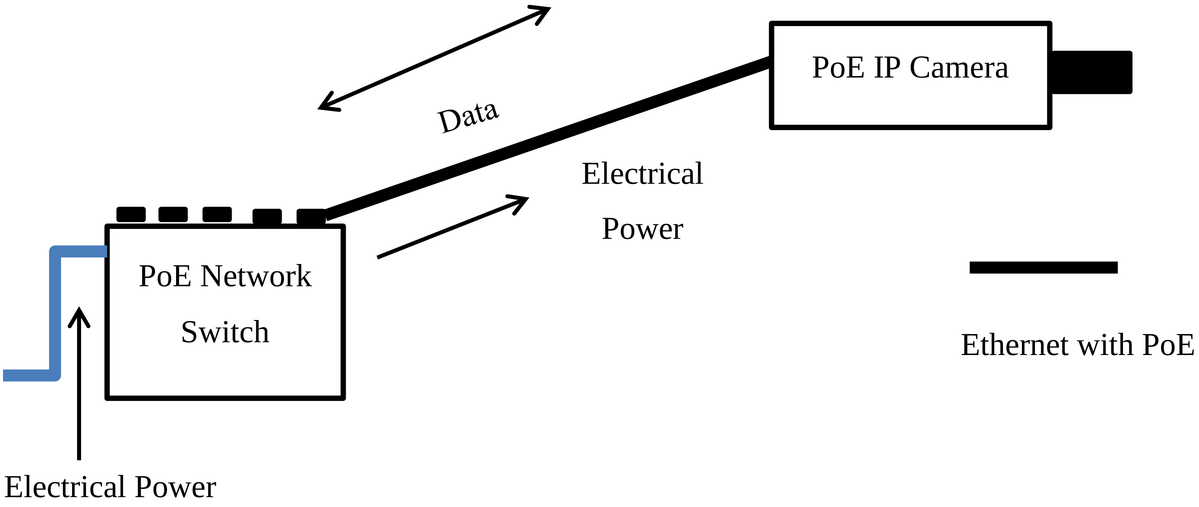

Figure 9. Using a PoE switch (website of Veracity global 2016, b)

2. **A midspan (or Power over Ethernet injector)**

   It is used to make PoE capability to conventional non-PoE network links. As shown in figure 10 (website of Veracity global 2016, b).

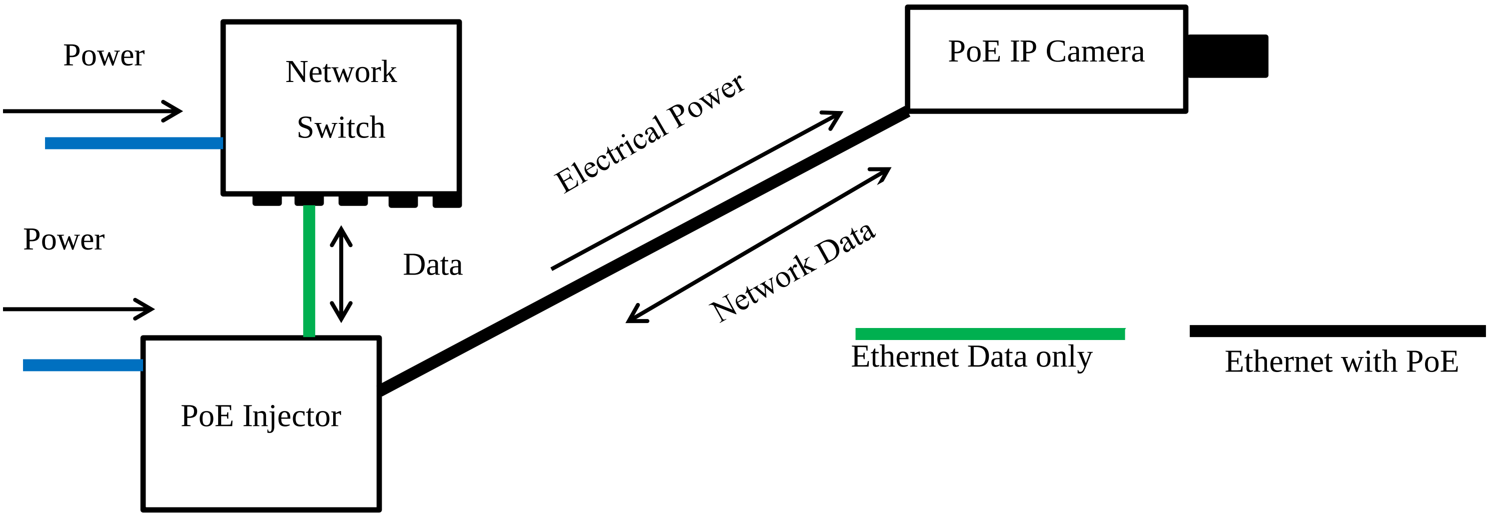

Figure 10. Using a PoE injector (website of Veracity global 2016, b)

Also for powered devices like IP cameras, it is possible to use a PoE splitter, which is patched to the network connection of the camera; it taps off the PoE power to a suitable value for the camera (website of Veracity global 2016, b).

3.1.3 IEEE 802.3af PoE

It is a developed technology , thanks to ieee 802.3af PoE it is possible to ensure reliable operation in any configuration using regular Ethernet, the user needs to do the normal wiring of the network, and the power delivery will be taken care of by the equipment.

The 802.3af PoE standard is suitable for devices that needs electrical power of up to 13 W. High power PoE systems are not always compatible with 802.3af PoE (website of Veracity global 2016, a).

3.2 IEEE 802.3at

This standard was introduced to increase the available power that can be delivered via Ethernet cables, also referred to as PoE Plus, PoE Plus means that a more full range of network equipment will be using power over Ethernet, this includes IP cameras with heater / blowers, It is important to mention that IEEE 802.3at is used alongside IEEE 802.3af, it is not a replacement for it, IEEE 802.3af is expected to be used by most of Ethernet devices for the near future, PoE Plus has the following characteristics:

1- **More electrical power**

It approximately doubles the amount of power available to the device, 25.5 Watts.

2- **It is compatible with IEEE 802.3af PoE**

Switches and injectors used in PoE plus recognize IEEE 802.3af powered devices and make PoE available to them as normal. On the other hand, PoE Plus powered devices can be connected to 802.3af PoE switches and injectors with the assumption that they restrict the amount of power used accordingly.

3- Smart power budgeting

IEEE 802.3at contains a range of power sources and powered devices for communication and negotiation for the allowance of power.

(Website of Veracity global 2016, a).

4 DEPLOYING WIRELESS LANS

The deployment of wireless LANs has many scenarios; the scenario of Wireless LANs used in a small offices and homes will be tackled.

The number of computers in a small office is usually very small, in general, a wireless LAN in a small office contain from 2 to 10 computers , it is usually used to share files, printers, and devices for backing up data.

Sometimes Wireless LANs of small offices share a single Internet connection, in most cases Wireless LANs used in small offices have the following requirements:

- **No high security**
- **Normal speed**
- **Small budget**

Thus, a wireless LAN can be used in a small office with no complexity, with reasonable level of security, has the ability to connect to the Internet, and doesn't cost much. The deployment of a wireless LAN in a house or a small office normally requires an Access Point (AP), and a wireless network interface card (NIC) for each device that is desired to be connected to the network. The usual problem that arises when deploying such a wireless LAN is selecting the right spot for the AP, the location determines the strength of the signal received by the network users.

Aps must be located in a position with the least obstructions; otherwise, the wireless LAN may not operate efficiently. It is recommended to do a site survey to find out which spot is in the center of the premises and from which the best signal can be received. Another problem when deploying a wireless LAN is the security issue, unauthorized persons may use their NICs to connect the network; hence, it is important to use authentication and encryption to reduce risk of security breaches (website of Computer help and tips).

Among the many benefits of the use of a local area network is the ability to include video devices within the network, and that video will become network video.

5 NETWORK VIDEO

Like in telephone communication, for example, network video is conducted either by wires or wirelessly, in this network; video, audio, and other data are received and transmitted over the infrastructure.

There are many advantages of network video especially in the field of security, for example network video used in surveillance is better than the traditional closed-circuit television (CCTV) analogue systems (Axis Communications a, 7).

5.1 Overview

As Network video is applied in security industry, it is often called IP-based video surveillance or IP surveillance, a wired or wireless IP network is used for the communication of video, audio, and other data. There is an option of applying Power over Ethernet (PoE) technology; in this case the network can feed power to network video devices. It is possible when using network video to monitor and record video from anywhere on the network, for example, this is possible in a local area network and on a wide area network like the Internet (Axis Communications a, 7).

Network video system circuits may include the following components:

- Network camera.
- The network.
- The server and storage.
- Video management software.
- Video encoder to connect analog cameras to IP network.

(Axis Communications a, 8)

5.2 Benefits

Network video has many benefits, many of them cannot be obtained from the use of traditional analog CCTV system (Axis Communications a, 8), and those benefits include:

5.2.1 High quality of image

It is very important, especially for security applications, to have a clear picture of incidents and faces of people involved. By the use of progressive scan and HDTV (High Definition Television) /megapixel technologies, it is possible for a network camera to give a good image quality and a high resolution, compared to an analog camera. The conversion of the images to a digital form is made only once in an IP camera system, unlike the multiple conversions made in an analog camera, the more the conversions are the weaker the signals become, hence, negatively affecting the quality of images (Axis Communications a, 8).

5.2.2 Ability of remote access

In network video any authorized user can have access to live and recorded videos for virtually any location the video is connected to, advantages of such feature is the ability to give other entities like security companies access to the images captured (Axis Communications a, 9).

5.2.3 Managing events and intelligent video

Usually, there are many unimportant videos recorded by cameras, Ip cameras can be programmed to send videos for recording only under specified circumstances, like the opening of a gateway or the presence of people, etc.. Or this can be made by a time schedule. Also it is possible to tag video recordings with a type of information called metadata so that to make it easier to search through videos (Axis Communications a, 9).

5.2.4 Ease of Integration

Devices used in network video systems which are based on open standards can easily be integrated to other video systems such as a building management system, while analog camera systems are seldom capable of integration with other systems (Axis Communications a, 10).

5.2.5 Scalable and flexible system

The growth of an IP video system can be made in very small additions like one camera at a time, number of applications like audio and video can be transmitted using the same cable or wireless media. Since network video uses standard IT devices and protocols; parts of IP network video system can be placed in another location and managed from virtually anywhere as long as it is connected to the network, for example, servers used for storage can be placed far from the location where the cameras are installed, this can be very important regarding, for example, the security of information (Axis Communications a, 10).

5.2.6 Cost

Usually an IP network video system costs less than a CCTV system; the network video equipment can be integrated or used using the already existing IP network. Network video can play a role in making more profits in businesses like in retail business when network video is used to monitor the flow of customers and organize the locations of staff and goods accordingly.

Supporting power over Ethernet (PoE) is a very important option in network video that saves costs of cables and installations. PoE makes it possible for the network video system to use Ethernet cables for both data and power supply (Axis Communications a, 10).

5.2.7 Security of communication

In network video there are many tools for information security; including: username and password, authentication, IP address filtering, and data encryption (Axis Communications a, 11).

5.3 Applications

There are many applications of network video; most of them are in the field of security surveillance (Axis Communications a, 12). The following are some of the typical applications of network video:

5.3.1 Retail business

The use of network video in retail stores plays an important role in reducing theft, management of staff and management of goods. By the help of network cameras; management can have a better idea about areas of store that need more staff and in which times and dates, also a better idea of locating the goods in a way comfortable to customers (Axiss Communications a, 12).

5.3.2 Transportation sector

In transportation sector, network video is of a big help in the field of security of people and assets, cameras installed in airports, harbors, stations, trains, busses, and other related locations can all be connected via a network to transmit images to a security center at which analysis and reviewing of images can help in stopping crimes or help in catching criminals. Beside security applications, cameras in transportation sector especially in airport can help in locating airplanes, vehicles, available parking spots, etc...(Axis Communications a, 12).

5.3.3 Business of banking and finance

Banks can use network videos in number of applications but mainly in security, and for example in monitoring the ATMs (Automatic Teller Machines) from a headquarters for security and analytical purposes (Axis Communications a, 13).

5.3.4 Surveillance in cities

Among the most important tools in fighting crime are surveillance cameras, cameras can help in preventing crimes by being a deterring factor, they can also help a lot in catching suspects and criminals. Thanks to wireless networks, a lot of network video cameras can be installed with reduced costs, such wide spread of cameras may enable police to respond to live criminal acts (Axis Communications a, 13).

5.3.5 Education sector

In addition to the security use of network video in education facilities, network video is used in distance learning, for example, students from different parts of the world can join their colleagues on campus in live lectures and they can interact with their teachers and their colleagues from their distant locations (Axis Communications a, 13).

5.3.6 Health sector

Network cameras is very useful in healthcare facilities, for example, a doctor can have a quick look at his patient from his office, or a psychiatric can observe patients held in locked rooms (Axis Communications a, 14).

5.3.7 Industry

It can help in providing safety, security, more efficiency. IP cameras can be used in monitoring manufacturing lines, for faster troubleshooting and maintenance due to the earlier detection and response to of failure location. And IP cameras can be useful in evaluation of staff performance (Axis Communications a, 14).

5.3.8 Infrastructure of critical nature

Network video plays an important role in the security and efficient operation of solar energy plants, wind energy plants, electrical substations, and any infrastructure facility which is usually located far from highly populated areas (Axis Communications, a 14).

5.4 Network cameras

There are many types of network cameras made for different needs, some of the things that are needed to be considered when purchasing a network camera are what it is needed for, how much light is a usually available and environmental conditions (Axis Communications a, 15).

5.4.1 Definition of a network camera or an IP camera

A network camera, shown in figure 11, usually referred to as IP (Internet Protocol) camera, is a camera that mainly used to transmit video and audio signals via an IP network, like a Local Area Network (LAN), an IP camera can be used for live images and/or recordings, there are different ways to control the operation of an IP camera, it can be operated according to a schedule, an event, or when requested.
The data that the camera captures can be saved locally and/or at a remote location. When connected to the Internet an IP camera can be easily accessed by authorized personnel (Axis Communications a, 15).

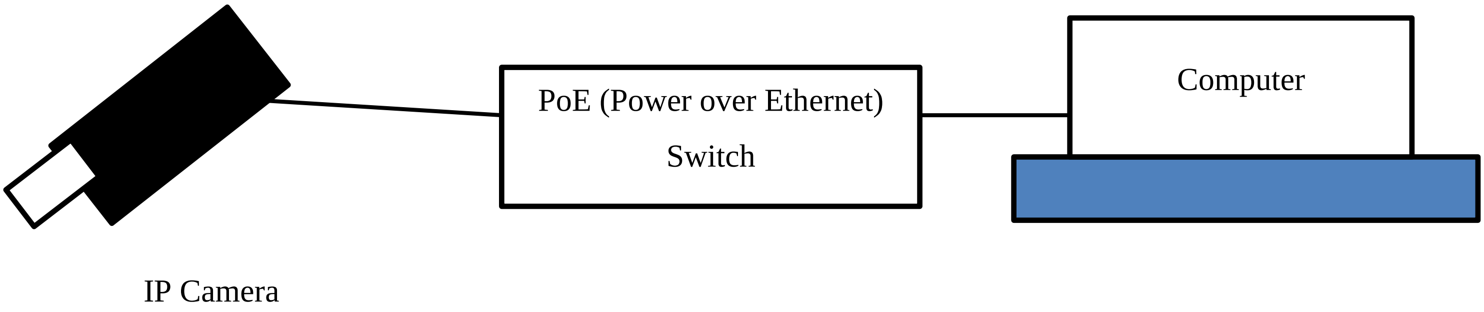

Figure 11. A network camera connects directly to the Internet (Axis Communications a, 15)

A network camera can be looked at as a unit that consists of a computer and a camera.
Lens, image sensors, processor(s), and memory are the main parts of in IP camera.

The processors are used for image processing, compression, video analysis, and network related functions.

In addition to saving video files, the memory is used mainly for the storage of the computer program of the camera.

The network camera, shown in figure 12, has its own IP address (like a computer), the IP camera can be directly connected to a wire-based or wireless network and can be located within the range of that network, that is not the case with a web camera which can only be operated when connected to a PC. Features of an IP camera may include audio capabilities, built-in support for Power over Ethernet (PoE), and slot of memory device for local storage (Axis Communications a, 15).

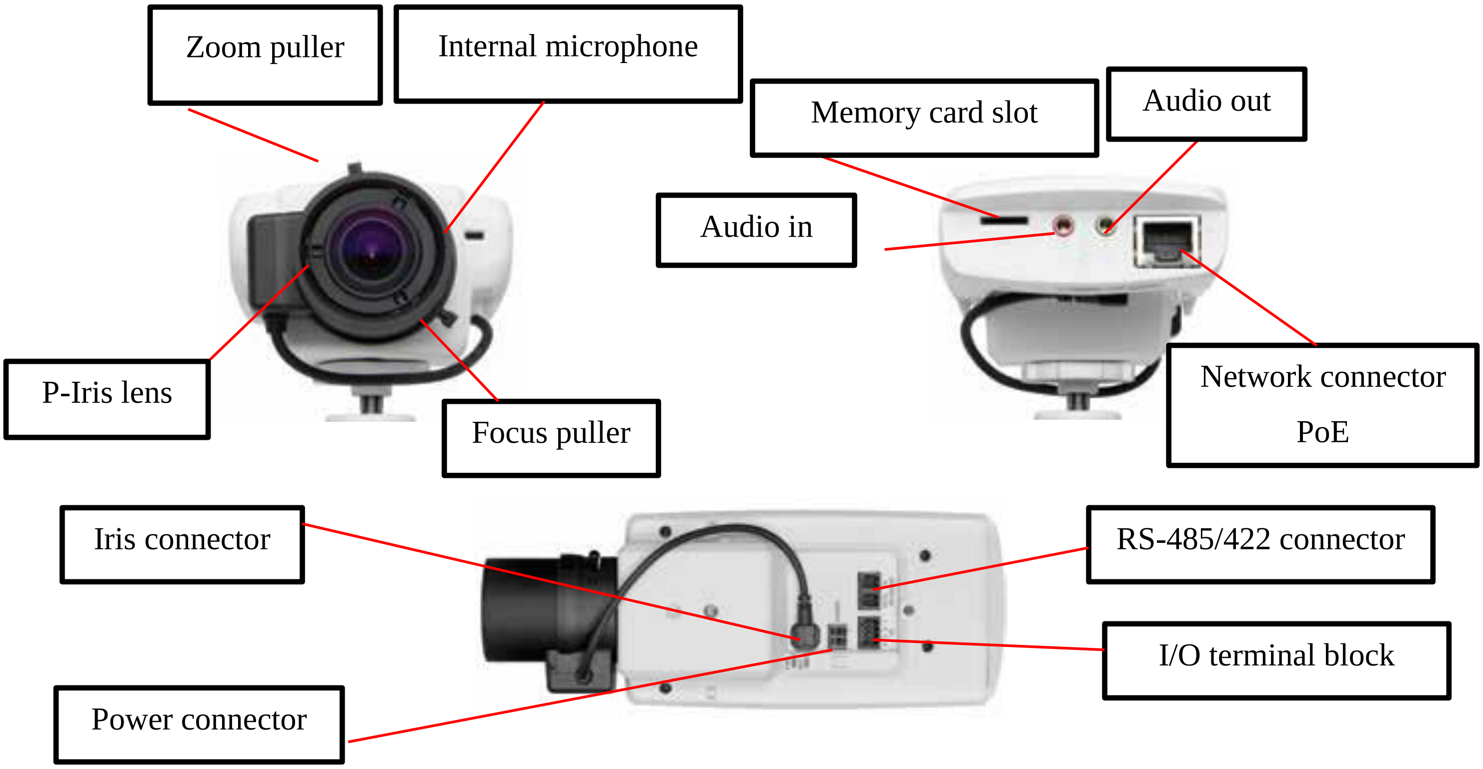

Figure 12. Front, back and underside of a network camera (Axis Communications a, 16)

By entering the IP address of a network camera in the address bar of the of the computer's browser, it is possible to access that camera remotely, once the connection is established; the start page of the camera and links to the configuration pages are automatically shown in the browser of the Internet (Axis Communications a, 17).

5.4.2 Handling of difficult scenes

An IP camera needs to overcome number of difficulties in order to be able to provide good quality images, which is very important in security applications. Many conditions affect the ability of the camera to capture clear image, some are:

- Changes in the level of light.
- Darkness.
- Fog and smoke.

(Axis Communications a, 18).

To enable the camera to provide usable video or pictures in spite of such conditions; some features are to be added to the camera (Axis Communications a, 18), including:

1- The f-number (Len's ability to gather light)

The smaller the f-number the better gathering light ability there is in the camera, and generally the better is the performance of the camera in low light conditions. For types of lighting higher f-number is preferred though.

Not only the lens of a camera defines the sensitivity to light, but also the image sensor and image processing play a role (Axis Communications a, 18).

2- Iris

In case of constant light level, manual adjusting feature of the iris of the camera lens is a sufficient adjusting feature, but that is not the case for scenes with different levels of light, for such scenes, automatically adjustable iris, DC-iris / P (Precise) Iris, is the practical choice (Axis Communications a, 18).

3- Day and night operation

An IP camera can be equipped with automatically removable infrared-cut filter, during daytime the filter is kept on, hence, the images taken by the camera is normal are in the colors that can be seen by the eye, during nighttime the filter is removed, allowing the camera to take advantage of the nearby infrared light to capture images and produce them in clear black and white colors. As shown in figure 13 (Axis Communications a, 18).

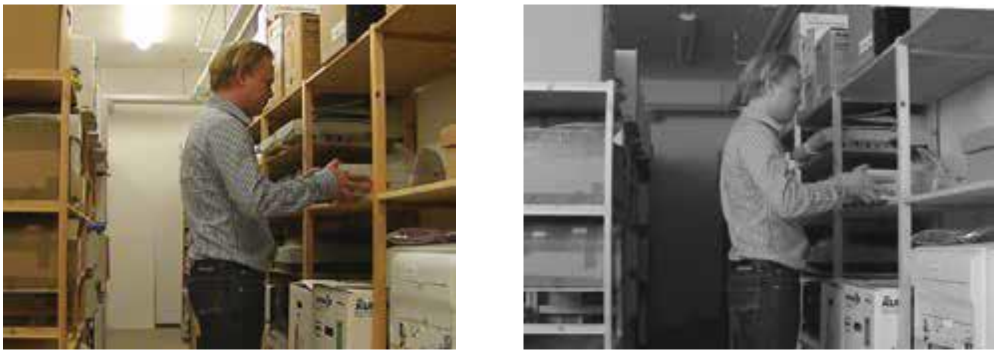

Figure 13. Daytime image Nighttime image

(Axis Communications a, 19)

4- Infrared illuminators

Infrared (IR) built-in light emitting diodes (IR-LEDs) or a separate infrared illuminator can be used in order to enable the IP camera to produce good quality black and white images in low light conditions or in complete darkness.

Although near infrared light from the moon or from street lights for example is not visible to human eye, it can be detected by the camera image sensor and utilized by the camera (Axis Communications a, 19).

5- Resolution

The resolution of a camera is determined by the number of pixels in the image furnished by the image sensor. The resolution (depending on the lens used) can mean either more details in the image or a wider view of the scene.

A camera of one megapixel sensor provide images of one million pixels or more, in case of using wider view of the scene, it can provide a wider coverage than a non-megapixel camera (Axis Communications a, 20).

6- Wide dynamic range (WDR)

When the camera is installed in a scene combined of very bright light areas and dark areas, like an entrance door area in a supermarket or a tunnel used by subway trains, in such scenes it is required to deal with high difference of light levels in one image, therefore; a camera with wide dynamic range feature is needed. Such a camera usually incorporates an image sensor which takes different exposures, for example, long exposure for dark areas and short exposure for very bright areas, and combines them into a single image making it possible to see objects in the very bright areas and in the dark areas (Axis Communications a, 21).

7- Thermal Radiation

Thermal radiation can also be used to generate images; figure 14, a thermal network camera does not need a source of light. Such a camera detects thermal radiation from every object that has a temperature higher than zero degrees Kelvin (Axis Communications a, 21).

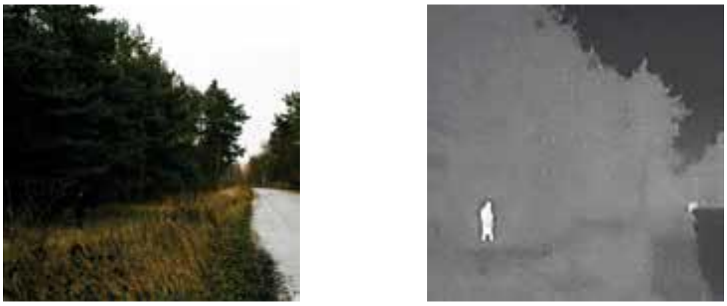

Figure 14. Conventional camera image Thermal camera image
(Axis Communications a, 21)

5.4.3 Types of network cameras

Network cameras can be put into two main types depending whether they are made for indoor and outdoor use or they are made for indoor use only.

Unless the outdoor camera has or equipped with protective enclosure, an external protective housing is needed (Axis Communications a, 24).

Regardless of being designed for indoor or outdoor locations, network cameras can be further classified into the following categories:

1- Fixed.
2- Fixed dome.
3- Covert.
4- Thermal.

(Axis Communications a, 24).

Fixed network camera

This type of network camera has a fixed viewing direction after it is installed, the Fixed Camera may come with fixed, variable focal length, or motorized zoom lens, in some cameras; the lens may be exchangeable.

A fixed camera is a conventional camera type, the camera and its pointing direction are clear to see, therefore it is recommended to use such cameras when it is needed to have a very noticeable camera, samples of fixed network cameras are shown in figure 15 (Axis Communications a, 24).

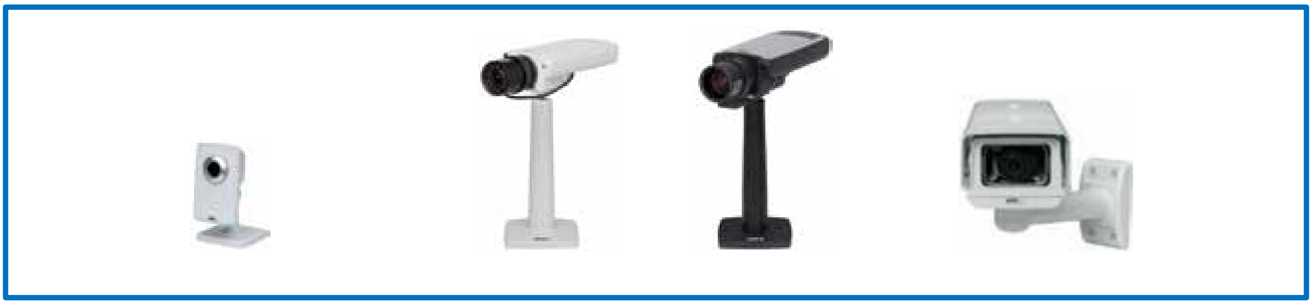

Figure 15. Samples of fixed network cameras (Axis Communications a, 24)

Fixed dome network camera

Putting a fixed camera in a dome design makes it a fixed dome camera, fixed dome network camera can be directed to point at any direction but this direction is not known easily, unlike the pointing direction of a fixed camera. Also it is not possible or it is not easy to temper with the pointing direction of fixed dome, samples of fixed dome cameras are shown in figure 16 (Axis Communications a, 24).

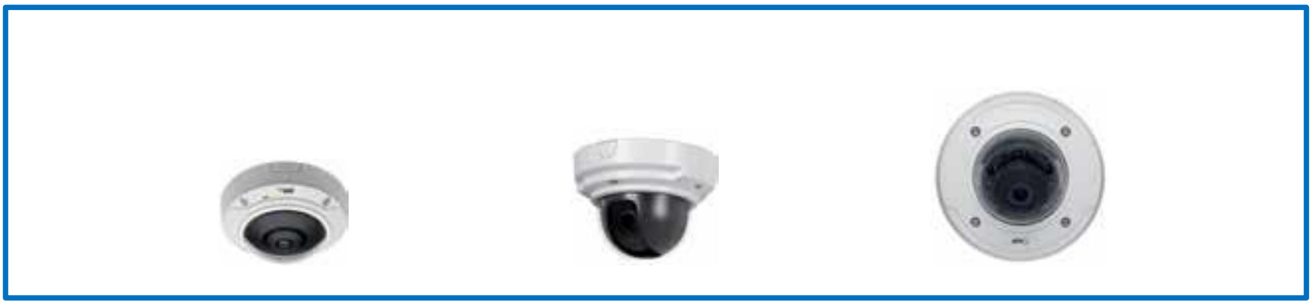

Figure 16. Samples of fixed dome network cameras (Axis Communications a, 24)

What is known as panoramic or 360° camera is a fixed dome network camera with wide-angle lens and megapixel sensor that provides 360° field of view, as shown in Figure 17 (Axis Communications a, 25).

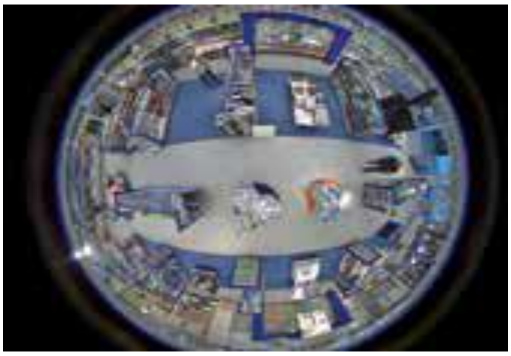

Figure 17. A view of a panoramic camera (Axis Communications a, 25)

Covert network camera

This type of cameras is designed to be placed within the environment in a way that it is almost impossible to be seen. Such cameras can be placed on their own in places where they are not easy to be discovered or they can integrated with other devices like an ATM (Automated Teller Machine), samples of covert network cameras are shown in figure 18 (Axis Communications a, 27).

Figure 18. Covert cameras (Axis Communications a, 27)

PTZ network camera

A PTZ network camera is a camera that can provide the following functions: Pin, tilt, and zoom, samples of PTZ network cameras are shown in figure 19 (Axis Communications a, 28).

Pan: Panning is moving the lens of the camera to one side or another.
Tilt: Moving the lens of the camera up and down keeping a constant horizontal level.
Zoom: Zooming is changing the focal length of the lens so that to make subjects seem closer or further away (website of Video maker).

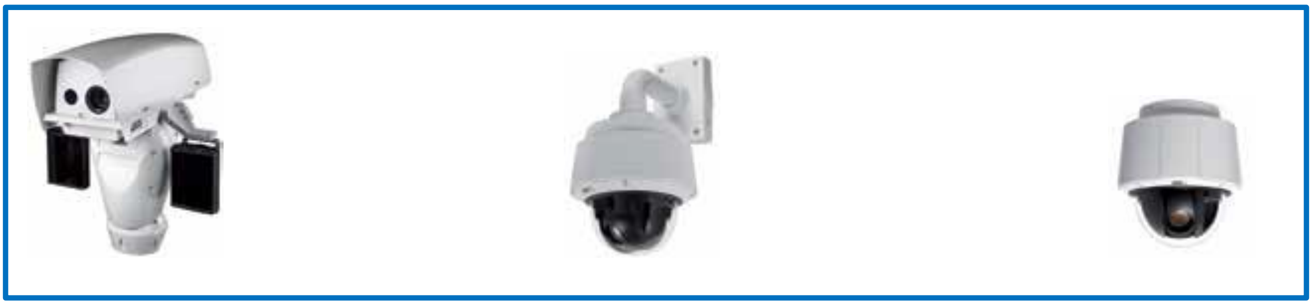

Figure 19. Samples of PTZ network cameras (Axis Communications a, 28)

Thermal network cameras

A thermal network camera uses the heat emitted from an object to create an image of that object, if the temperature of the object is within certain limits, such images are in black and white in general, they can be colored artificially though, so that different shades can be easily distinguished, samples of thermal network cameras are shown in figure 20 (Axis Communications a, 31).

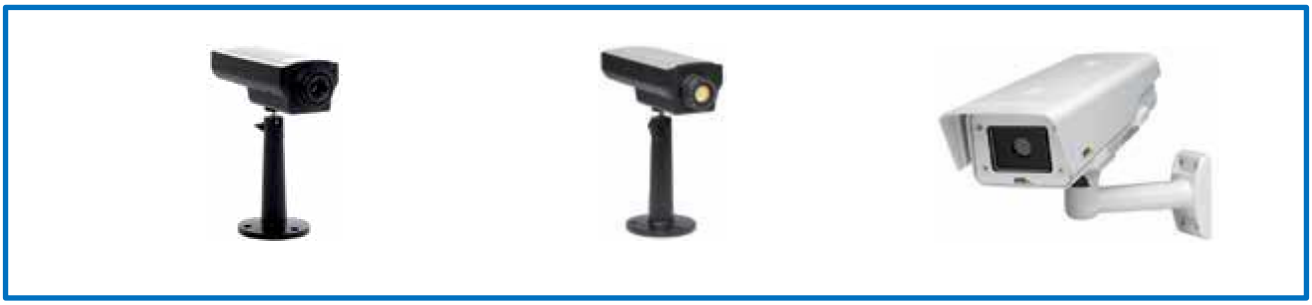

Figure 20. Samples of thermal network cameras (Axis Communications a, 31)

Thermal network cameras are very useful for detecting people, objects, and events in environment of low or zero vision level, like shadows, total darkness, smoke, etc... Since thermal cameras are mainly used to detect suspicious actions, they usually do not provide reliable identification; therefore a thermal network camera is used along with conventional network surveillance cameras in monitoring system (Axis Communications a, 32).

5.4.4 Guidelines for selecting a network camera

Since there are many types of network cameras, it is recommended to consider some guidelines before purchasing a network camera:

- The aim of surveillance

  For example; is it just for viewing a scene? Or details are required, is it essential to determine identities of persons? The aim of surveillance determines the field of view, the location of the camera, and the type of the lens of the camera.

- The area needed to be covered

  For the scene that needs to be covered, it is important to determine the number of locations required to be monitored, how large they are and how far or close they are from each other, knowing those things determine the type and number of network cameras needed.

(Axis Communications a, 33)

- Environment
  - Light

    Network cameras have different sensitivities for light, there are two factors that should be considered for that matter: first is the lowest f-number on the lens of the camera (the lower that number is the more light sensitive the camera is); The other thing to be considered is the lux specification (the lower, the better), the lux specification takes into account the joined performance of number of factors like the lens and image processing.

  - Protection

    It is very important when the camera is required for an outdoor location or in a location that is accessed by potential vandals, it is important to select a camera with specifications suitable for such environments.

    Also the temperatures and other weather conditions of the environment should be considered.

- Type of surveillance (Overt or covert)

  Taking that into consideration when selecting the network camera, will help in purchasing the right camera type and also help in selecting the mount and housing of the camera, whether they are non-discreet or discreet.

(Axis Communications a, 34).

- Resolution

  Detailed images (required or not).
- Compression

  Whether saving in bandwidth and storage essential or required
- Audio

  If audio is required, it should be considered whether one-way audio or two-way audio is needed.
- Management of events and Intelligent video

  Although event management is usually taken care of by software, it is enhanced by the use of input/output ports and intelligent functionalities of the camera (if any), therefore, when it is required for example to make the operation of the camera triggered by a certain event for the sake of security or none security purposes, the appropriate camera type with the appropriate features should be selected.
- Open interface and software

  If there is a need to integrate the camera with other systems, a camera with an open interface should be considered. Also it is important that the camera be supported by application and management software that enable easy installation and upgrades of network video devices.

(Axis Communications a, 35).

Beside the selection of the right network camera, it is important to select the right vendor, also when it is required to purchase number of cameras; it is a good idea to purchase one unit to test it first (Axis Communications a, 36)**.**

5.5 Video Encoders

5.5.1 An easy way to convert to network video

The invention of network video caused a dramatic change in the field of surveillance in many aspects. Although there are advantages of IP-based surveillance systems, which include high improvement of image quality and management of events, but that does not mean that all Closed-Circuit TV (CCTV) surveillance systems are not practically usable. There is more than one option here; it is not either IP system or CCTV system. There is a solution that combines the two together so that to keep the existing old system and to have the advantages of the new one at the same time (Axis Communications b, 3).

A shift in technology

The video encoder is the element that lumps the IP system and the CCTV system in one entity. A compression chip and an operating system are contained in a video encoder; the operating system is responsible of converting analog signals to digital signals. A video encoder is shown in figure 21 (Axis Communications b, 3).

There are tens of millions of analog cameras in the world; many of them has an average lifetime of about six to eight years, so some of them can be operated for years, also it is important to consider the cost of the installation of coaxial cables needed for the CCTV system. In the case of a building that do not have existing network infrastructure; the use of network video may not be considered as an economical choice (Axis Communications b, 3).

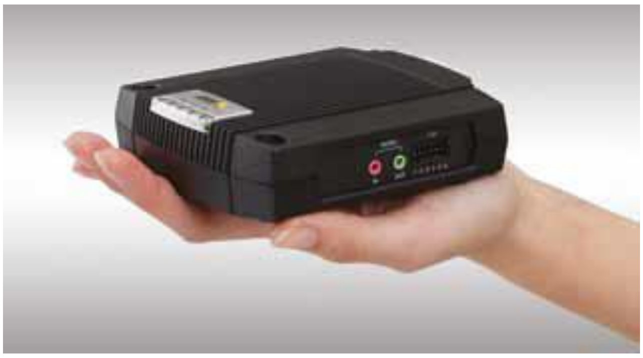

Figure 21. AXIS Q7401 Video Encoder (Axis Communications b, 3)

When the DVR (Digital Video Recorder) replaced thee VCR (Video Cassette Recorder), some advantages were achieved:

- No need to replace tapes.
- More consistent image quality.
- Less work needed to find exact video sequences.

(Axis Communications b, 3).

Although DVRs developed over the years, but still there were not able to provide the benefits that can be gained from network video systems, for instance; when a DVR is used, integration with fast developing software is not easy, because video is still stored in proprietary equipment (Axis Communications b, 3).

Important and advanced functions

By using a video encoder, a user of a CCTV surveillance system can view images from any computer connected to the network, because the video encoder receives the analog signals from the analog camera, it converts and compresses them into a video stream similar to that taken from a network IP camera (Axis Communications b, 4). The video encoder has other functionalities that can be utilized:

- The detection of distributed video motion.
- Alarm for tempering.
- The management of events.
- Integration of audio.
- The provision of the base for other intelligent functions, such as the recognition of number plates.

PTZ (pan/tilt/zoom) control is provided by many video encoders, enabling the control of analog cameras by a computer.

Another important feature can be added to the list of the benefits of using video encoders and that is that the video encoder may support Power over Ethernet (PoE), meaning that the power to the camera is fed via the same cable used for data transmission, therefore savings are achieved in cables (Axis Communications b, 4).

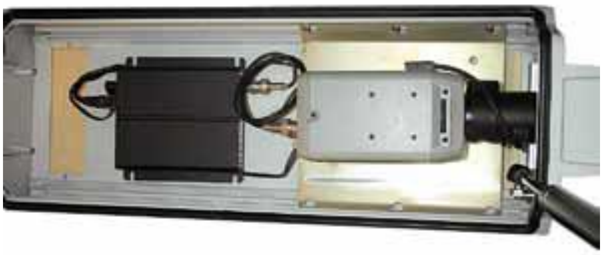

Figure 22. A one – channel video encoder connected to an analog camera (Axis Communications b, 4)

One of the features of video encoders is the ability to provide fine-tuning and aspect ratio correction which ensures undistorted images when using a computer screen. Another advantage of using a video encoder is that regardless of the distance where the analog camera is located, it is possible to retain the quality of images captured, because those images are travelling as digital images.

In case there are few analog cameras located in a remote location, the type of the video encoder typically used is the most common type which is called the **standalone** version; it has single or multi-channel connections to be used to connect analog cameras, a standalone video encoder is usually put close to the analog camera(s) (Axis Communications b, 4).

Scalability and flexibility

When suing network video, it is easy to add new cameras to the system, this makes things easy for installation and / or expansion, thus scalability is one of the advantages of using a video encoder. For a CCTV system using video encoders, the operator has the opportunity to choose to buy elements from different vendors since recording and management is based on computer standards (hardware and software), therefore making the task of upgrading and / or maintenance an easy one.

The use of standards gives the video systems using video encoders the ability to be integrated with other systems like IP – based building management systems, and that adds to the advantage of converting an analog video system to IP-based video system by the use of video encoders (Axis Communications b, 4).

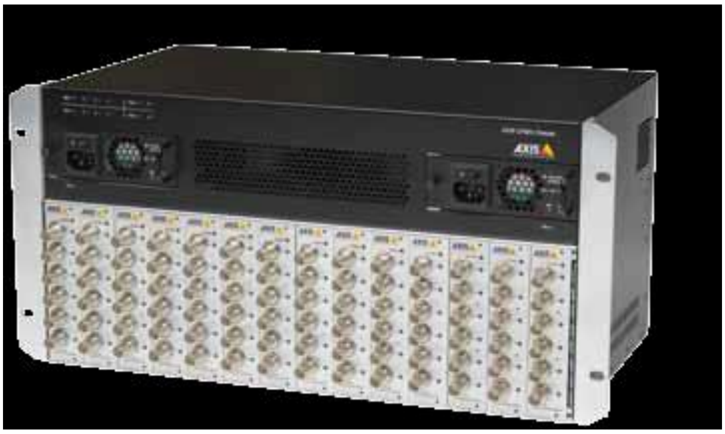

Figure 23. A chassis of a video encoder capable of supporting 84 analog channels (Axis Communications b, 5)

Security and storage

When it comes to the migration from an analog surveillance system to an IP-based one, video encoders are considered an excellent solution, especially when they are, for instance, used in an enterprise where large number of analog cameras is involved, security personnel in the enterprise can then be able to utilize the useful features that the network video offers and still benefit from elements of the analog system that was in use.

When using video encoders; edge storage becomes available, this gives products in the network video system, such as video encoders, the ability to use SD (Secure Digital) memory card for storing information locally, one of the advantage of that is the ability to retrieve parts of the recordings that was not recorded in the central recording system due to power failure for example (Axis Communications b, 5).

5.5.2 Evolution of video surveillance systems

1. **Analog CCTV systems using VCR (Video Cassette Recorder**). As shown in figure 24 (Axis Communications b, 6).

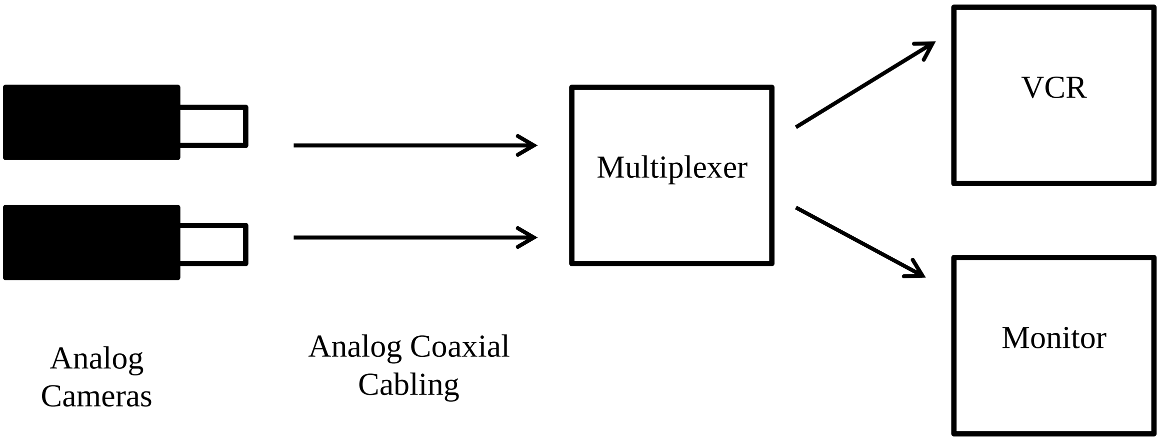

Figure 24. A classical analog video surveillance system (Axis Communications b, 6)

2. **Analog CCTV systems using DVR (Digital Video Recorder).** As shown in figure 25 (Axis Communications b, 6).

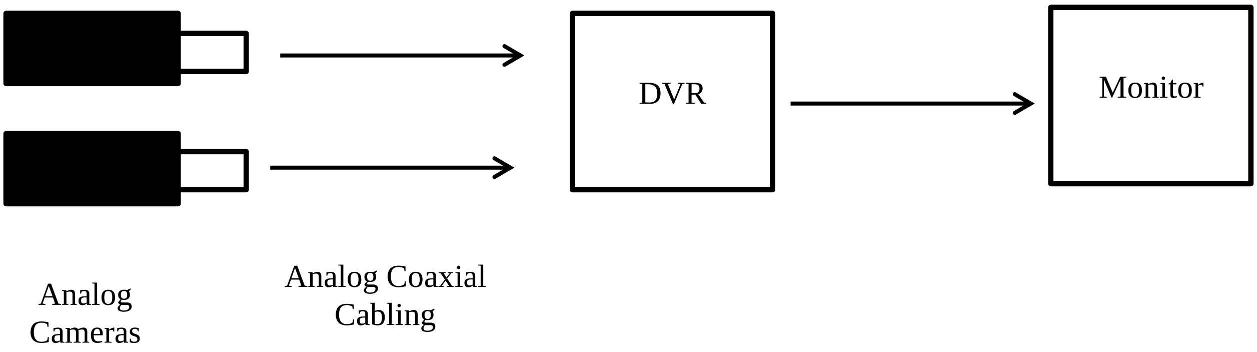

Figure 25. A surveillance system containing analog cameras and a DVR which performs multiplexing and digital recording (Axis Communications b, 6)

Main advantages of the DVR system:

- No need for tapes.
- Consistent quality of the recording.
- Ability of quick data search.

(Axis Communications b, 6).

3. **Analog CCTV systems using network DVR.** As shown in figure 26 (Axis Communications b, 6).

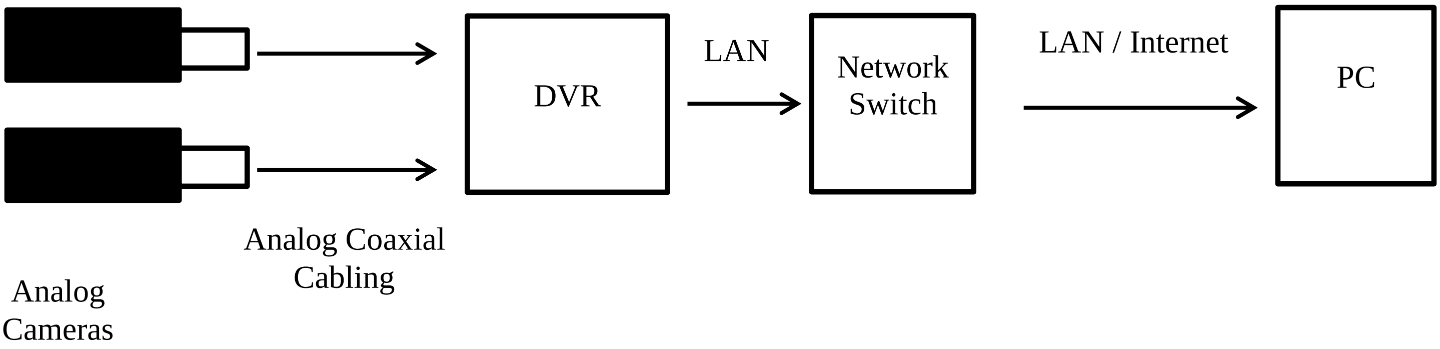

Figure 26. Networked analog cameras using a network DVR remote monitoring and digital video recording (Axis Communications b, 6)

Advantages of the network DVR system:

- *Ability to monitor video remotely by using a PC*
- *Ability to operate the system remotely*

(Axis Communications b, 6).

4. **Network video systems using video encoders.** As shown in figure 27 (Axis Communications b, 7).

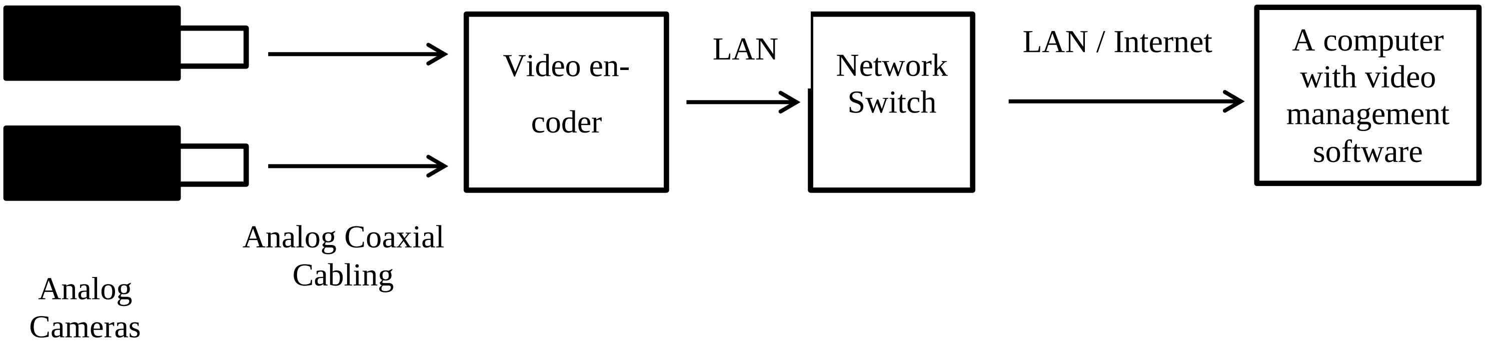

Figure 27. Network video system using a video encoder (Axis Communications b, 7)

Advantages of network video system using a video encoder:

- *Ability to use network and PC server hardware*
- *Scalability of one camera at a time*
- *Off-site recording possibility*
- *Intelligence distribution possibilities*
- *Ability of easy integration with other systems*
- *Capability to use PoE*
- *Ability of future expansion*

(Axis Communications b, 7)

5. **Network video systems using network cameras and coaxial cables.** As shown in figure 28 (Axis Communications b, 7).

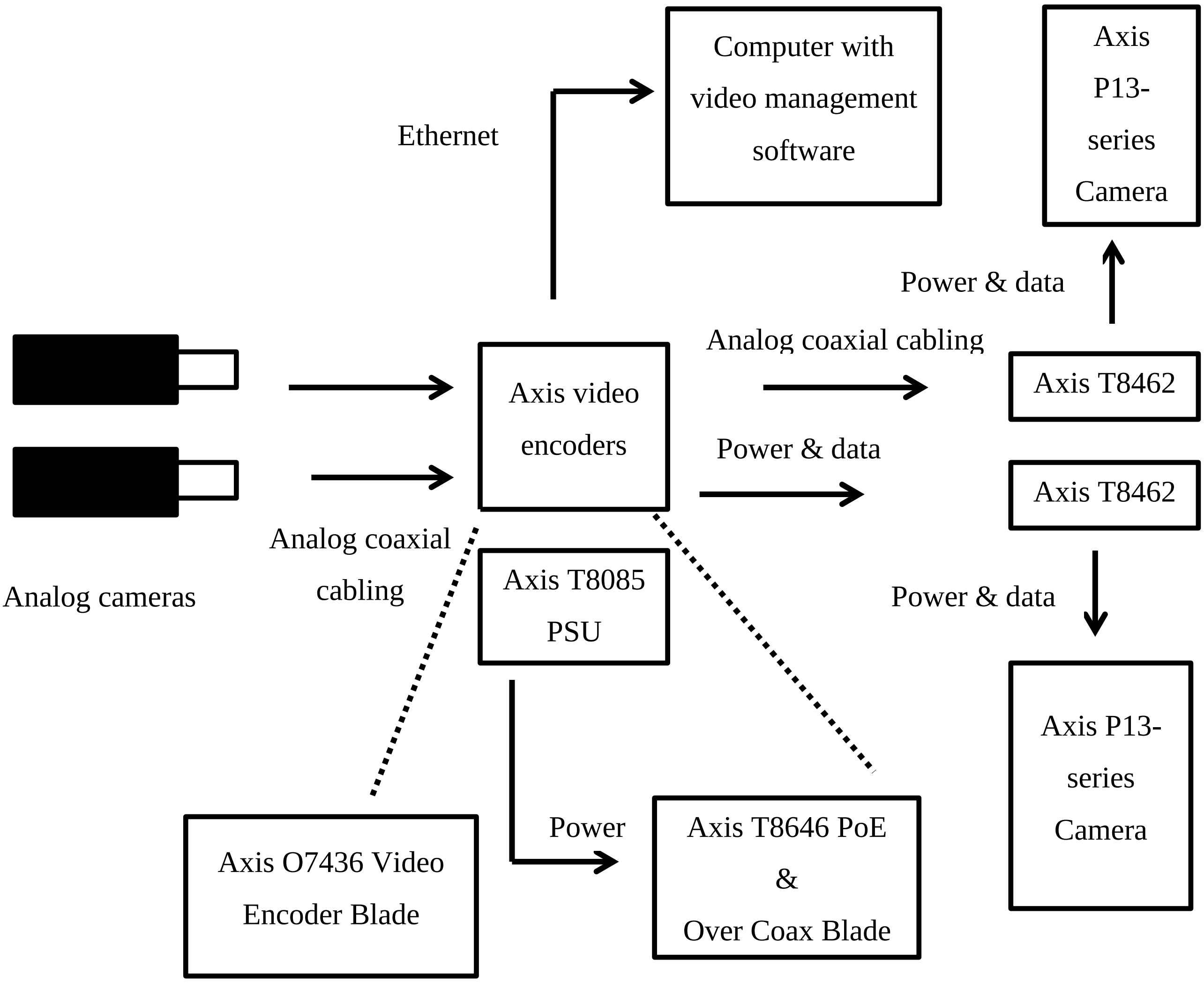

Figure 28. A network video system using network cameras and coaxial cables (Axis Communications b, 7)

Advantages of network video system using network cameras and coaxial cabling:

- Re-cabling is not needed
- Ability to carry PoE and PoE+ by the coaxial cable
- Ability to use existing video encoder chassis
- Easy installation
- Configuration is reliable and migration is seamless

(Axis Communications b, 8).

6. **Network video systems using network cameras.** As shown in figure 29 (Axis Communications b, 8).

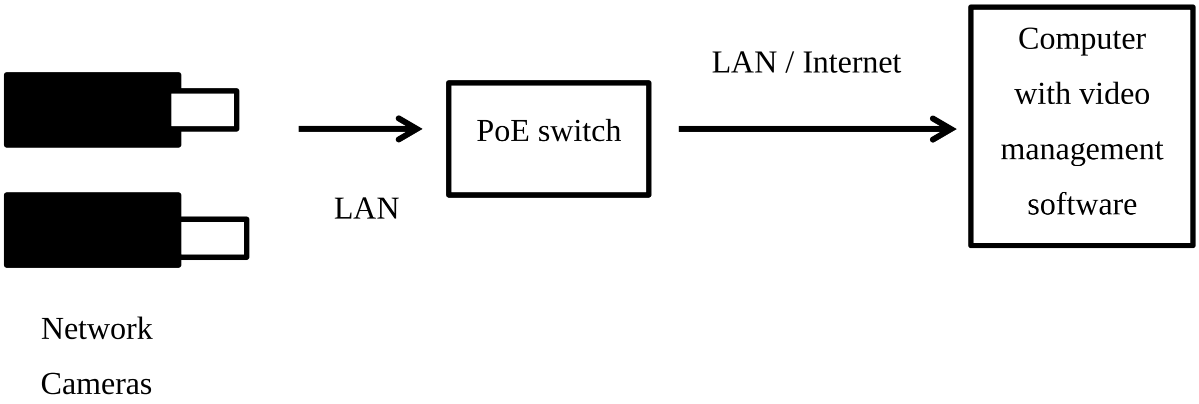

Figure 29. A network video system using network cameras (Axis Communications b, 8)

Advantages of network video system using network cameras:

- *The ability to use high resolution.*
- *The image quality is consistent.*
- *Ability to use PoE.*
- *Ability to utilize functionalities such as zoom and audio with video.*
- *Using IP for settings of cameras and adjustment of the system.*
- *Flexibility and scalability.*

(Axis Communications b, 8).

6 A HYPOTHETICAL CASE

In this part, a case of a hypothetical firm will be presented, calculations related to energy, cost, and time will be made and security matters will be tackled.

6.1 Description

The hypothetical firm is an engineering firm; it is in a single floor building, a diagram of the offices in the firm is shown in figure 30, the firm consists of the following departments:

- Management
- Legal
- Contracts
- Human Resources (HR)
- Finance
- IT
- Inventory
- Engineering
- Security
- General Services

Each of those offices is used by staff (at least one), in each one; there are the following IT items:

- ❖ Computer
- ❖ USP , 1000 Volt Ampere (1kVA)
- ❖ Printer
- ❖ Scanner

Due to security reasons, a CCTV system was installed in the office, there are around 10 analog cameras installed and distributed inside and outside the building.

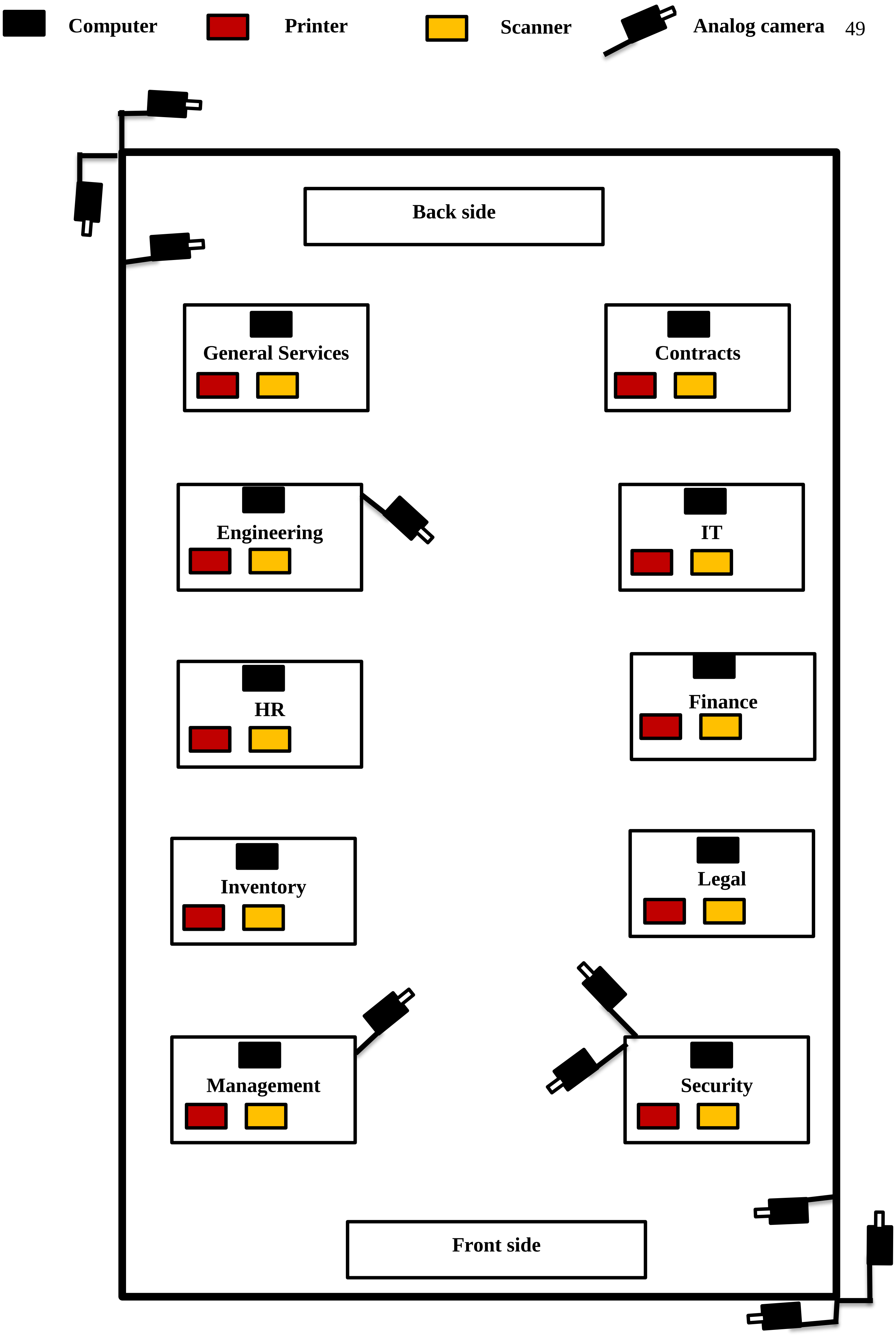

Figure 30. Diagram of the engineering firm

6.2 Problems and analysis

6.2.1 Energy

It was noticed by one of the staff (an electrical engineer) that electrical power bills are relatively high. He thought that there are opportunities of energy savings.

Table 1. below shows the number of IT items along with estimations of costs and power consuption of IT items and analog security cameras.

Table 1. Cost and estimated power consumptions of IT devices and security cameras

Item	**Estimated cost (€)**	**Estimated rated power (Watt)**	**Number of items**	**Tottal estimated cost (€)**	**Total estimated rated power (Watt)**
Computer	500	50	10	5000	500
Printer	50	1000	10	500	10000
Scaner	30	100	10	300	1000
Analog cameras (outside)		6	4		24
Analog cameras (inside)		6	6		36

Assuming that the devices are operated 2 hours a day, 5 days a week; the number of operating hours per year is approximately 2 hours x 5 days x 4 weeks x 12 months, and that is equal to **480 hours** per year.

Assuming that the 4 security cameras outside the office are operated 24 hours a day during the whole year; the number of operating hours per year is approximately 24 hours x365 day, and that is equal to **8760 hours** per year.

Assuming that the 6 security cameras inside the office are operated 10 hours a day during the whole year; the number of operating hours per year is approximately 10 hours x 365 day, and that is equal to **3650 hours** per year.

Table 2 shows the estimated approximate energy needed per year for each type of IT devices and the security cameras.

Approximate annual energy needed in kWh (kilo Watt hour) for computers is 500 Watt x 480 hour, which is equal to **240 kWh.**

Approximate annual energy in kWh needed for printers is 10000 Watt x 480 hour, which is equal to **4800 kWh.**

Approximate annual energy in kWh needed for scanners is 1000 Watt x 480 hour, which is equal to **480 kWh**.

Approximate annual energy in kWh needed for analog cameras located outside the building is 24 Watt x 8760 hour, which is equal to **210 kWh.**

Approximate annual energy in kWh needed for analog cameras located inside the building is 36 Watt x 3650 hour, which is equal to **130 kWh.**

Table 2. Approximate estimated annual power consumptions of IT devices and security cameras

Items	**Total estimated energy required in kilo Watt hour (kWh) per year**
Computers	2400
Printers	4800
Scaners	480
Analog cameras (outside)	210
Analog cameras (inside)	130

6.2.2 Time

During busy days, when almost all the staff had to work even during weekends, the manger needed several times to hold sudden short important meetings with key personnel, he noted that it takes about 10 minutes for the staff just to gather in his office and to get back to their offices, and after that it takes about 5 minutes for each of them to resume what he / she was doing before attending the meeting.

The manager still wanted to conduct such meetings but he was hoping that he can do that without having to bring the staff all the way to his office for each meeting.

Also, the manager noted that there were considerable delays in the process of sharing documents and information between staff.

6.2.3 Cost

One of the IT staff realized that the number of IT items bought annually is more than needed; some of them are rarely used, like the UPS and the printer in the General Service department.

6.2.4 Security

Some security related matters were reported recently to management by security staff; they were related to the CCTV system, for example: failing to have a clear image of a suspicious person who was noticed one day outside the firm building.
Also the manger felt that it is important to have the ability of viewing the images of the security cameras while he is not in the office, like when he is home or abroad.

Related to another matter; the Security department noticed on several occasions that some hard copies of some of the confidential documents were distributed and seen by people who should not have access to such documents.
So, a decision was made to enhance the system of security cameras installed and to find a solution to reduce or minimize the risk of confidential documents being seen by unauthorized personnel.

6.3 Solutions

All those 4 problems can be solved technically; the answers are in the use of LAN (local area network) and network video. Network video can be implemented by replacing the existing analog cameras of the CCTV system by IP cameras; or by converting the existing analog cameras to IP cameras by the use of video encoders.
The solutions that can be implemented by the use of a LAN and network video can be put as the following:

6.3.1 Energy

The solution to the energy problem by using a LAN and network video comes through the utilizing of **sharing** and **power over Ethernet** (PoE).

- By using IP cameras instead of analog cameras or by converting the existing analog cameras to IP cameras by using video encoders; PoE can be utilized; hence reducing energy requirements for the operation of cameras by about 50%. The annual estimated energy required for security cameras as shown in table 2 above is (210+130) kWh, which equals to **340 kWh**, so if power supplied to the cameras is reduced by 50%, the energy savings will be 340x50/100 kWh, which equals to **170 kWh** per year. And that is around 0.4 kWh per day, an amount of energy enough to operate a 400 Watt water boiler for one hour a day for a year.
- By using a LAN, some resources can be shared, which leads to reduction in energy needs, and as illustrated below:
  1. Sharing documents via the LAN between departments will reduce the need to print hard copies, this could mean around a 50% reduction, the annual estimated energy required for printing as shown in table 2 is 4800 kWh, so if printing jobs are reduced by 50%, the energy savings will be 4800x50/100 kWh, which equals to **2400 kWh** per year. And that is around 6.5 kWh per day, an amount of energy enough to operate a 1000 Watt heater 6.5 hours a day for a year.
  2. Sharing documents via the LAN between departments will reduce the need to scan documents as the document are needed to be scanned only one time then shared between the related departments, this may lead to the reduction of scanning jobs by about 90%; the annual estimated energy required for scanning as shown in table 2 above is 480 kWh, so if scanning jobs are reduced by 90%, the energy savings will be 480x90/100 kWh, which is approximately equal to **430 kWh** per year. And that is around 1 kWh per day, an amount of energy enough to operate a 100 Watt bulb for ten hours a day for a year.

Figure 31 illustrates the use of network video and the new distribution of scanners and printers in the firm assuming the use of a local area network (LAN) and network video.

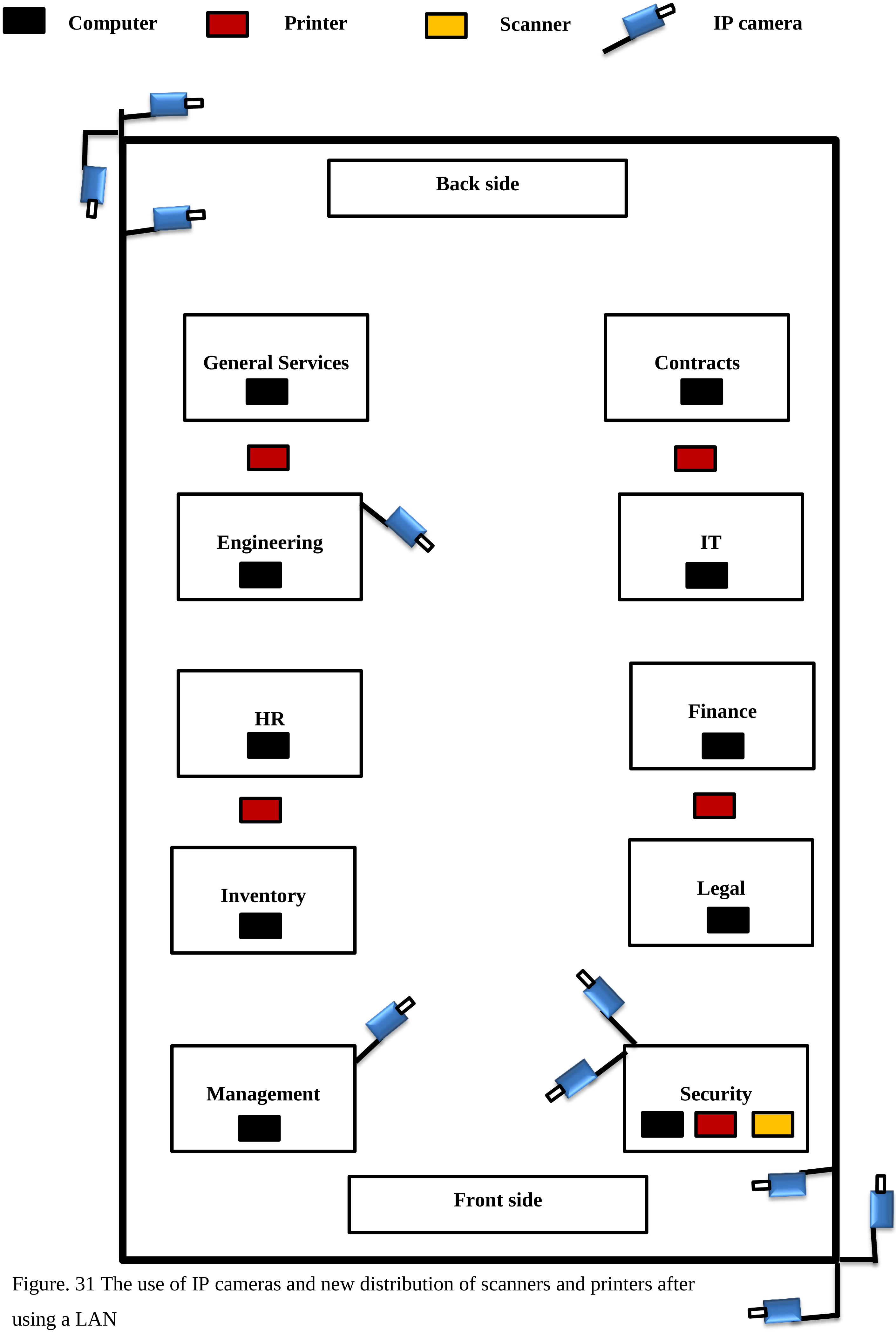

Figure. 31 The use of IP cameras and new distribution of scanners and printers after using a LAN

6.3.2 Time

By utilizing some of the benefits of LAN and network video; management found solutions to some of time related problems or inconveniences, and that is as follows

- By using instant messaging and video conferencing, the manager can notify and hold meetings with related staff. So when no physical meetings are needed, the time spent for notification for the meetings and for staff to come and return to and from the manager office is spared and that can be a lot of time per year. Assuming that there is a need for a meeting (when no physical attendance is needed) twice per week, which means about 8 times a month or around 100 times a year. If the average time needed for one meeting for the staff to be notified and be gathered in management office and then go back to their offices, if that time is 15 minutes, then that time needed for 100 meetings is <u>15 minutes/60 x 100</u>, and that is equal to **25 hours** per year, and that is equal to the time of 3 working days (assuming an 8 hours working day).
- By using the benefit of sharing of documents between staff via the LAN; considerable amount of time can be spared. Assuming that the time needed for staff to physically (by hand) share documents is 10 minutes per day, then it is around 50 minutes per week (assuming 5 working days a week), and it is around <u>50 minutes/60 x 4 weeks x 12 months</u> per year, which is equal to **40 hours** per year, and that is equal to the time of 5 working days (assuming an 8 hours working day).

6.3.3 Cost

By utilizing some of the benefits of LAN and network video; the ratio of the income profit to the outgoing expenses can get higher, this can be achieved by the following:

- Because of sharing some of the IT resources (like printers), the cost for purchase and maintenance of some of IT items will go down, as shown in table 1, the purchase cost of printers is **€500** and the purchase cost of scanners is **€300,** this amount can be reduced to **€280** when reducing the number printers by 50% and reducing the number of scanners by 90%, like shown in figure 31, such reductions can be made due to the use of sharing via LAN.

- Due to the use of sharing documents via the LAN, energy needed for some of the IT items will be reduced, as shown above in 6.3.1, energy needed for the operation of security cameras will be less when using the PoE option, as illustarated above in 6.3.1, the energy savings due to the use of PoE is around **170 kWh** per year, if the price of one kWh is **€0.15,** the annual cost savings from energy savings are equal to **€25.5**. Also, the energy savings per year due to sharing some IT resources is around <u>2400 kWh + 430 kWh</u>, which is equal to **2830 kWh** per year, if the price of one kWh is **€0.15**; the annual cost savings from energy savingings are equal to **€424.5**. Hence the energy bill will be less than that before the use of LAN and before converting to IP cameras by around **€450** per year. It is worth mentionong that there will be some expenses for the installtions and purchases of items related to LAN and IP cameras or the convertion to IP cameras process.

- Sparing time by using some of the benifits of LAN (as illustrated above in 6.3.2) can lead to more production which normally translated to more income.

- Because of less printing and less sharing of hard copies, the use of papper and ink will be reduced; therefore less money is needed for that.

6.3.4 Security

- By the use of IP cameras, it is possible to obtain clear images of faces of people; also it is easier to navigate for certain event or time.
- By utilizing the sharing of documents between staff via LAN, and hence the reduction of printing hard copies and of physical transfer of documents; the chances of unauthorized persons having access to some information are reduced.

6.4 Conclusions

The installation of a local area network and the use of network video can provide solutions to some of the problems related to energy, time, cost, and security.
Although the above savings may not seem significant, but it is believed that the savings would be much higher if they are made, for instance, for buildings containing more than 100 offices.

7 IMPLEMENTATION OF A WIRELESS LOCAL AREA NETWORK

7.1 Description

The implemented wireless local area network (WLAN) consisted of the following components:

- A laptop computer
- A desktop computer
- A printer
- A router

7.2 Procedure

- A HomeGroup was made in the laptop computer.
- The router was connected by an Ethernet cable to the laptop computer and was configured to work as a wireless access point.
- The laptop computer and the desktop computer were connected to the router via Wi-Fi connection.
- The HomeGroup was joined from the desktop computer.
- A printer was connected by a USB cable to the laptop computer, the wireless LAN is shown in figure 32.

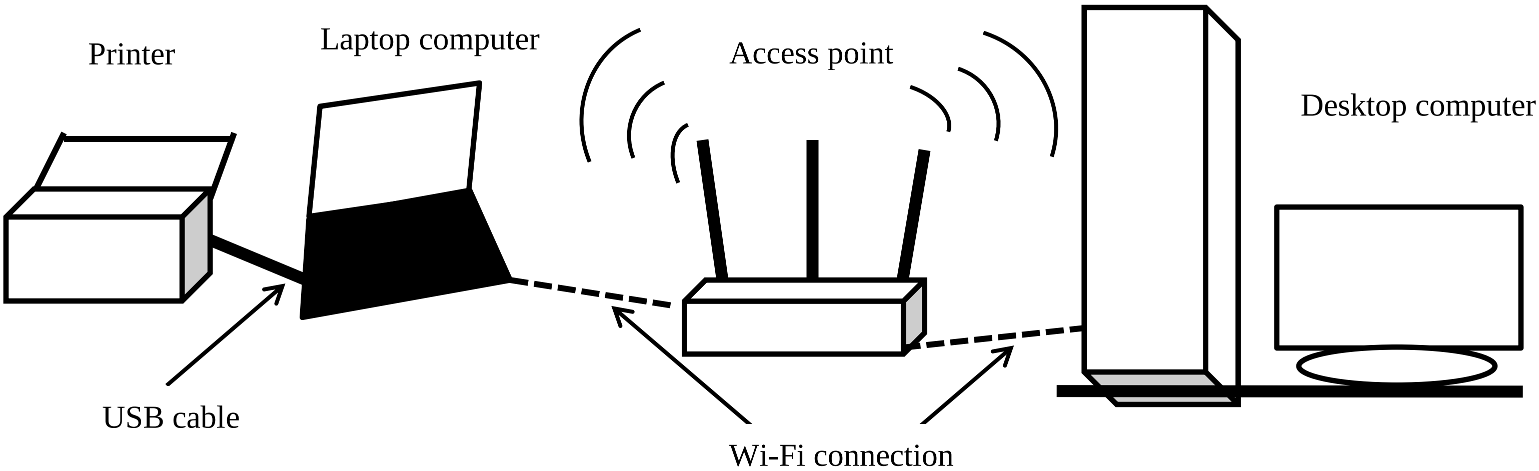

Figure. 32 A Wireless Local Area Network (WLAN).

7.3 Results

Files and resources were shared.

- Files were shared between the laptop computer and the desktop computer.
- A picture was printed from the desktop computer via the printer which was connected by a USB cable to the laptop computer.

8 IMPLEMENTATION OF A NETWORK VIDEO

8.1 Description

The implemented network video system consisted of the following components:

- A laptop computer
- An IP wireless camera
- Router1 (already configured to work as an access point)
- Router2

8.2 Procedure

- Using an Ethernet cable, The IP camera was connected (from one of the LAN ports) to Router1 (which was already configured to work as an access point).
- The laptop computer was connected wirelessly to the access point.
- The software of the IP camera was set up in the laptop computer and the IP given to the IP camera was known and a video feed from the IP camera was obtained. The LAN which was established was as shown in figure 33.

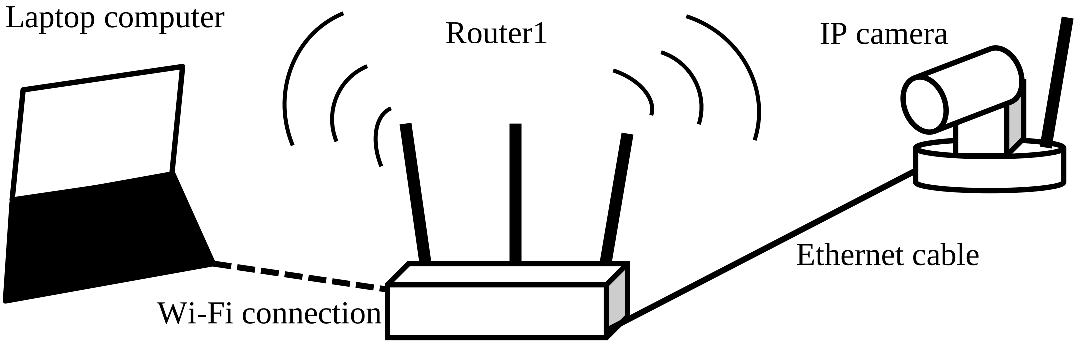

Figure. 33 Network video using local area network (LAN)

- Using the tools provided by the IP camera software, the monitoring page of the camera was entered and a number of setting options (like WLAN settings) and controls (like moving the camera up and down) were available to apply on the camera.

- A video feed was available from the camera.
- The IP camera was connected via an Ethernet cable to Router2 (from one of the LAN ports) and the monitoring page was entered. Although Router 2 was connected to the Internet, but that has importance or no role in the procedure.
- Using the WLAN settings, the camera was configured to be connected wirelessly to Router1.
- The connections which were established were as shown in figure 34.

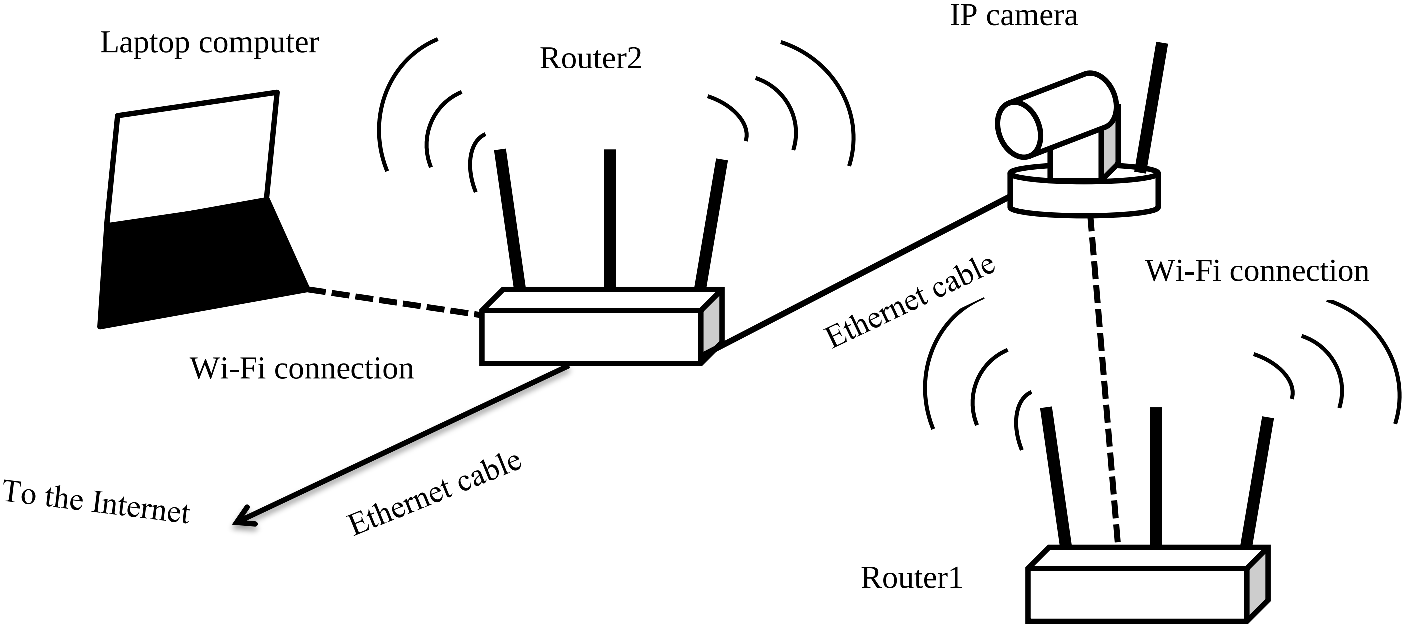

Figure. 34 Configuring the wireless connection of the wireless IP camera

8.3 Results

- A network video system was established using a wireless LAN.
- A video feed was obtained wirelessly from the wireless IP camera.
- The WLAN which was established was as shown in figure 35.

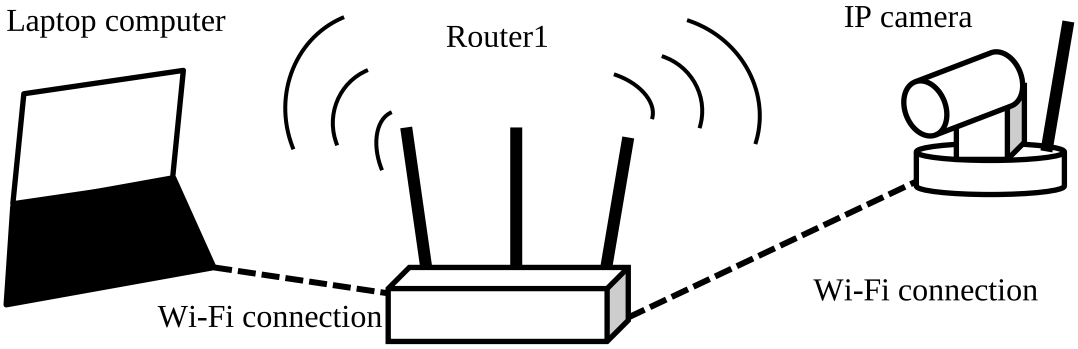

Figure. 35 A network video using a wireless local area network (WLAN)

9 SHOWING DIFFERENCE IN IMAGE QUALITY BETWEEN AN ANALOG CAMERA AND AN IP CAMERA.

9.1 Using an IP camera and an analog camera

Below are two images of almost the same scene, one taken by an IP wireless camera and the other is by an analog camera, the analog camera was connected by wire to a TV set and a video feed was established, then a photo of the TV screen was taken, this photo is shown in figure 36.

After connecting the IP wireless camera to a wireless local area network, a video feed was established, and then a snapshot was taken by the IP camera, this snapshot is shown in figure 37.

It is noticeable that there isn't much difference in the quality of the two images, however, a subjective comparison can be made when using two cameras of the same characteristics (including being both wired) except for one being IP and the other being analog.

Figure 38 shows the two cameras used for taken the images shown in figures 36 and 37.

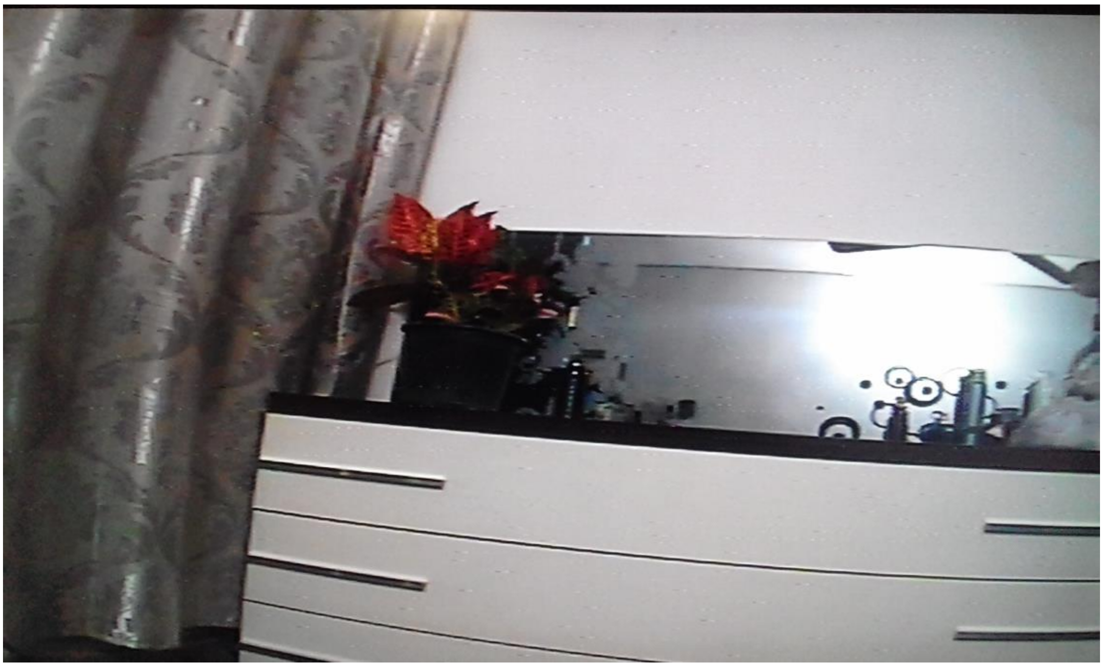

Figure 36. Picture of the screen of the TV to which the analog camera was connected

Figure 37. Snapshot taken by the IP wireless camera connected to a wireless LAN

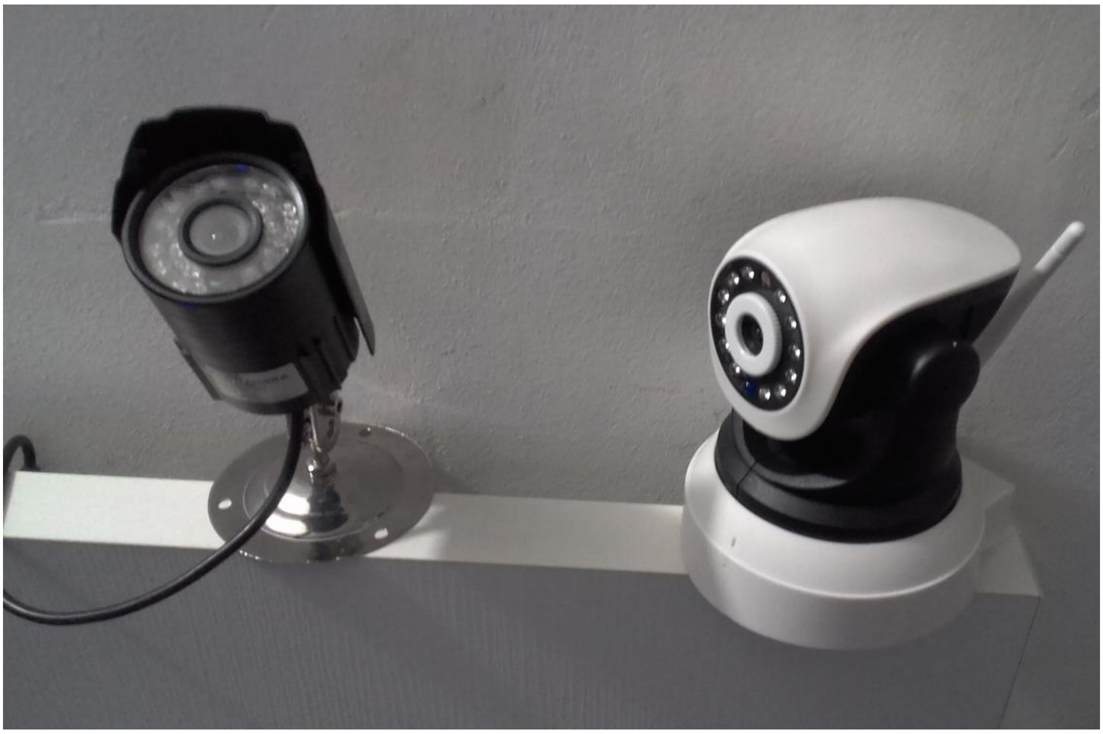

Figure 38. Analog camera and wireless IP camera used.

9.2 Picture quality

The best advantage of IP cameras compared to digital cameras is probably the quality of the picture obtained.

For delivering an image with 1,000,000 or more pixels, megapixel resolution utilizes a megapixel sensor; more details are captured with more megapixels, hence; an image of better quality is obtained.

The most commonly used resolution in analog cameras is 4CIF (common intermediate format) , it has a resolution of 704x576 pixels (0.4 megapixels), while a format of a low megapixel 1280x1024 pixels provides more than 3 times the resolution that a good analog system can provide. There are IP cameras that can already go to 8 megapixels.

In an IP network video system the recorded video has the same image quality of the live video and that is because of the way the video is transmitted and stored in the NVR (network video recorder).

Because the transmission of data is in a digital format, IP network video is less vulnerable to picture interference compared to analog CCTV systems.
Coaxial or twisted pair of copper cables is used in analog CCTV systems for transmission of video signals; the video signal of analog cameras can be badly affected if, for example, those cables are close to cables carrying electrical current for supplying electrical power.

Figure 39 shows differences in picture quality between analog camera / 4CIF and IP cameras with different megapixels (website of TRINITY cctv solutions 2017).

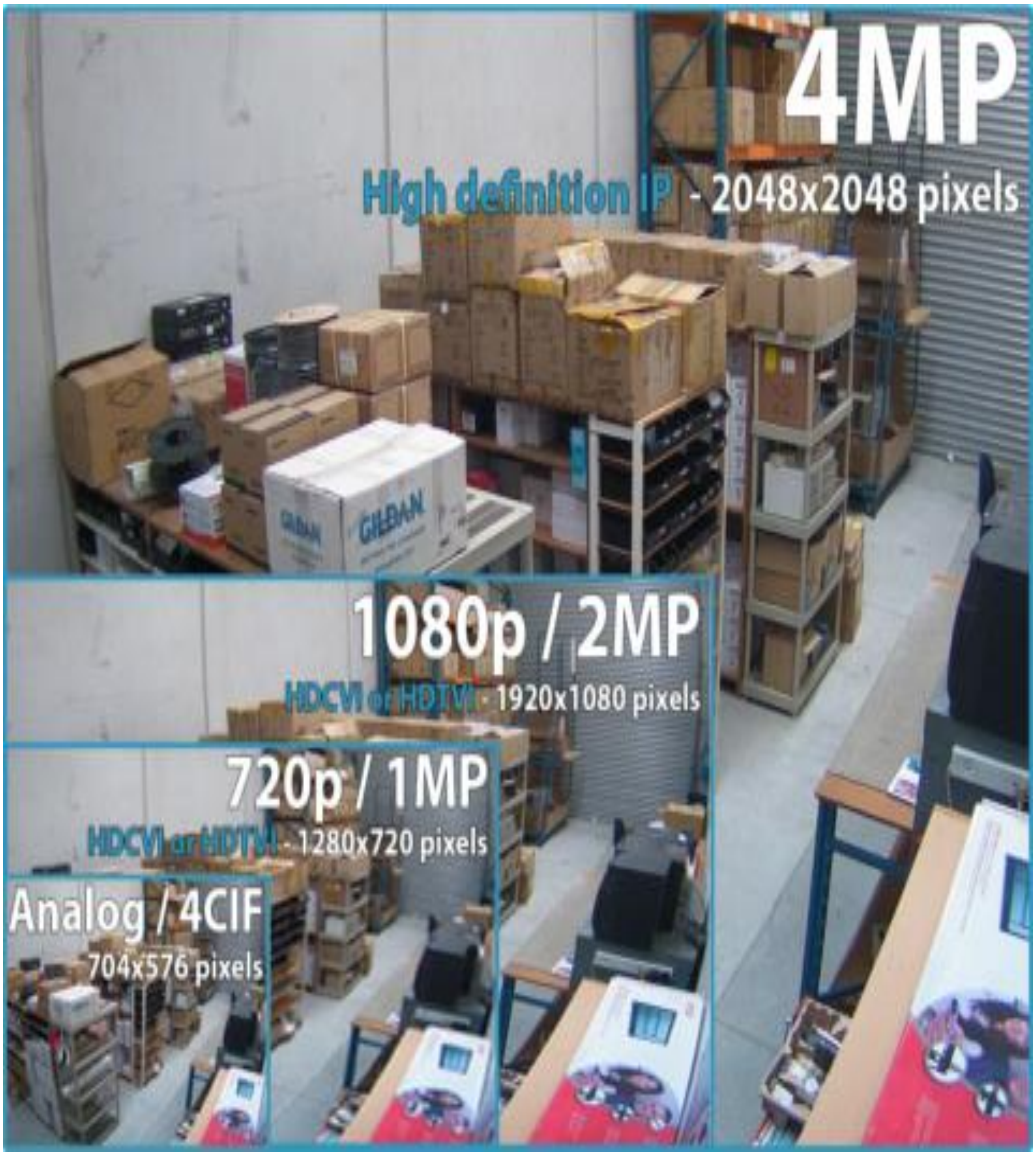
4MP
High definition IP - 2048x2048 pixels
1080p / 2MP
HDCVI or HDTVI - 1920x1080 pixels
720p / 1MP
HDCVI or HDTVI - 1280x720 pixels
Analog / 4CIF
704x576 pixels

Figure 39. Difference in image quality between analog and IP cameras (website of TRINITY cctv solutions 2017)

The follwing differnces in the pictures can be noticed:

- The IP images are bigger than in the case of analog image.
- The level of details captured are higher than in the case of analog image.
- More clarity provided by IP camera.

(Website of TRINITY cctv solutions 2017).

Why an HD (high definition) image is important?

In real life, there are many ocasions when HD images are needed, the following hypothetical situation can be considered as an example:

A compay that has a warehouse in which different kinds of products are stored, one day; the manegment was notified that there was a certain parcel of products, this parcel was picked up from the warehouse by one of the company staff and to be delovered to a client, but the parcel did not reach its destination, now it is required by managemt to know the warehouse staff who delivered the parcel and the peson who picked it up from the warehouse.

After finding the point in time at which the parcel was taken, an image can be obtained from the recorded video and an attempt is to be carried out to know the people involved regarding the parcel taken from the warehouse.

Now there are two scenarios and they are sismilar to what is shown in figures 40 and 41 respectively , the **first one** is that the image is captured using an anlog CCTV camera with high resolusion and the recording of the video feed is done to 4CIF DVR (digital video recorder), the **second scenario** is that the image is captured using a 3 MP (megapixel) IP camera which records to an NVR (network video recorder).

It is clear that the faces of the staff involved can not be distingushed in the first scenario while it is possible to do that in the second scenario.

It is also clear that the image of the IP camera is much larger even at pixel diemnsions, and when this size is enlarged to an A4 paper size; it retianed its clarity and details. Which was not the case of the image of the analog camera.

It worths mentioning here that an NVR (network video recorder) provides much better search and playback service than a digital video recorder (DVR). For the parcel example, the user can search for the image in the history by just drawing a box around the parcel and the NVR will search out all the files of the movement of that parcel. While in the case of a DVR, the user can search for movement on the analog camear but without the abilty to search for a certain area on the screen (website of TRINITY cctv solutions 2017).

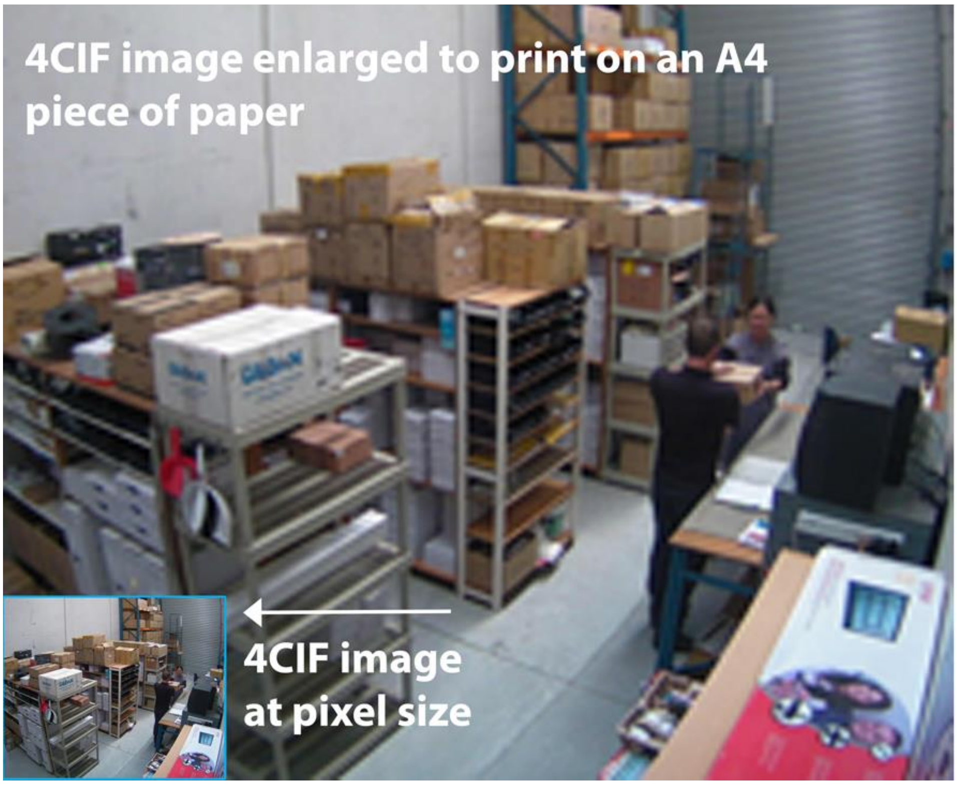

Figure 40. Image captured by an analog camera (website of TRINITY cctv solutions 2017)

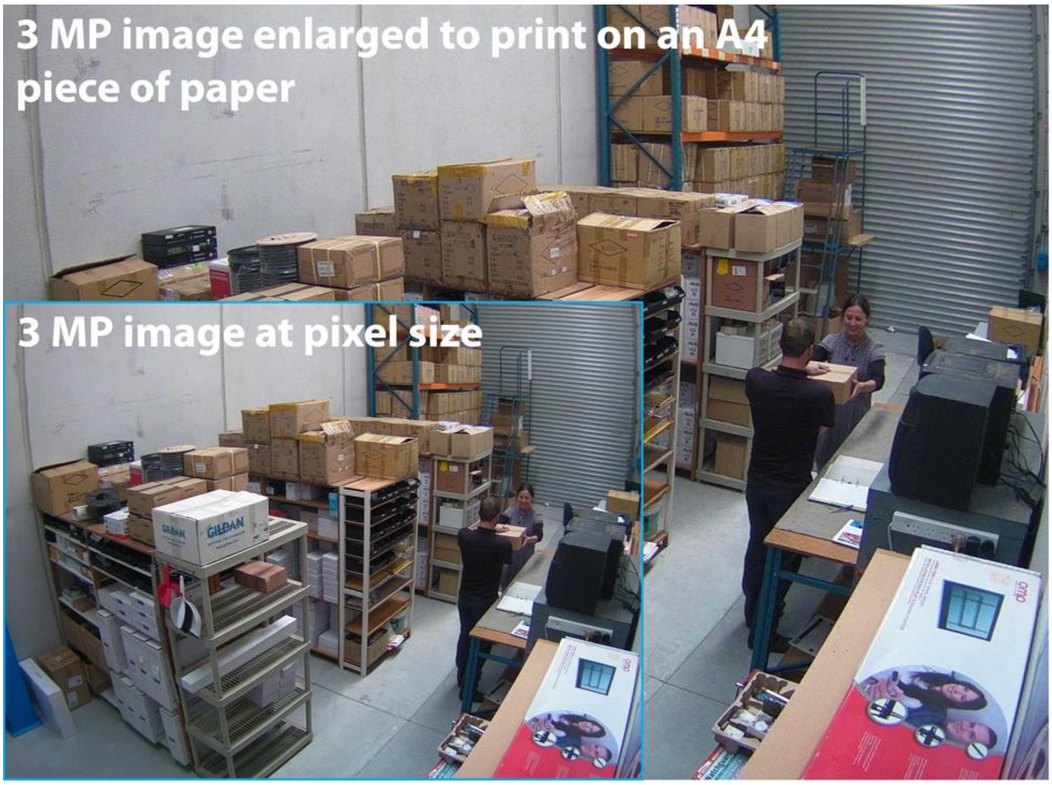

Figure 41. Image captured by an IP camera (website of TRINITY cctv solutions 2017)

Network video using IP cameras tend to be more expensive than analog CCTV systems, but the user should make a decision whether or not the use of a less expensive system will be efficient for the purposes required (website of TRINITY cctv solutions 2017).

10 ACCESSING A WLAN FROM THE INTERNET

Some people have home networks which they want to have access to remotley, like having access to important information stored in personal computers at home.

A home networks can be easily given memorable and easy to use address by the use of dynamic DNS (Domain Name System).

DDNS (Dynamic Domain Name System) makes the Internet user friendly.

An IP address is the resource's network address on the Internet of every Internet-acceessable resource, the IP address is in the format 123.123.123.123.

The human friendly request of , for example, a web site like Google.com is resolved by a DNS server into a machine friendly address (website of How- to Geek 2016).

10.1 WAN and LAN

Wide Area Network (WAN) is the IP address provided by the ISP (Internet service provider) to the Local Area Network (LAN).

The address provided to the LAN by the ISP is unique on the Internet at any given time.

A LAN can be a home network; this network may include several devices like: a Router, computers, smart phones, and printers. The device that the WAN IP address is assigned to is the Router that's why all routers have a WAN port, so that the WAN address is taken from that port.

In most cases, for home and office networks, the IP address given to the Router is not used by a compute (website of c|net 2015).

The IP version Ipv4 is practically the version that is used (and expected to be used in the foreseeable future) by all consumer-level Internet services and application.

The IP version Ipv6 is also available though.

An IP address must be provided for each device so that it can be connected to the router and then to the Internet. The router gives such IP address to each of the connected devices in a LAN, and it is called the LAN address.

For home and office networks, the WAN IP is kept by the router and the Internet connection is provided to connected devices within the LAN.

A single WAN IP address is sufficient for a router to provide Internet connections to 254 devices or clients (website of c|net 2015).

10.2 Dynamic Domain Network Service (DDNS).

The WAN IP address of a LAN can be obtained by going to whatismyipaddress.com using a computer within that LAN. This IP address can be used to access that LAN from the Internet remotely (for instance, from another country).

It isn’t easy to remember that WAN IP address and in most cases, that WAN IP address is subject to changes, therefore it is much better that this address be translated to something easy to recall and constant. For that DDNS is used. DynDNS.com can be used.

A domain can be obtained from a DynDNS (Dynamic Domain Network Service), like **Habib.dynu.net**, this domain is unique on the Internet once it is created.

In most or all cases, home and office routers are able to host a DDNS address.

If, for a home LAN, **Habib.dynu.net** was chosen as a DDNS address and the 8080 port of the router management feature was used; the router can be accessed from outside that home LAN when being remote from home, for example, by writing **Habib.dynu.net:8080**, the home router web interface can be accessed and the home LAN can be managed remotely. This can be done for almost all home routers (website of c|net 2015).

10.3 Port forwarding

Accessing the router remotely from outside the LAN it is connected to represents the first step when it is desired to access a particular device in that LAN.

For example, if it is required to access a service on one of the computers in the LAN, (which means accessing a service hosted by that computer), it is needed to activate that service on that computer, this means enabling the **Remote Desktop Connection** feature, then it is needed to configure the router to forward the port of that service to the computer involved. The port forwarding feature, in many routers, is also referred to as Virtual Server.

Although all Windows operating systems have the Remote Desktop client software (and can be downloaded for Macintosh), machines which are usable as a target for Remote Desktop connection are only those running certain editions of Windows (like Business).

After a restart a computer, the IP LAN address of that computer can be changed, the IP Reservation feature of the router can be used for retaining the same IP LAN address for that computer (website of c|net 2015).

11 CONCLUSIONS

Wireless local area networks and network video have many benefits and applications; among those benefits is the ability, in many cases, to save cost, time, and energy.

Although wired-based network video has advantages over wireless network video, including being more liable, and although IP video (network video) system may sometimes cost more than a conventional analog video system; the organization or the user should make a comparison between advantages and disadvantages, taking in consideration the priorities of the organization or the user, before deciding which system to use and which method of connection to implement.

Power over Ethernet (PoE) is a very important technology in the aspects of cost and energy savings, such technology can only be applied when using an IP system like a network video system.

The information gathered showed that the main advantage of using a network video system over the use of an analog video system is related to security matters.

The calculations made showed that the installation of a local area network and the use of network video can provide solutions to some of the problems related to energy, time, cost, and security.

The wireless video network implemented showed that the implementation of a wireless local area network and /or a video network for a house or a small office is neither hard nor difficult nor expensive.

References

-Geier, J. 2002. Wireless LANs. Second edition, USA: Sams publishing. Referred 8.12.2017. http://materias.fi.uba.ar/6637/material/SAMS_Wireless_Lans.pdf

-Axis Communications a. Technical Guide of Network Video. Referred 29.11.2017. https://www.axis.com/files/brochure/bc_techguide_60870_en_1411_lo.pdf.

Axis Communications b. Video encoders – brings the benefits of IP surveillance to analog systems. Referred 29.11.2017. https://www.axis.com/files/whitepaper/wp_encoders_57556_en_1404_lo.pdf.

Wikipedia. Referred 30.11.2017. https://en.wikipedia.org/wiki/IEEE_802.11.

Website of the University of Texas at Arlington. Referred 30.11.2017. https://www.uta.edu/oit/policy/ns/docs/wireless-paper-vijay.pdf.

Website of SANS Information Security Training | Cyber Certifications | Research. Referred 30.11.2017. https://www.sans.org/reading-room/whitepapers/wireless/wireless-lan-security-issues-solutions-1009.

Website of WIFI NOTES. Referred 30.11.2017. http://wifinotes.com/wlan-architecture.html.

Website of Veracity global, a. Referred 30.11.2017. http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-2.aspx.

Website of Veracity global, b. Referred 30.11.2017. http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-1.aspx.

Website of COMPUTER HELP AND TIPS. Referred 2.12.2017. http://computer-help-tips.blogspot.com/2011/04/wireless-lan-deployment-scenarios.html.

Website of Video maker. Referred 2.12.2017. https://www.videomaker.com/article/c10/14221-camera-movement-techniques-tilt-pan-zoom-pedestal-dolly-and-truck.

Website of TRINITY cctv solutions. Referred 2/12/2017 https://trinitycctv.co.nz/cctv-and-security-cameras/learn-about-cctv/how-good-is-the-picture-from-an-ip-camera/.

Website of How- to Geek. Referred 2.12.2017. https://www.howtogeek.com/66438/how-to-easily-access-your-home-network-from-anywhere-with-ddns/.

Website of c|net. Referred 2.12.2017. https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/.