ŽILVINAS RAKAUSKAS

WAREHOUSE COMPUTER NETWORK MODERNIZATION PROJECT

Bachelor’s / Master’s thesis

Double Degree programme

2021

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)	**Degree title**	**Time**
Žilvinas Rakauskas	Bachelor of Engineering	May 2021

Thesis title

Warehouse computer network modernization project

48 pages
1 page of appendices

Commissioned by

Supervisor

Matti Juutilainen

Abstract

The purpose of this thesis is to analyze a company’s current wireless network and its insufficient video surveillance system and to choose the best options to fulfill the higher requirements by greatly improving wireless network coverage, for current and new production facilities.

The main goal of this project was to detect the weak points of the current wireless network, figure out where the wireless network coverage is the weakest and why, find out what problems the security had with video surveillance, and what new planned warehouse needed to be fully prepared for work.

After further analysis, it was noted that the current network has many outdated switches and unmanaged access points that did not meet the current expectations and often caused coverage problems even from slightest disturbances; communication with warehouse management system and newer devices struggled as well. As a result, employees were not able to reach maximum efficiency which caused the company to lose revenue.

Another problem was video surveillance of the same production facilities. Security guards noted that they were not satisfied with current camera coverage in the area and the quality of footage. Since most of the network and cable system had to be modernized, it was decided to completely renew the video surveillance system.

Per request, all the new switches, access points, CCTV cameras and video recorders had to be from Ubiquiti and Dahua to ensure the best communication between devices.

The end goal of this project was a fully working wireless network, calculated to guarantee maximum area coverage, appropriate hardware chosen for this task and better video surveillance ensuring security in most vital points. Every change in device position and configuration must be clearly noted in the floor plans to be easier to read for the managing IT companies.

Keywords
wireless network, video surveillance, configuration

CONTENTS

1 INTRODUCTION

As the number of jobs increases and information is transferred to the cloud, there is a growing need for uninterrupted internet access. Wireless network is already in use in UAB “Kika Group”, but the equipment itself is not working as they would like to, so to ensure this, the network needs to be substantially upgraded in most places. Fast connection, impeccable equipment, easy-to-monitor network provides employees with a comfortable work environment. Therefore, happy employees bring an impact on productivity and quality at work, which is why most business owners are trying to invest in such technologies and upgrades.

1.1 Issue

The main issue with this project is to set up a wireless network that supports many devices and works without interferences. Pick-up/storage of goods takes place in the company's warehouses. This process is controlled by radio frequency terminals with built-in barcode scanners. These devices communicate with the server via a wireless network, so in the event of a connection failure, it is not possible to receive/add goods to/from the warehouse. The wireless network, which is currently in use, is implemented with the Motorola x AP solution. Barcode scanners are connected in a closed VLAN that covers most of the storage space. This solution is bad because of the equipment itself, which often breaks down and cannot ensure a smooth operation. The company currently has plans to build and prepare an additional production facility, which also needs wireless communication, as the collection of the finished products from the production facilities and transportation to the warehouse is accounted by the warehouse management program, which uses wireless scanners operating via a wireless network. Production facilities and transportation to the warehouse is accounted by the warehouse management program, which uses wireless scanners operating via a wireless network. All the work of the warehouse must be monitored using video cameras to be able to trace the events of interest, to stop any misconduct of technological processes.

1.2 Goal

Our goal is to develop a work plan and conduct tests to find out where the internet connection will be strongest and most uninterrupted. Also, in several places, replace network equipment with a newer and supportive of wireless networking features. Video surveillance network upgrades will be required in several locations.

1.3 Tasks

These are the tasks that are needed to follow in order to complete this project.

- perform an analysis of the existing network, identify its shortcomings,
- perform an analysis of communication technologies that could be used at work,
- prepare a wireless network project,
- prepare a video surveillance network project,
- select the necessary equipment,
- perform equipment configuration,
- perform testing of the prepared network,

After all these tasks, the project should be finished and implemented to the fullest.

2 ANALYTICAL PART

In this part, we will analyze current network area coverage, its hardware and video surveillance system and its problems.

2.1 Situational analysis

UAB “Kika Group” specializes in the production of pet food. With high production volumes, constant movement of goods, and many employees, most processes are automated, adapted to a wireless and wired network to maximize productivity of the employees. Most network devices work unreliably, often stalling work. The entire warehouse area is not covered by wireless connection. The company has plans to build and prepare a new production facility, which also requires the installation of a network.

2.2 Network analysis

The network of this company is local, designed with a star topology design. This method of network design is the most popular due to the possibility of controlling many devices from one point. The connection of new devices, the development of the network or the simple installation of equipment does not affect the operation of the entire network, only a small portion of devices, so companies usually choose this option when designing their network.

2.2.1 Network layout

To understand the situation better, we can look how the network devices are placed in the facility.

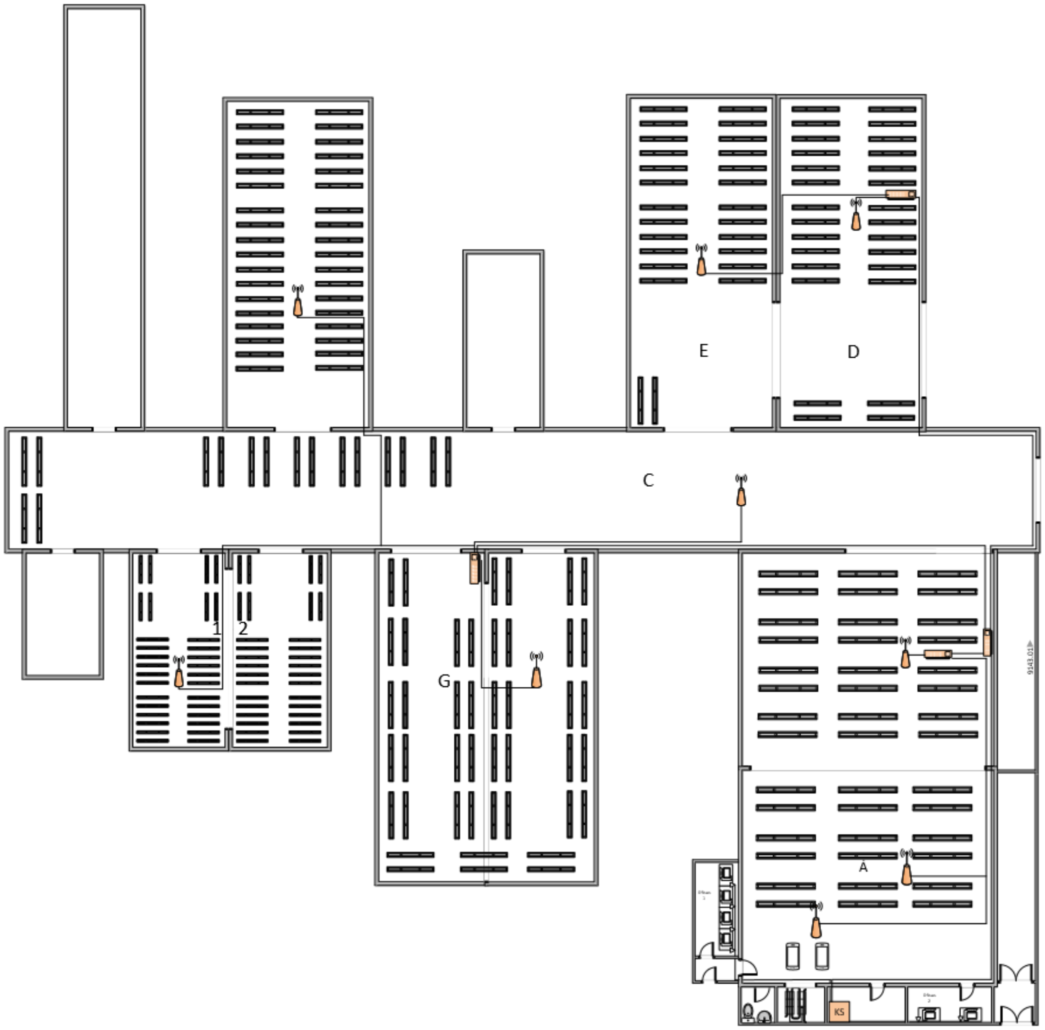


Figure 1 Physical topology of the current network

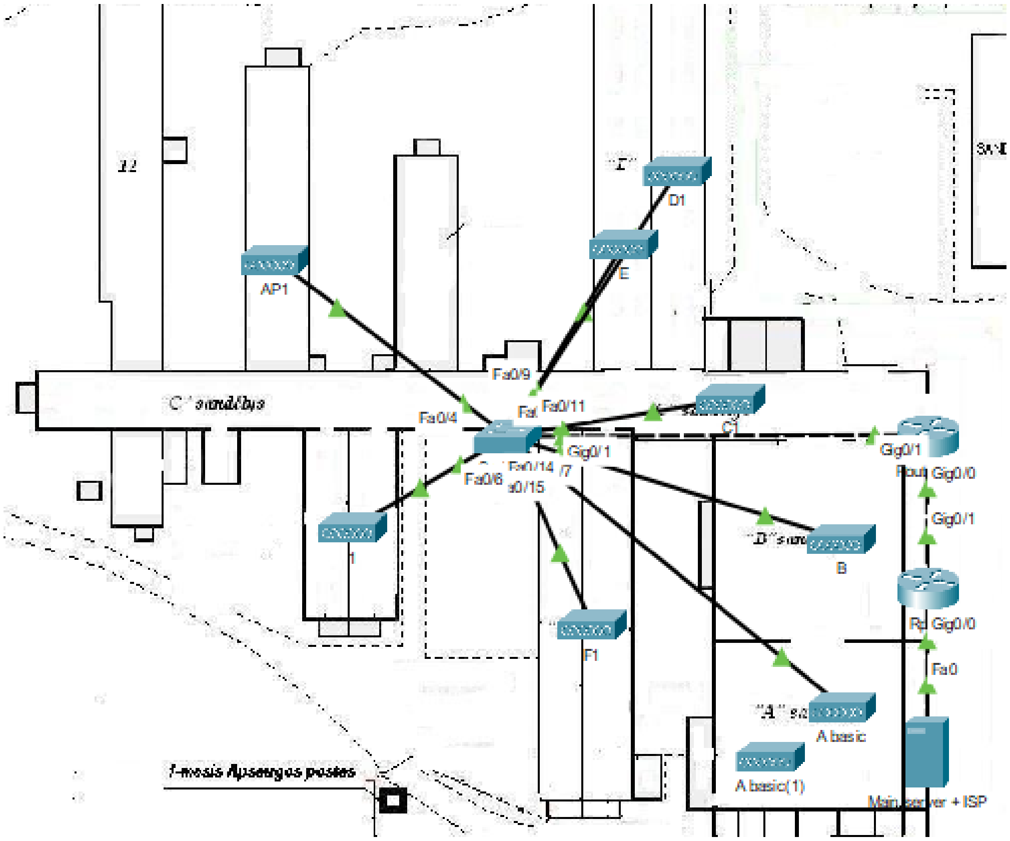


Figure 2 Logical topology of the current network

The simplified network layout is shown above. Only basic network equipment is visible. The network also has many unmanaged switches that are not shown.

2.2.2 Current wireless network coverage

The current wireless network cover at 2.4GHz and 5GHz has already been measured using *the* ***ExtremeCloudIQ*** network design tool.

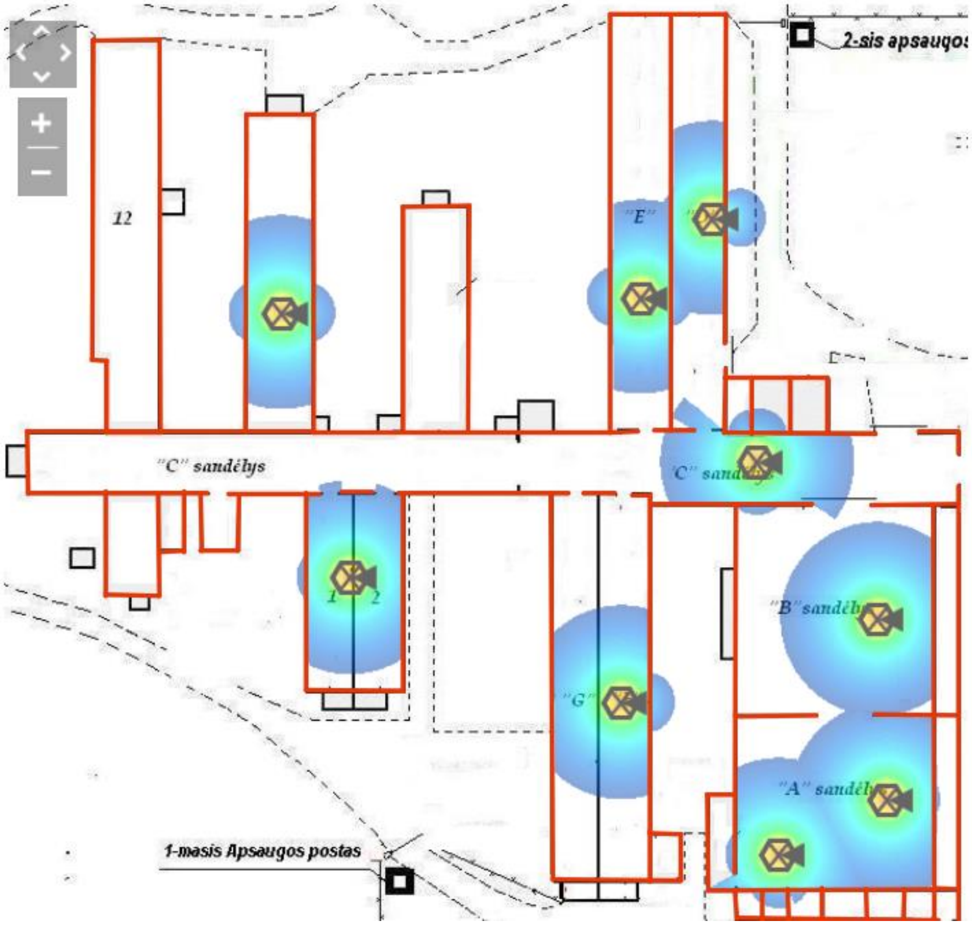


Figure 3 Wireless reach range at 5GHz

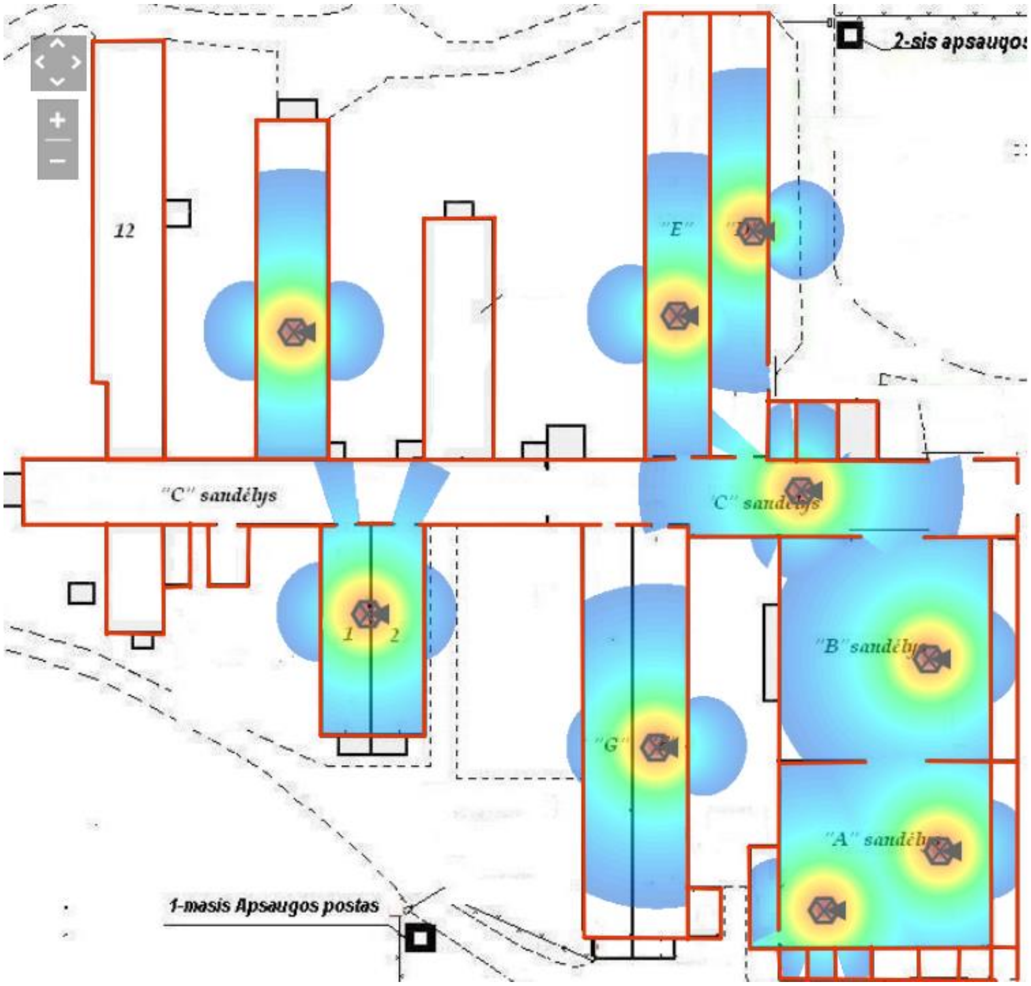
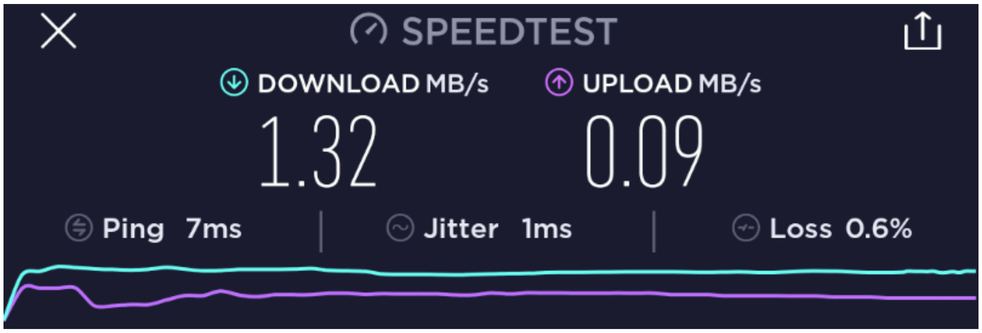


Figure 4 Wireless reach range at 2.4GHz

Currently, the company's wireless network uses the 802.11ac standard in most locations. This operates on 2.4Ghz and 5Ghz radio frequencies, but Motorola RFS4000 and APs in the company's warehouses only support the 802.11n standard, which affects file transfer. The signal itself suffers from the slightest side factors. Employees constantly complain that to maintain the best connection throughout the warehouse, you cannot place the goods high. The strength of the signal shown above exists only under ideal conditions.

The measured internet speed in one of the warehouses showed what the connection is really in these places. For wireless scanners used, this signal strength is too low.



DOWNLOAD MB/s 1.32

UPLOAD MB/s 0.09

Ping 7ms | Jitter 1ms | Loss 0.6%

Figure 5 Measured bandwidth

In order to upgrade all outdated network equipment, the company's network will have to have 802.11ac. A two-frequency and high-speed network will provide better connectivity in new facilities or warehouses with updated equipment. It should also be noted that standard 802.11ac is backward compatible, so there is no need to worry about the compatibility of some older devices with the new wireless network access points installed.

In the examples above, we can see that the wireless signal covers a large part of warehouses, but in some the connection does not reach all premises. For example, warehouse C has only one wireless access point, which covers only half of the warehouse. The rest of the network of these production facilities consists of a wired network. Connected radio terminals communicate with the Equinox server on a separate VLAN network in the company's warehouse.

2.2.3 Network hardware

The hardware used is mainly made up of Motorola, HP, Cisco, and Ubiquiti network equipment.

Motorola AP + Controller is the current solution for a virtual private network located in the company's warehouses. The Motorola RFS4000 model operates in 802.11n standard and has 5 *PoE* ports that supply Motorola wireless access points. This equipment is outdated and no longer in production, which is why there are problems repairing it. There is no way to update the software or simply replace it with a new device. The PoE port also often crashes, which leads to a power failure to remote wireless access points, and they stop working.

New wireless network installations are running on Ubiquiti wireless access UniFi series devices. UniFi access points and switches were perfect for this work due to their price/quality ratio and one of the essentials: a simple remote-control interface. Currently, two AP models are used throughout the warehouse area.

Table 1 Differences between the UniFi AP used

	 UniFi AP-AC-LR	 UniFi AP-AC-PRO
Used:	Inside	Inside/Outside
Maximum speed at 2.4GHz	450 Mbps	450 Mbps
Maximum speed at 5GHz	867 Mbps	1300 Mbps
Port support	10/100/1000 Ethernet	10/100/1000 Ethernet

In the table above, we can see that these wireless access points differ mainly in terms of usage and maximum speed at 5GHz.

2.2.4 Equinox server

For warehouse process management, the company uses Equinox Europe software "Equinox VISION WMS" *(Warehouse management system*). This system manages all warehouse processes and operations in real time. All items entering the warehouse are registered in the system according to the default parameters (vendor, item code, packing type, lot, serial numbers, expiration date, quantity, etc.). The location of the goods stored under this system may be determined based on different criteria. For example, goods for animals can be found according to which animals are intended, what packaging, etc. Warehouse customer orders are entered into the system using order entry windows. Orders are transferred to a vision system where they are re-processed into instructions for collecting and packaging goods.

According to these instructions, warehouse operators can use radio terminals operating in the warehouse and connected to wireless communication to collect orders, accept new goods, or perform stock counts. All prior information about shipments and prepared goods is sent to customers, and financial matters are transferred to accounting systems.

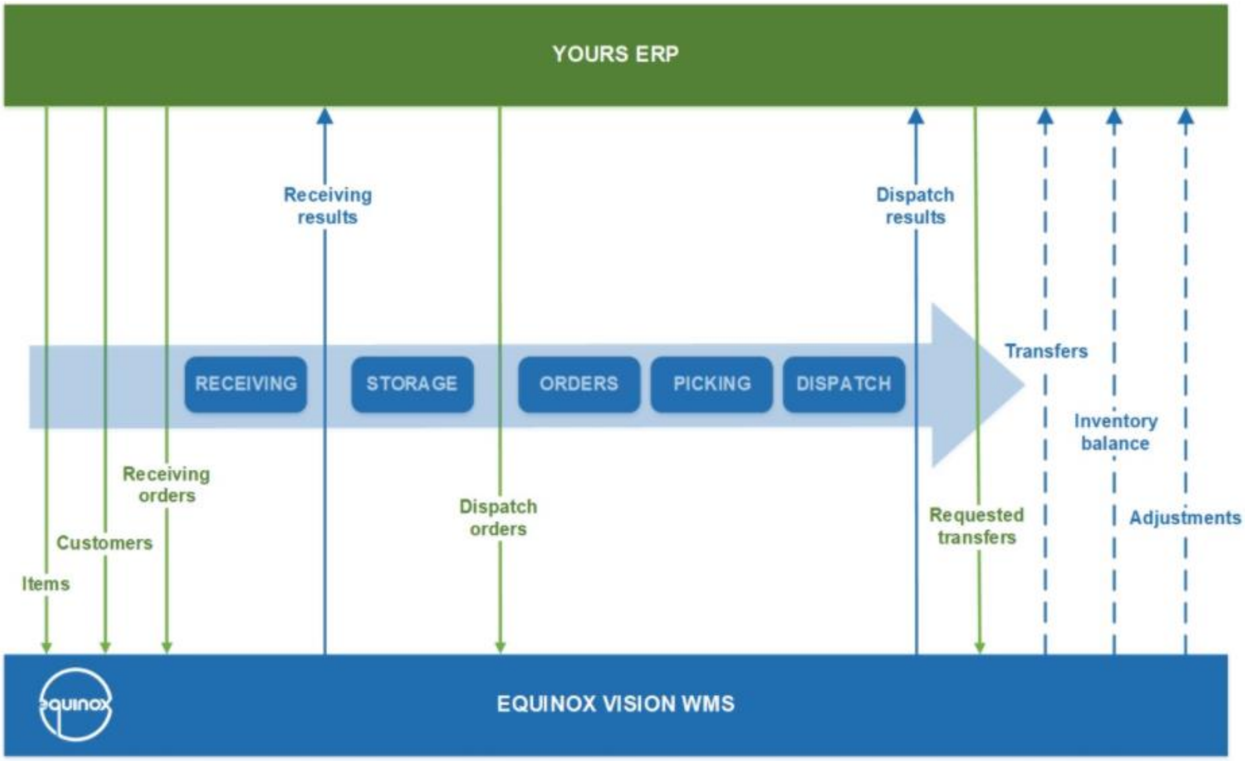


Figure 6 Data exchange with Equinox server

(source.: https://www.old.equinox.lt/wp-content/uploads/2020/04/Integration-with-ERP.jpg)

2.3 Video Surveillance analysis

Video surveillance is one of the tools for monitoring the processes taking place in the warehouse, as well as protecting against theft, burglary or accidents that require witnesses to find the culprit. For these reasons, many individuals or legal entities install video surveillance systems to insure and protect their property. The company is equipped with a number of cameras that cover most of the area. Main warehouses and production facilities are monitored.

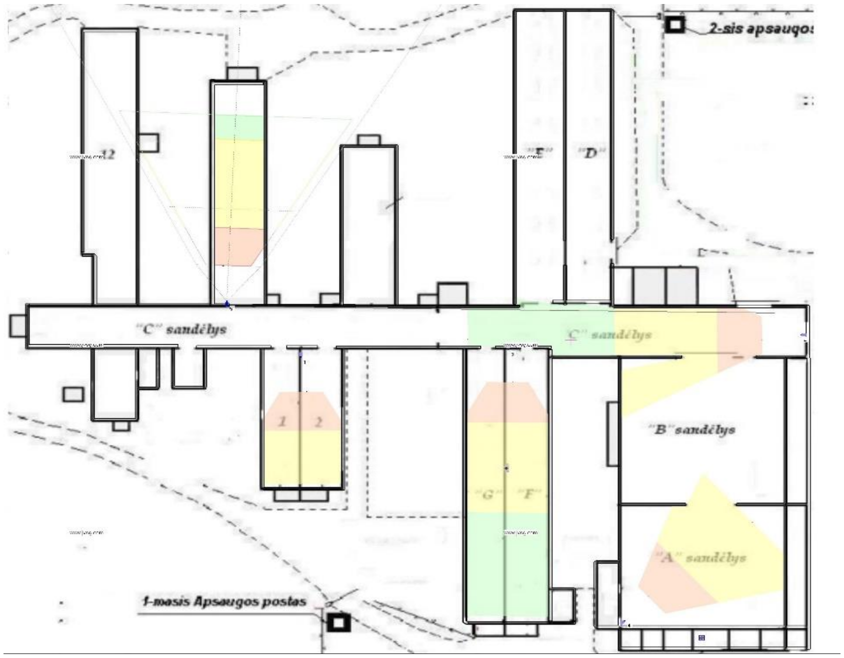


Figure 7 Currently monitored area

Video surveillance systems are divided into two groups: **DVR** *(digital video recorder)* and NVR *(network video recorder).*

Table 2 Differences between DVR and NVR

	DVR	**NVR**
Power plug	1 coaxial cable without audio support per camera	1 PoE network cable supporting audio, video, power functions
Preparation for installation	It is more difficult to prepare the plug, takes longer	Quick plug preparation, faster connection
Hub	Requires an additional hub for power, takes up more space	One switch is enough, everything looks tidier
Camera	Uses analog cameras, the image is processed by an additional DVR device	The cameras themselves process the image

The company's video surveillance system is based on DVR technology. This system is fundamentally outdated. The video recorder works unreliably, often crashing. Analog cameras are being used, and they have quite poor resolution, so the recorded image is not good. These cameras do not have the ability to process the recorded image in themselves, so every bit of information, with the help of a coaxial cable, goes to an additional DVR recorder that processes the image. As a result, recorded image lags, breaks and is simply too poor for this company.

Currently, the company's employees, responsible for security, are missing video in some warehouses. CCTV is completely missing in warehouses E, D, B and partly in C. The quality should be improved in warehouses 1–2 and A. Also, part of the premises should be monitored in the new production warehouse.

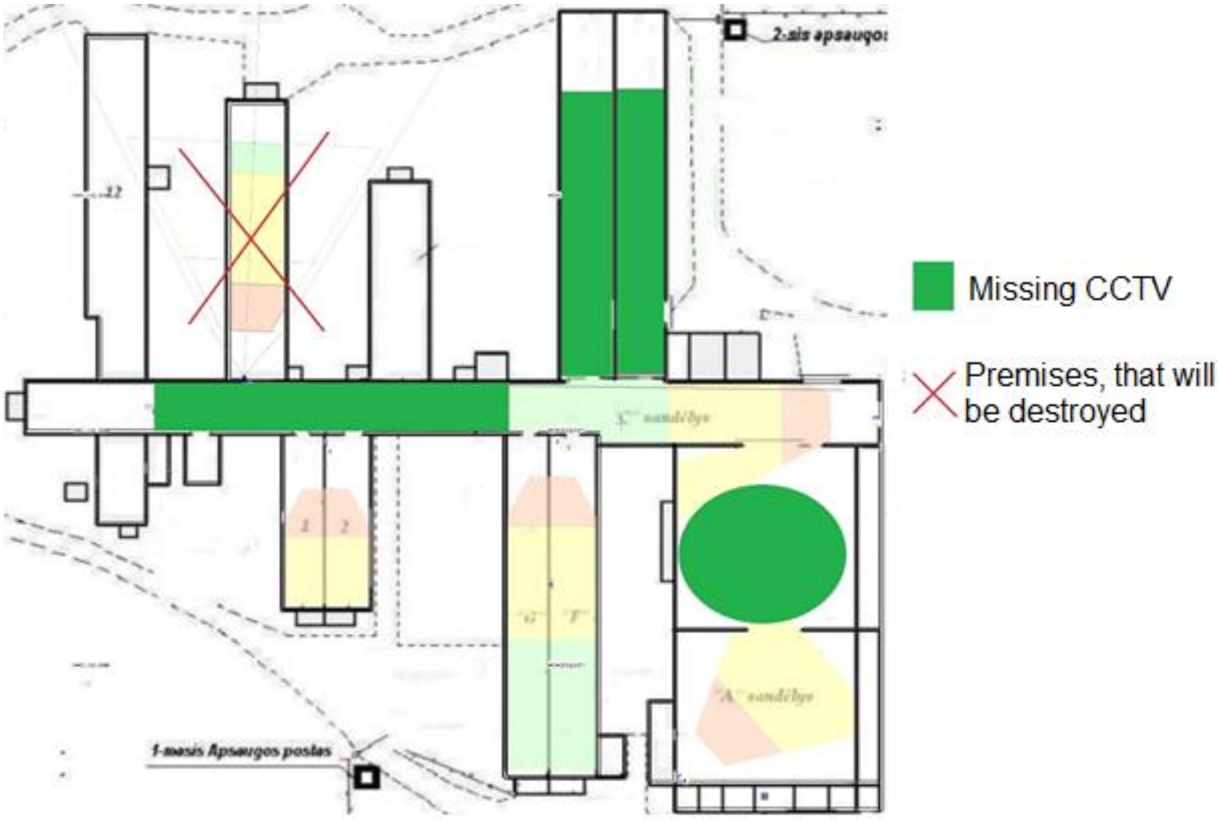


Figure 8 Places where monitoring is missing

2.3.1 Technology analysis – video surveillance equipment

The IP video surveillance systems used in the company are realized on the basis of Dahua manufacturer, so you need to continue to maintain the policy of one manufacturer in order to ensure full compatibility between the separated components of the system. For these reasons, only devices offered by the Dahua manufacturer will be selected.

2.3.2 Cameras

In order to choose your own video surveillance system, you need to understand what video cameras are and what they can do. One camera type example will be used for comparison.

Table 3 IP comparison of camera types

Camera types	Cable required	Resolution	Comfort	Purpose
PTZ Camera	Cat5/6 or PoE	Up to 5MP	Full camera control	Open areas, large spaces
Wireless Cameras	Power cable	Up to 5MP	Requires only one cable, so it is easy to connect	Indoor and outdoor
Bullet Camera	Cat5/6 or PoE	Up to 4MP	Small, easy to hide	Indoor and outdoor
Dome Camera	Cat5/6 or PoE	Up to 5MP	Strange video surveillance angle	Indoor and outdoor
Battery camera	-	1080p	Portable, easy to install	Indoor and outdoor
4G Camera	-	1080p	Portable, has no Wi-Fi	Remote locations where cables are not available

For this project, we will choose cameras with at least a 4MP resolution. This choice was decided based on an assessment of the quality of 2MP, 5MP and 8MP monitoring. 2MP is not a bad option, but when you zoom in a little, the image fades. The image monitored by 5MP cameras is already brighter, it is possible to see the license plates of passing cars, recognize a person walking across the street. 8MP cameras are much brighter but are much more expensive and take up significantly more file storage space, so they will not be fully utilized in this project. For these reasons, the choice is between 4MP and 5MP cameras. In the table below, I compared three IP cameras.

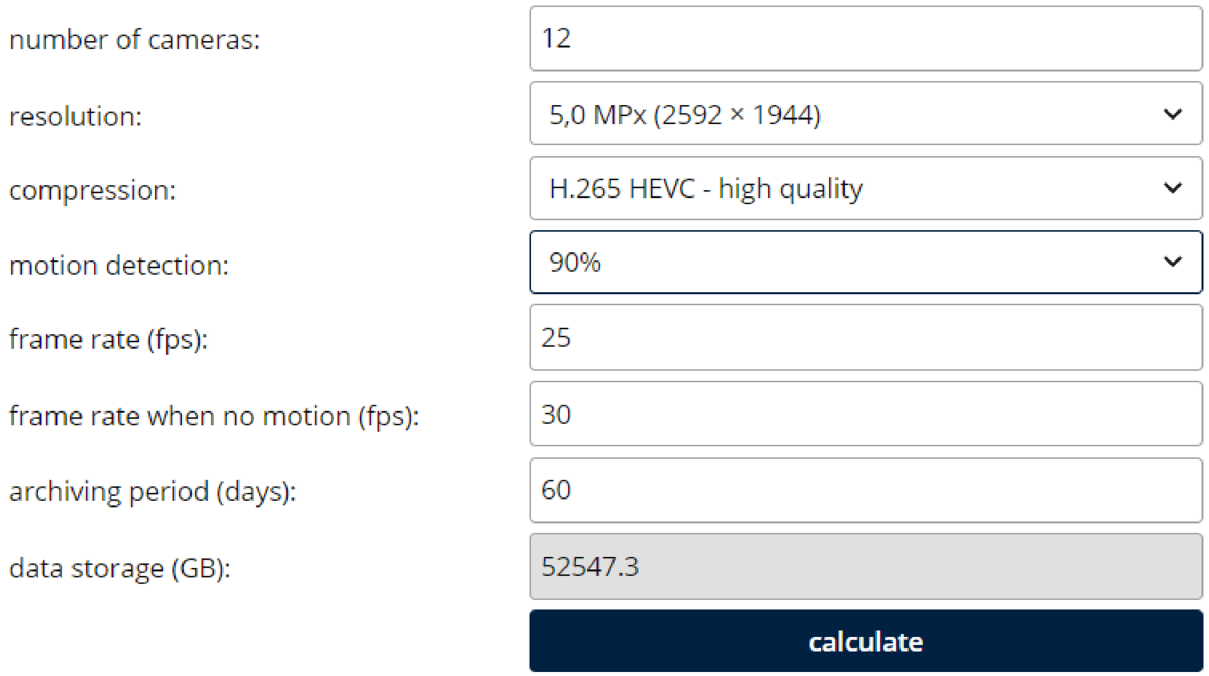
Table 4 Comparison of optional IP cameras

	IPC-HDBW5431E-Z5E	**IPC-HDBW2531R-ZS-S2**	**IPC-HDBW1531E**
Motion detection	Available	Available	Available
Maximum resolution	2688x1520 (4MP)	2592x1944 (5MP)	2592x1944 (5MP)
Frames per second	25/30FPS	25/30FPS	25/30FPS
Detectable distance	Up to 100m	Up to 40m	Up to 30m
Zoom	5x	-	16x
Image compression	H.265+/H.265/H.264+/H.264	H.265; H.264; H.264B; MJPEG	H.265/H.264H/MJPEG
Price	EUR 450	EUR 290	EUR 170

Of all three cameras, the **IPC-HDBW1531E** is enough for our project, as it is a bright camera that can zoom in if necessary, has motion detection and is more affordable than its competitors.

2.3.3 Video recorder - NVR

In order to choose the best option, we first need to calculate how much storage space will be needed for all the cameras we have selected. This is done perfectly by the website https://www.cctvcalculator.net/en/calculations/storage-needs-calculator/, where we enter the information of our selected cameras and see how much space will be needed. It is worth noting that the image recorded by the cameras, at the company's request, must be archived for 60 days.



number of cameras: 12

resolution: 5,0 MPx (2592 × 1944)

compression: H.265 HEVC - high quality

motion detection: 90%

frame rate (fps): 25

frame rate when no motion (fps): 30

archiving period (days): 60

data storage (GB): 52547.3

Figure 9 NVR device capacity calculator

Thanks to the calculator, we can see that for this project all cameras will require as much as 52.5TB of space. All NVR devices of the Dahua manufacturer support hard drives up to 10TB and are divided into 2HDD, 4HDD and 8HDD types. These types indicate how many hard disks fit in the drive. In our case, an 8HDD device is required.

Table 5 Comparison of an optional NVR device

	NVR5816/5832/5864-16P-4KS2E	NVR5816/5832/5864-4KS2
Supported number of IP cameras	16/32/64 Channel	16/32/64 Channel
Supported compression algorithms	Smart H.265+/H.265/Smart H.264+/H.264/MJPEG	Smart H.265+/H.265/Smart H.264+/H.264/MJPEG
Supported resolution	Up to 12MP	Up to 12MP
PoE support	Yes	No
Price	EUR 795	EUR 575

By comparison, we can see that these two devices differ only in PoE support. Since it is planned to connect the NVR device to the cameras using switches, there is no need to pay more for a feature that we will not use.

For this device we will also use **SEAGATE Surveillance AI Skyhawk 10TB** hard drives, which are specially designed for video surveillance systems and will fit perfectly into the NVR device.

2.4 Network addressing analysis

The ISP provides the company with a public **Class B** address, which is then translated into an internal network addresses. Here, we will see how the addresses are divided.

2.4.1 IP addressing

The internal network of the company is divided into two subnets. For security reasons, 172.16.1.1 – 172.16.1.99 are provided to network switches, and 172.16.1.100 – 172.16.1.254 are provided to wireless access points.

2.4.2 Dynamic IP addressing

Here we see the spread and connection of dynamic IP addresses on the internal network. These IP addresses are used for the main network equipment– switches, routers, servers, wireless access points. The remaining address space is reserved for future network development.

Table 6 Dynamic addressing table

Type	Allocated subnet	Start IP addresses	End of IP addresses	DNS 1	DNS 2	Mask
DHCP	172.16.1.0	172.16.1.2	172.16.1.99	212.59.1.1	212.59.2.2	255.255.0.0
Workstations	172.16.1.0	172.16.1.100	172.168.1.254	212.59.1.1	212.59.2.2	255.255.0.0

2.4.3 Dynamic addressing table for endpoint devices

In this table we can see the distribution of IP addresses throughout all the endpoint devices

Table 7 Dynamic addressing table for endpoint devices

Type	Allocated subnet	Start IP addresses	End of IP addresses	DNS 1	DNS 2	Mask
Warehouse scanners	172.16.2.0	172.16.2.2	172.168.2.49	212.59.1.1	212.59.2.2	255.255.0.0
Analog cameras	172.16.2.0	172.16.2.50	172.168.2.99	212.59.1.1	212.59.2.2	255.255.0.0
Remaining devices	172.16.2.0	172.16.2.100	172.168.2.254	212.59.1.1	212.59.2.2	255.255.0.0

All the endpoint devices are on the same subnet and are given fifty addresses each.

2.5 Technology analysis – wired infrastructure of computer networks

To ensure the excellent functioning of the network, it is necessary to properly study what technological solutions will be needed.

2.5.1 Cables

There are two types of cables used to install computer networks: optical and twisted pairs.

A twisted pair cable is a cable designed to connect devices to a local network. Consisting of pairs of color-sorted copper wires. Most often, for one wire, there are four pairs which are protected from the outside by an additional layer of insulation. In this way, twisted wires reduce signal interference. These cables are divided into two groups: shielded and unshielded.

Shielded twisted-pair – each pair is individually covered with a metal layer, and all pairs are co-coated with an additional plastic armor. These cables are most often used when it comes to protecting passing signals from additional interferences that may occur from devices with strong magnetic fields.

Unshielded twisted-pair – all pairs are co-coated with an additional plastic armor. No metal layers.

Table 8 Categories of twisted pairs of cables

Cable category name	Maximum speed	Frequency	Use
CAT 5E	1000Mbps	100MHz	1000BASE-T Ethernet
CAT 6	10Gbps	250MHz	10GBASE-T Ethernet
CAT 6A	10Gbps	500MHz	10GBASE-T Ethernet
CAT 7	10Gbps	600MHz	Experimental

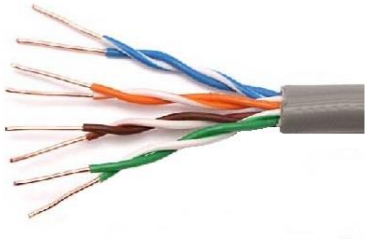


Figure 10 CAT5 cable

(source.: https://www.lemona.lt/LIUSE/Images/UTPmono.jpg)

Optical cable– a cable consisting of one or more optical fibres for the transfer of light. This cable is a great option for transporting a very fast amount of big data. Most often, the length of this cable reaches only 1-2 kilometers.

Figure 11 Optical cable

(source: https://5.imimg.com/data5/DD/CO/MY-25392387/fiber-wire-500x500.png)

2.5.2 Switches

Nowadays, in every home, there are a plethora of devices that can be connected to the Internet. Most often, one network cable comes to one apartment. With so many devices and only one cable, there is a problem. It is for such cases that switches are adapted. A switch is a device that performs the work of a network hub. Switches are divided into managed and unmanaged.

Managed switches are programmable, their settings are changed, it is possible to increase connection efficiency, monitor packets, network, quickly notice failures and connection interference.

Unmanaged switches are used on the ***plug-and-play*** principle when it is enough just to connect all the cables and then the automatically recorded settings are applied to your part of the network. Such a switch does not have the ability to monitor the network at the current time, make changes to the settings.

2.5.3 Wireless network standards

Wireless network technology is very popular due to its convenience, coverage, and ease of installation. When using wireless communications, data is transmitted using radio frequencies, so the user does not need to think about wires, or the number of devices connected. Wireless technology is described in IEEE 802.11 standards that are customizable to all devices that may require a wireless Internet connection. The table below compares IEEE 802.11 standards.

Table 9 Comparison of IEEE 802.11 standards

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Frequency, Ghz	5	2.4	2.4	2.4; 5	2.4; 5
Speed	Up to 54 Mbps	Up to 11 Mbps	Up to 54 Mbps	Up to 450 Mbps	1 Gbps
Benefits	Uses 5 Ghz, so there is no risk of interference due to connection overlap.	The most popular technology; quite cheap option	Backward compatible, supports a large number of users	Resistant to disturbances; Can work at 2.4 Ghz and 5 Ghz	High transmission speeds; Strong signal range.
Disadvantages	Various objects, walls have a significant influence on signal strength	Uses a frequency of 2.4 Ghz like other devices, causing connection overlap issues			Older devices do not support this standard
Distance in a closed room	35 m	35 m	38 m	70 m	35 m
distance in an open room	120 m	140 m	140 m	240 m	-

2.6 Conclusion and decision

In case of problems with outdated equipment in the company's warehouses, as well as the start of planning for the construction of new premises, it was decided to carry out a major renovation of outdated wireless equipment, which should increase the productivity of warehouse employees and facilitate work for the company supervising the network. It was also decided to install a wireless network in the new facilities after the conclusion of construction works using new equipment that could be managed.

3 PROJECT

Project part is where we choose equipment on desired basis, place the devices, plan the work, configure everything etc.

3.1 Chosen equipment

Here, we will go through the main hardware components, that we chose for this project.

3.1.1 Network switches

To ensure full compatibility of network devices in the company, it was decided to replace the old Motorola switches in the warehouses with UniFi Switch 16 (150W). These switches are managed, so it is a great choice for companies that maintain the company's network to make work easier and easily solve network problems. These devices are high quality, popular and have an attractive price. It is worth noting that the software is constantly updated, so their security is ensured. In addition, all sixteen ports support the PoE feature, which allows you to power wireless access points or new IP cameras with a single LAN cable. This is convenient in that the number of cables is noticeably reduced, since only one instead of two cables is enough.

All UniFi switches have mounting brackets on their sides, so they are suitable for installation in network cabinets or directly to the wall. The new premises will have a 24-port, 250-watt switch, which basically has the same functionality, only more ports.

Figure 12 UniFi Switch 16 150W

(source: https://www.ui.com/unifi-switching/unifi-switch-16-150w/)

3.1.2 Access points

UniFi AP AC LR was selected as the access point. They were chosen due to several factors: the ability to connect 250 users at the same time, as well as good signal coverage, attractive price, and quality. This model is specially designed for long distances, making it perfect for large warehouse spaces. This UniFi model has a single LAN port through which it receives power. The kit also includes a PoE adapter to power from the network outlet as well. A great choice for simultaneous support for both frequencies.

UniFi AP AC LR specifications:

- Power supply: 802.3af
- Maximum possible energy consumption: 6.5W
- Operating frequencies: 2.4 GHz and 5 GHz
- Maximum TX power Max. TX Power 2.4 GHz – 24 dBm, 5 GHz – 22 dBm
- Antenna Reinforcement Antenna Gain: 2.4 GHz – 3 dBi, 5 GHz – 3 dBi
- Radio frequency: 2.4 GHz – 450 Mbps, 5 GHz – 867 Mbps
- Wireless standards: 802.11 a/b/g/n/k/v/ac
- Wireless security: WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
- Maximum number of users: 250+

Figure 13 UniFi AP AC LR

(source: https://www.katalita.lt/full/uap-ac-lr_front.jpg)

3.1.3 IP cameras

Following an analysis of the CCTV equipment and after hearing the security officer’s problems, it was decided to partially update the CCTV system. The system will be upgraded to an NVR-based system. Selected IP dome cameras with a 5MP IR lens that can display the image in dark places.

These cameras can receive power through an additional power cable, so you can connect directly to the switch or network outlet. What is more, these cameras have motion sensors and a "corridor" mode, making them a great choice for darker rooms.

Figure 14 Dahua 5MP IP Camera

(source: https://www.eproma.lt/6977-large_default/ip-vaizdo-kamera-kupoline-5-mp-28-mm-ipc-hdbw1531e.jpg)

3.1.4 NVR

For the recorder, we chose Dahua production **DHI-NVR5816/32/64-4KS2** NVR, which is perfectly compatible with our selected cameras. This device supports up to 16 cameras at a time, up to 200Mbps of data speed and up to 12MP cameras, so if there is a need to use brighter video cameras in the future, it could be done without an NVR update. It is worth noting that most Dahua NVR devices have the PENTAPLEX feature that allows you to perform five different actions at once without device crashes. These include recording, rendering, viewing a recording, copying recordings, controlling your device and remote network access.

Figure 15 Dahua NVR Device

(source: https://www.dahuasecurity.com/asset/upload/product/20180824/DHI-NVR5816-5832-5864-4KS2_Datasheet_20180824.pdf)

3.1.5 Additional required equipment

Additional equipment is considered to be hardware components or furniture that helps the main components to function and ensure uptime stability.

UPS

We will also place a UPS device next to each switch to maintain the power supply in the event of power outages. One network switch can use up to 150W, and the minimum that a UPS can support is 480W, so we do not have to look for expensive options. For each new switch, I chose the **EATON 5E 850i USB** device, which will be enough to maintain the power supply for more than four minutes.

Figure 16 UPS for switches

(source: https://www.varle.lt/static/uploads/products/622/ups/ups-eaton-5e-850-480w-850va-tower-4xiec.jpg)

Network cabinet

The network cabinet is designed to put several network devices in one place, and it will provide protection against impact or dust. Also, it is a great way to maintain general organization of cables. The width of all cabinets is a standard 600 mm, and the height is different, so in this project, to choose the correct size of the cabinet, we need to know how much space the built-in equipment will take up. Each cabinet will have a network switch, a UPS, and incoming/outgoing cables.

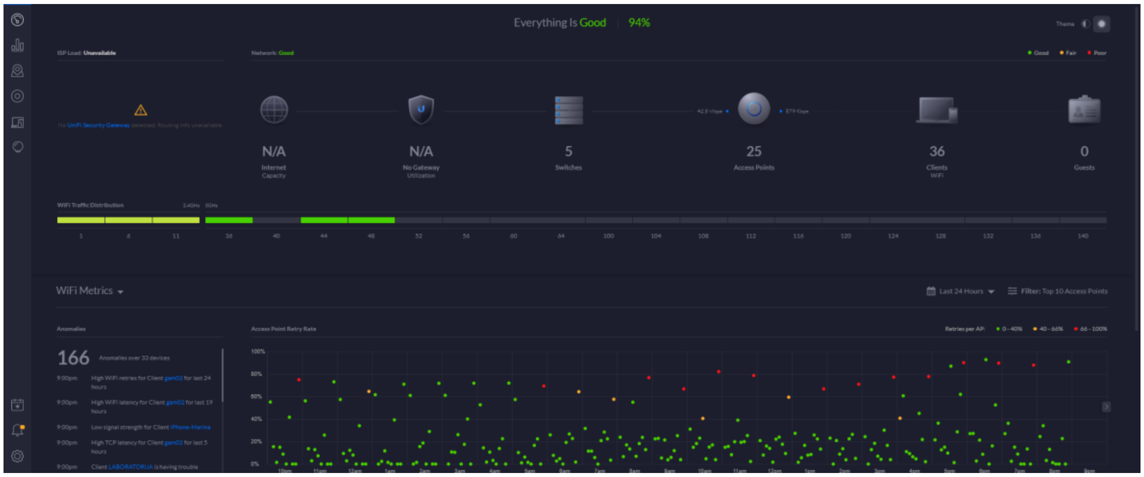
The 16-port switch has dimensions of 443 x 43 x 221 mm, a 24-port switch is 485 x 43.7 x 285.4 mm, and a UPS is 288 x 148 x 100 mm. We will need a cabinet that's taller than 210mm to accommodate said devices and still have room for correction. 6U-sized cabinets will be perfect for this project.

Figure 17 6U Network cabinet

(source: https://www.katalita.lt/full/292732_2.jpg)

3.2 Network monitoring interface

To manage and monitor the performance of network devices, we will use specially adapted software – UniFi Dashboard. This is a monitoring software for UniFi devices that provides information about the work of devices, their load, the placement on the map, configurable information and VLANs. This system greatly facilitates centralized remote maintenance and configuration of devices.



Everything Is Good | 94%

ISP Load: Unavailable

Network: Good

No UniFi Security Gateway detected. Routing info unavailable.

N/A Internet Capacity

N/A No Gateway Utilization

5 Switches

25 Access Points

36 Clients WiFi

0 Guests

Anomalies

166 Anomalies over 33 devices

9:00pm High WiFi retries for Client gam02 for last 24 hours

9:00pm High WiFi latency for Client gam02 for last 19 hours

9:00pm Low signal strength for Client iPhone-Marina

9:00pm High TCP latency for Client gam02 for last 5 hours

9:00pm Client LABORATORIJA is having trouble

Figure 18 UniFi Controller Control Panel

3.3 Configuration of network devices

To start the configuration of new devices, you first need to download the UniFi Controller software, which will give us access to UniFi devices in the control panel browser. After the installation process, we register our account and at the same time connect the UniFi switchboard to the network and to our computer to prepare it for configuration. We start the UniFi Controller server, which opens https://localhost:8443/ website for us.

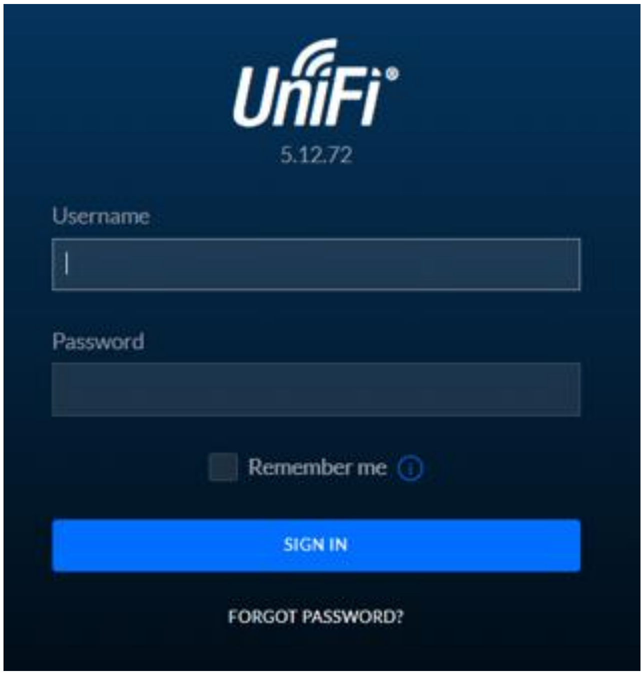
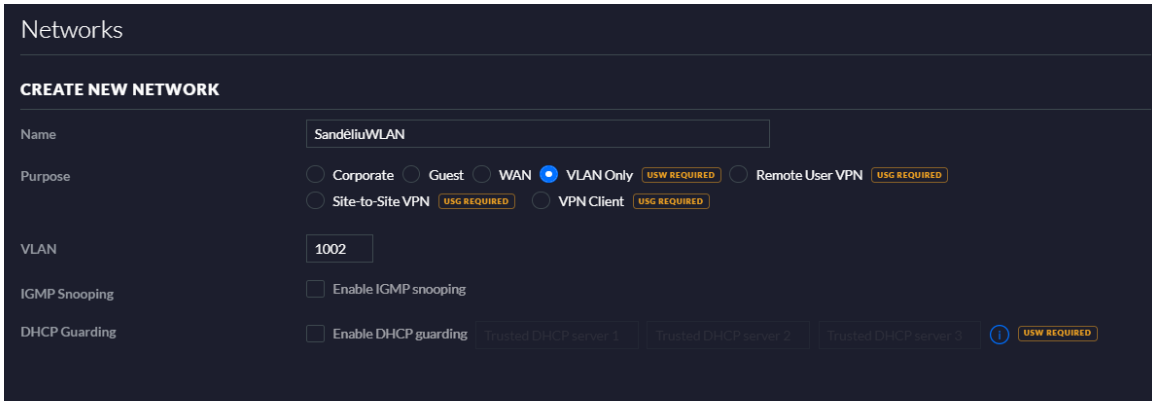


Figure 19 Sign into the Control Panel

After logging in, we go to the **DEVICE** subsystem and wait for the UniFi Switch 16 150W switch to be detected, then we press **ADOPT** to connect it to our control panel. Another task is to create a new closed VLAN so that all APs can communicate with each other and are not accessible to other users. Basically, we will create the same thing as before, only with new equipment and in the general control panel.



Networks

CREATE NEW NETWORK

Name: SandėliuWLAN

Purpose: ○ Corporate ○ Guest ○ WAN ● VLAN Only USW REQUIRED ○ Remote User VPN USG REQUIRED ○ Site-to-Site VPN USG REQUIRED ○ VPN Client USG REQUIRED

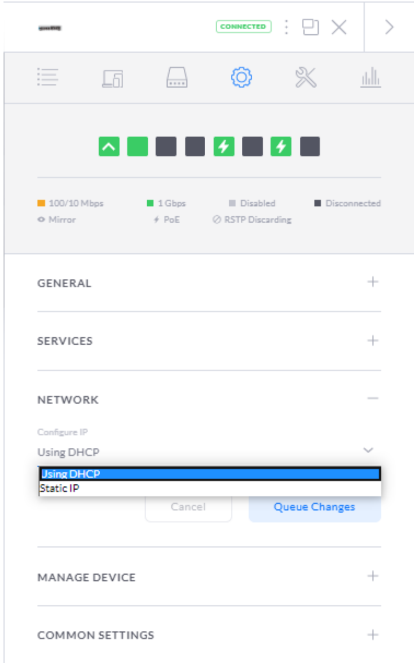
VLAN: 1002

IGMP Snooping: □ Enable IGMP snooping

DHCP Guarding: □ Enable DHCP guarding Trusted DHCP server 1 Trusted DHCP server 2 Trusted DHCP server 3 USW REQUIRED

Figure 20 Network building interface

Because the company already has a DHCP server installed, we give them a clear name when configuring new switches and select the DHCP address retrieval configuration. A moment later, the device gets its address. Control Panel is convenient in that each device has its own address nearby, so you never have to look for lost IP addresses to connect to a managed device.

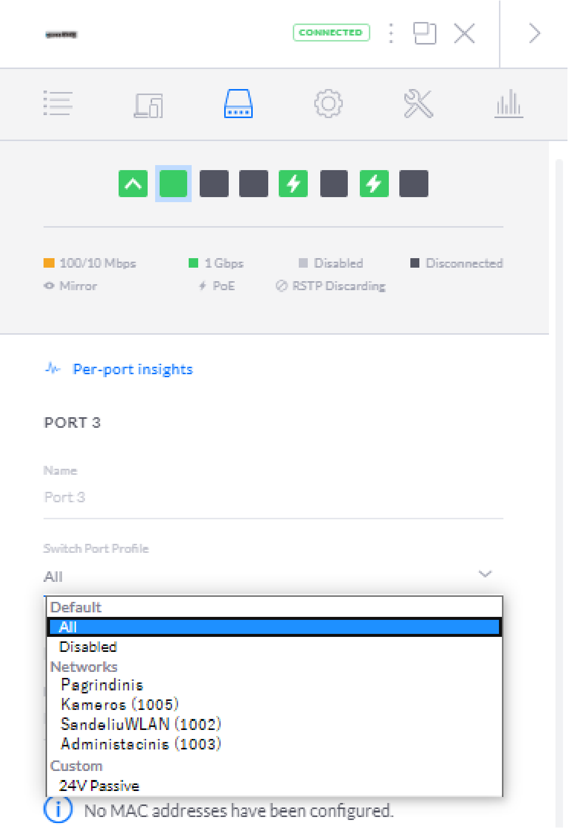


Configure IP: Using DHCP

Using DHCP
Static IP

Figure 21 Switch IP configuration

After the switch reboots, we can start a port configuration that will allow us to automatically assign a new device to a closed network. We select a port and press **Switch Port Profile,** where we can choose from many ready-made network profiles. In our case, SandeliuWLAN is chosen, which we have previously created.



PORT 3

Name
Port 3

Switch Port Profile
All

No MAC addresses have been configured.

Figure 22 Switch port configuration

The same configuration must be performed for all switches in the facilities. Access points receive an IP address from a DHCP server and are assigned to **Pagrindinis** network. After that, they are assigned to a special WLAN group that has 8 different SSID registered for different devices.

The DHCP server provides addresses for these devices between the **172.16.1.50** and **172.16.1.99** subnets because the first 50 addresses are already occupied by equipment outside warehouses.

3.4 Configuration of IP cameras

To start configuring the cameras, we need to first prepare the NVR that will record the image that the cameras are watching. We provide static addresses to all IP cameras and the NVR device. We do this for two reasons: to be able to always access or connect to these devices and to make it a much safer way than DHCP. The subnet we are using is designed mainly for enterprise cameras. Because we also change old cameras, we can use the entire subnet from our first addresses.

Table 10 Addressing used for cameras

Type	Subnet allocated	Start IP addresses	End of IP addresses	DNS 1	DNS 2	Mask
New Cameras	172.16.2.0	172.16.2.2	172.168.2.49	212.59.1.1	212.59.2.2	255.255.0.0

We download the Dahua Configuration Tool and there we find out the static default address of the NVR device, with the help of which we can log into control panel in the browser. Later, we will always log in to this address to open this NVR configuration panel. As the main device, we give it an address 172.16.2.2.

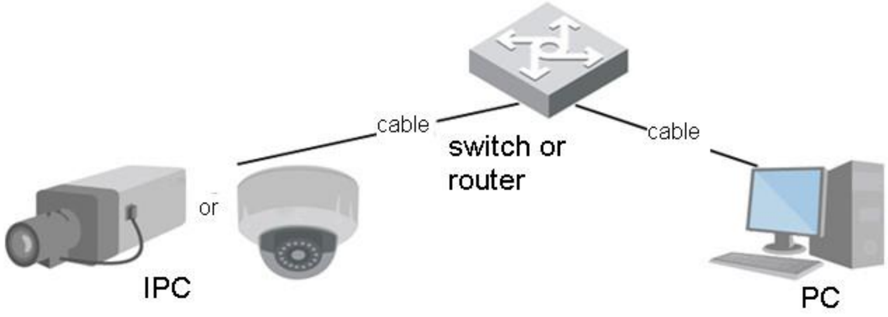
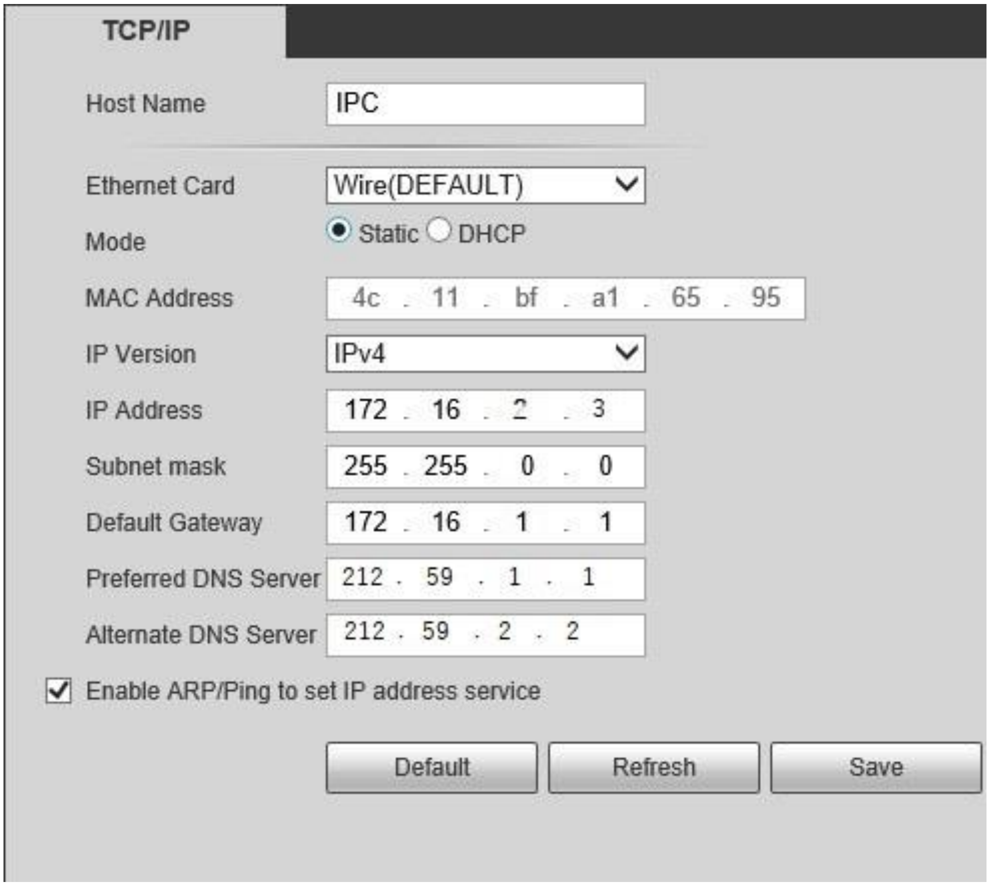


Figure 23 Connecting NVR and cameras to the switch

[source: https://www.security.us.panasonic.com/docs/advidia/E-37-V-Dome-Camera-Operation-Manual-V1.pdf]

After changing the static address of the recorder, we connect the cameras and NVR to the same switch to assign static addresses to the cameras. All address assignments are executed through the same NVR Configuration Panel. We assign addresses between **172.16.2.3** and **172.16.2.16** for these cameras.



TCP/IP

Host Name: IPC

Ethernet Card: Wire(DEFAULT)

Mode: ● Static ○ DHCP

MAC Address: 4c . 11 . bf . a1 . 65 . 95

IP Version: IPv4

IP Address: 172 . 16 . 2 . 3

Subnet mask: 255 . 255 . 0 . 0

Default Gateway: 172 . 16 . 1 . 1

Preferred DNS Server: 212 . 59 . 1 . 1

Alternate DNS Server: 212 . 59 . 2 . 2

☑ Enable ARP/Ping to set IP address service

Figure 24 Camera configuration

Changing addresses allows cameras to be disconnected and installed in their intended locations. The NVR device will detect them as long as they are on the same network, so it doesn't matter if multiple switches carry the signal. Later, we can use the software for video surveillance of Dahua cameras.

3.5 Updated WLAN in warehouses

Using the ***ExtremeCloudIQ*** network design tool, it was calculated in which warehouse locations it is ideal to install new wireless network access points. To calculate as accurately as possible, the walls of the buildings and the equipment using the 802.11ac standard were selected to suit the situation.

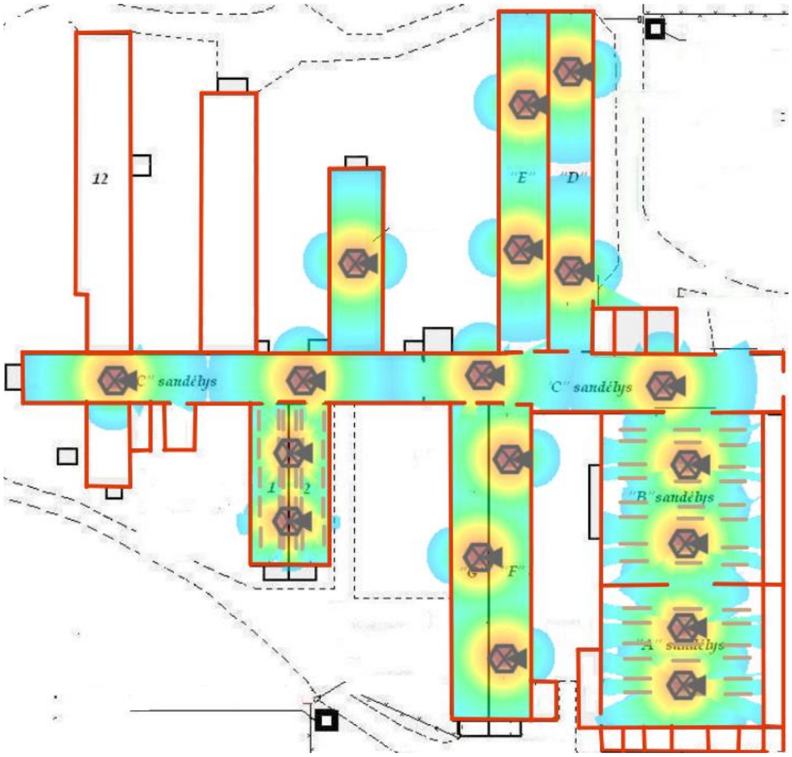


Figure 25 Designed WLAN at 2,4GHz

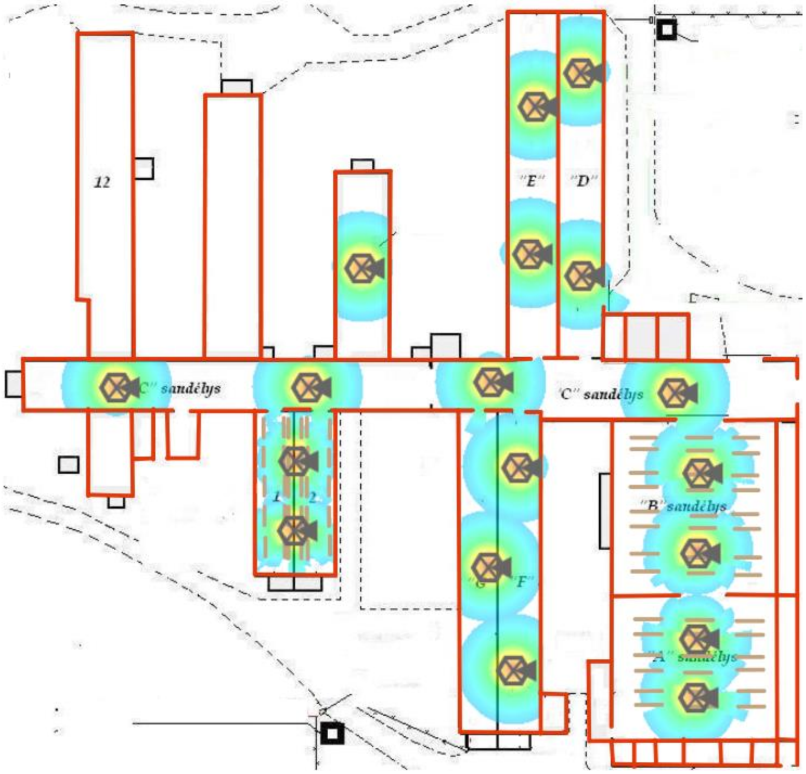


Figure 26 Designed WLAN at 5GHz

Based on the layout created in the ***ExtremeCloudIQ*** design program, we can notice that the 5GHz frequency does not cover the entire territory that we want to cover, but thanks to the chosen access point model, wireless scanners, having detected a weak 5GHz signal, will be able to switch to a 2.4GHz frequency connection without any issues. All this is enabled by simultaneous dual-band technology at access points, which allows you to support both frequencies at the same time, so you do not have to switch to another SSID that supports a stronger signal each time the connection signal is weakened.

Figure 27 Signal Strength Levels

The following method shall be used to demonstrate the strength of the signal. Red indicates the strongest signal area (-35 dBm), and blue indicates the weakest (-70 dBm and above).

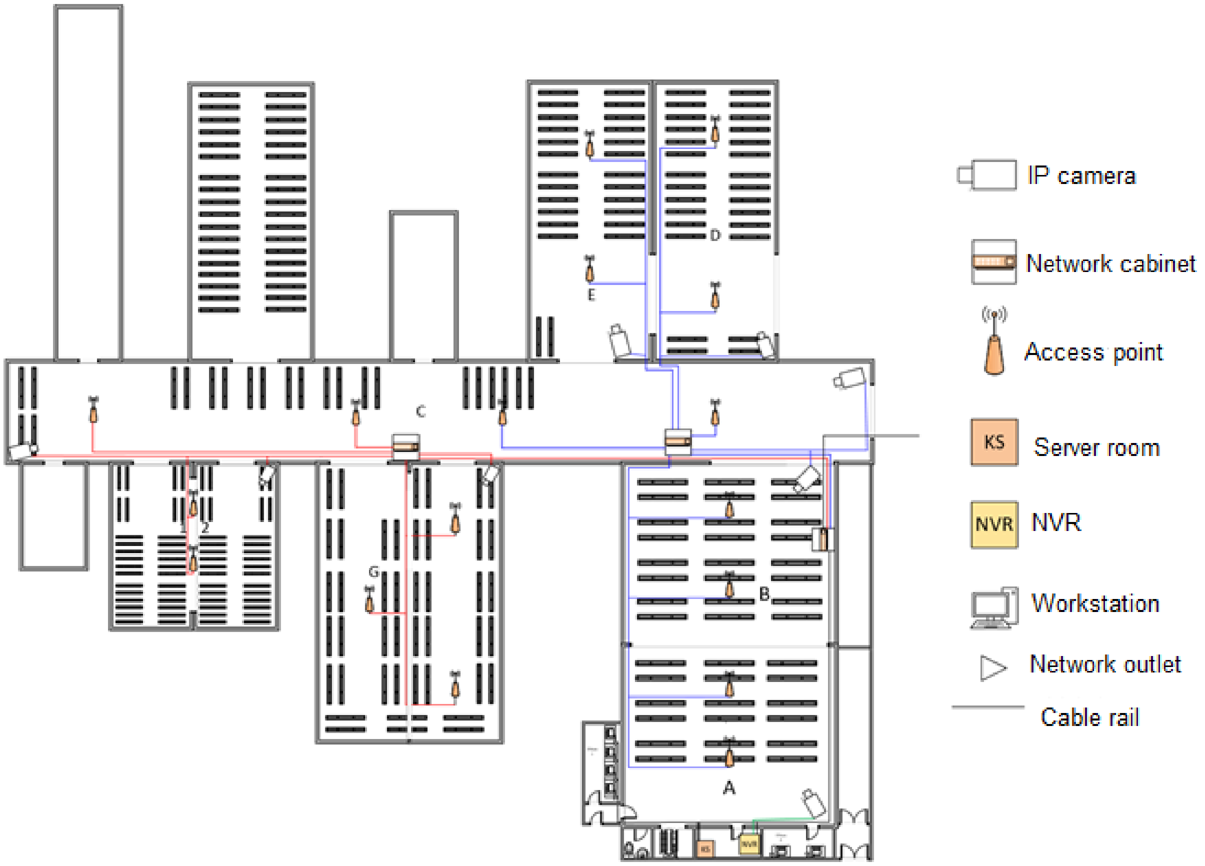


Figure 28 Physical topology of the newly designed warehouse network

The updated network in warehouses will look like this. The red and blue lines represent devices that will be connected to two 16-port UniFi switches. The black line marks the optical network cable traveling from the trunk router to the switch installed in the new premises.

3.6 Design of new indoor wireless access points

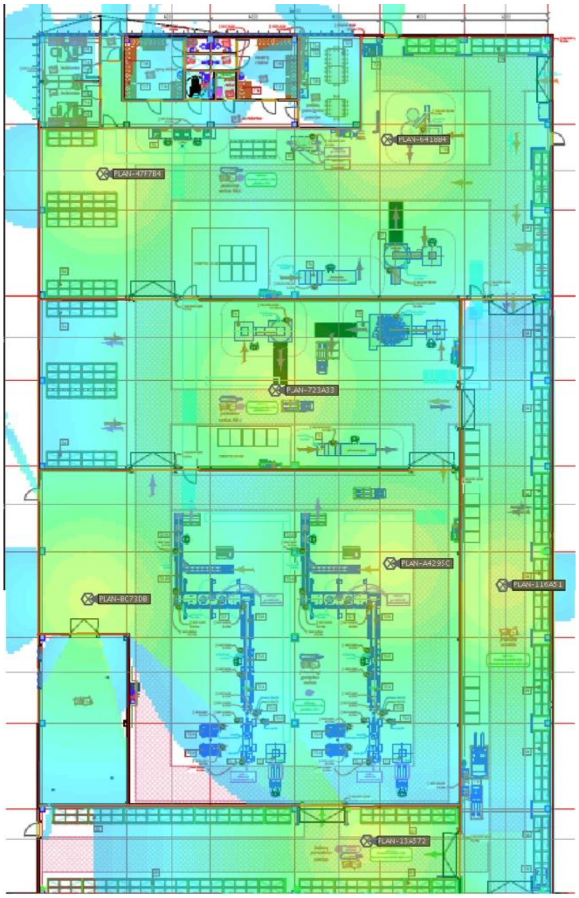


Figure 29 New production workshop wireless network coverage 5GHz

In this plan, we see the distribution of access points in new premises and the signal they emit at 5GHz. Although not all are covered by this signal, signal power is enough for all the most important devices.

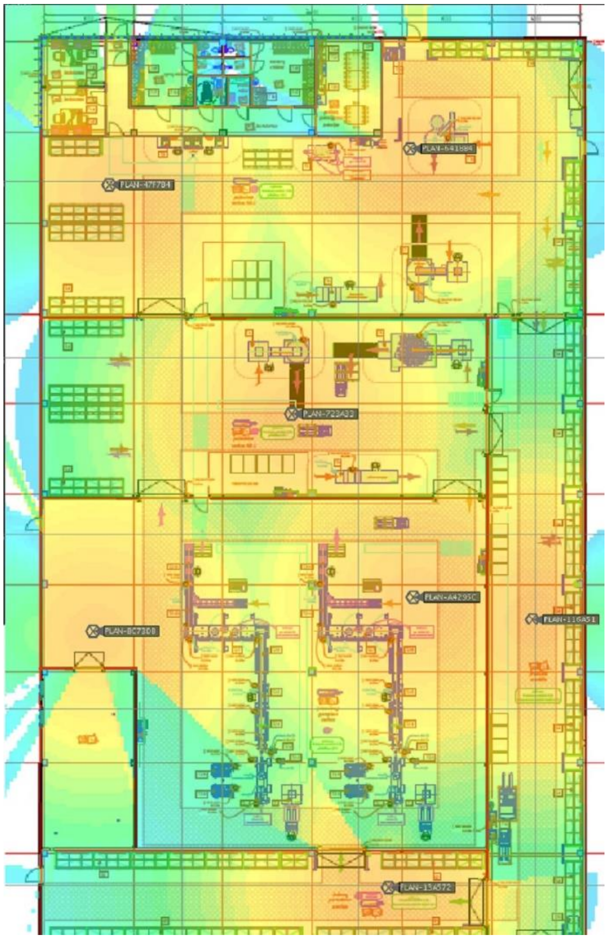


Figure 30 New production workshop wireless network coverage 2.4GHz

In the event of signal interference, the devices will be able to switch over the 2.4GHz connection within a few moments and continue to work. As a result of this AP layout, the Internet connection will remain throughout the production workshop. Even if one of the access points were to stop working, the signal emitted by the others would cover those places where the signal would disappear.

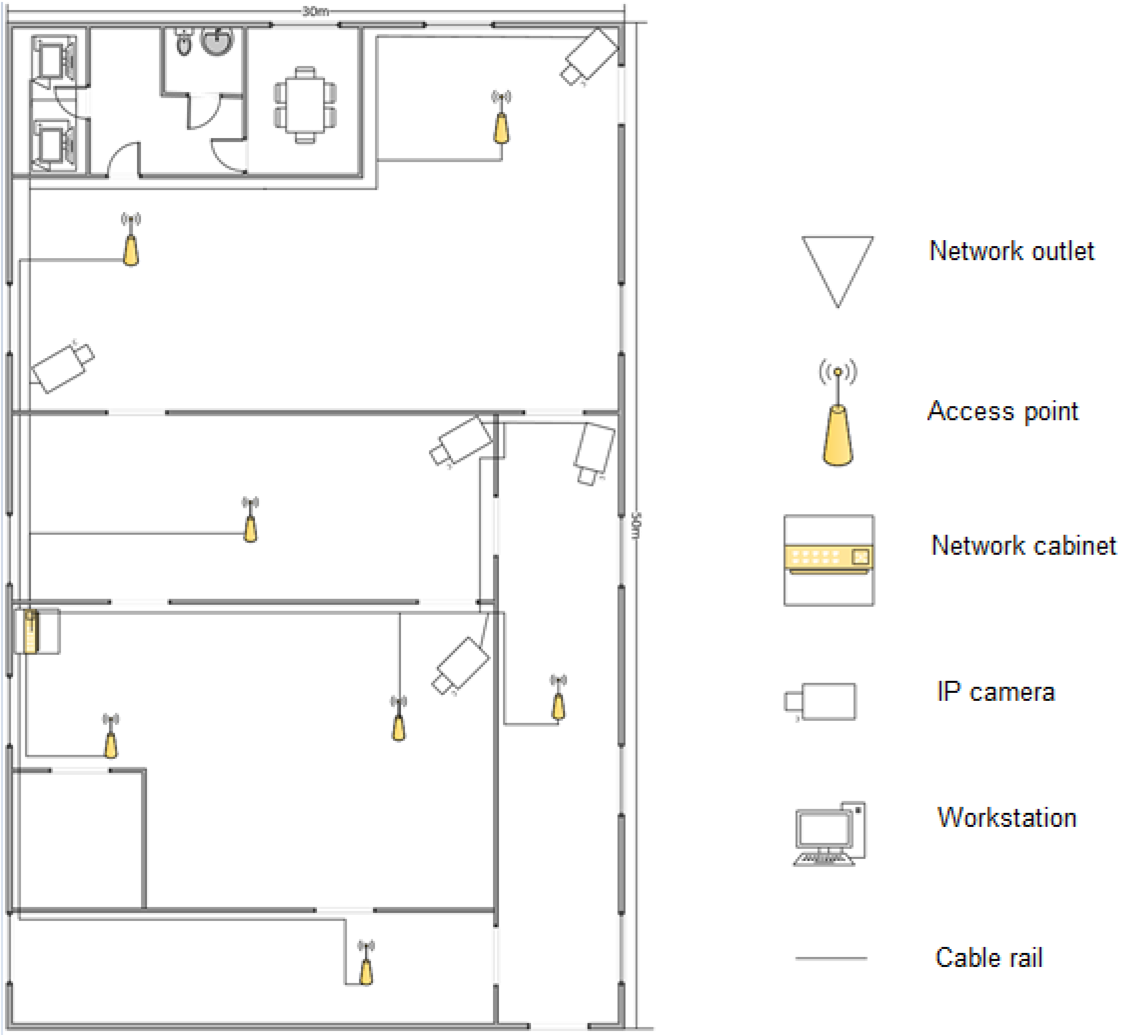


Figure 31 Physical network topology of the new production workshop

In this new production workshop, the **1Gbps** network signal will have to come from the main router in the old warehouses via an optical cable to the 24-port switch in the network cabinet. Due to future installations in the premises and the electrical interference they cause, all devices will be connected using CAT6-screened cables. Seven network access points and five cameras are connected directly to the switch, and computers in classrooms are connected through network outlets.

3.7 Updated addressing tables

Here we can see the updated dynamic and static addressing tables. Dynamic addressing, or DHCP, is for general network equipment like access points or switches and workstations.

Table 11 Updated dynamic addressing table

Type	Subnet allocated	Start IP addresses	End of IP addresses	DNS 1	DNS 2	Mask
Network equipment	172.16.1.0	172.16.1.2	172.16.1.99	212.59.1.1	212.59.2.2	255.255.0.0
Computerised workplaces	172.16.1.0	172.16.1.100	172.168.1.254	212.59.1.1	212.59.2.2	255.255.0.0

Static addressing is for endpoint devices. These devices require some sort of security measures and static addressing provides that.

Table 12 Static addressing table for endpoint devices

Type	Subnet allocated	Start IP addresses	End of IP addresses	DNS 1	DNS 2	Mask
IP cameras	172.16.2.0	172.16.2.2	172.168.2.49	212.59.1.1	212.59.2.2	255.255.0.0
Warehouse Scanners	172.16.2.0	172.16.2.50	172.168.2.99	212.59.1.1	212.59.2.2	255.255.0.0
Remaining devices	172.16.2.0	172.16.2.100	172.168.2.254	212.59.1.1	212.59.2.2	255.255.0.0

These tables are great for when new devices need setting up.

4. TESTING PART

I tested this project in the Cisco Packet Tracer network design program. This software cannot give devices an IP address, so DHCP will only work on endpoint devices.

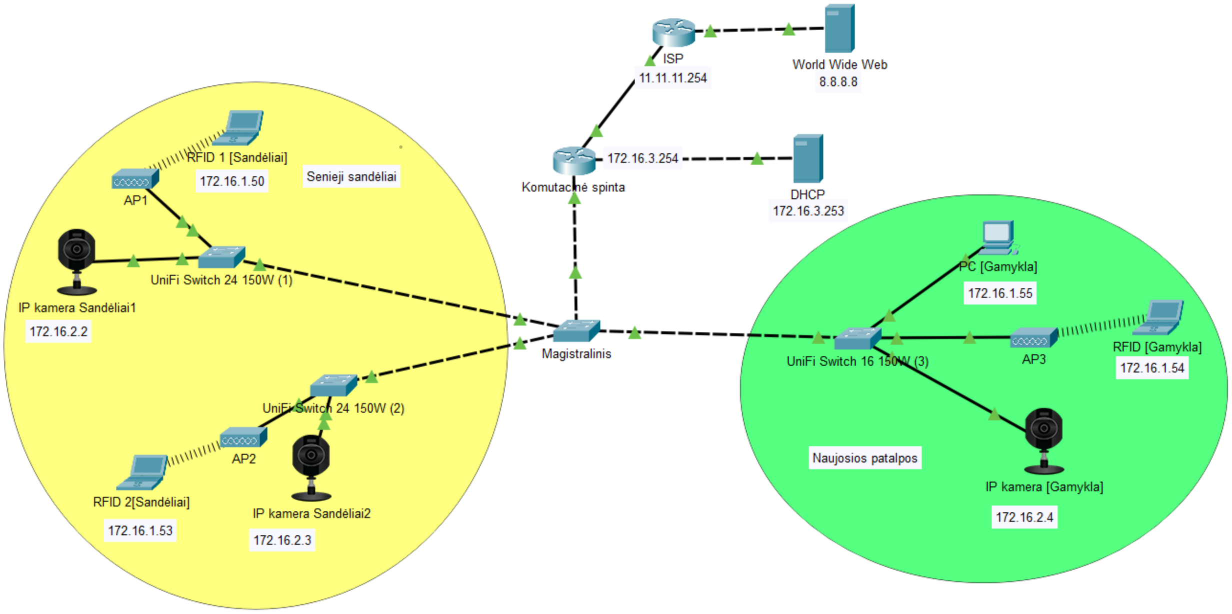
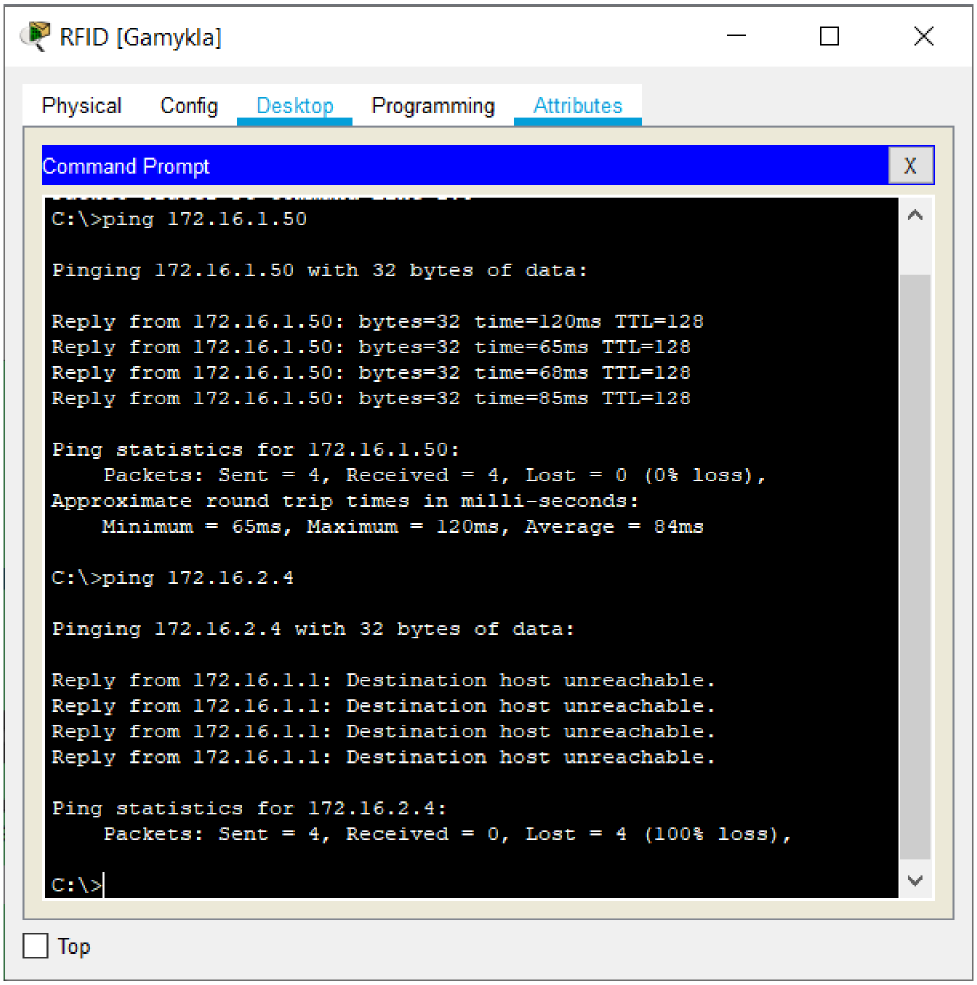


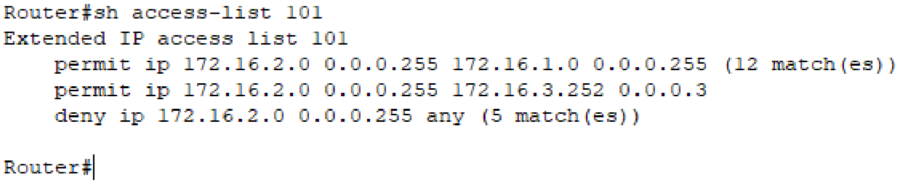
Figure 32 Network logical topology

In the plotted diagram, we can see a working newly prepared network. Yellow indicates the part of the net in the old premises, while green indicates the newly installed production workshop. All devices for communicating with the EQUINOX server are equipped with a separate VLAN. Devices on the same closed network in both rooms reach each other, but IP cameras do not reach these devices, which provides a little more security. In the illustration below, we can see that the RFID (scanner) of the new factory located in VLAN11 cannot reach the IP camera connected to the same switch, which belongs to VLAN12



```
C:\>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=120ms TTL=128
Reply from 172.16.1.50: bytes=32 time=65ms TTL=128
Reply from 172.16.1.50: bytes=32 time=68ms TTL=128
Reply from 172.16.1.50: bytes=32 time=85ms TTL=128

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 120ms, Average = 84ms

C:\>ping 172.16.2.4

Pinging 172.16.2.4 with 32 bytes of data:

Reply from 172.16.1.1: Destination host unreachable.
Reply from 172.16.1.1: Destination host unreachable.
Reply from 172.16.1.1: Destination host unreachable.
Reply from 172.16.1.1: Destination host unreachable.

Ping statistics for 172.16.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

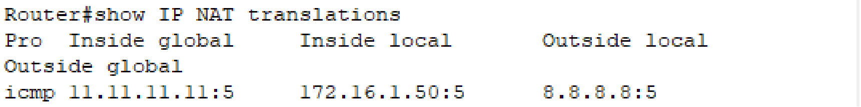
Figure 33 Availability of cameras and other VLAN devices



```
Router#sh access-list 101
Extended IP access list 101
    permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 (12 match(es))
    permit ip 172.16.2.0 0.0.0.255 172.16.3.252 0.0.0.3
    deny ip 172.16.2.0 0.0.0.255 any (5 match(es))

Router#
```

Figure 34 ACL performance test

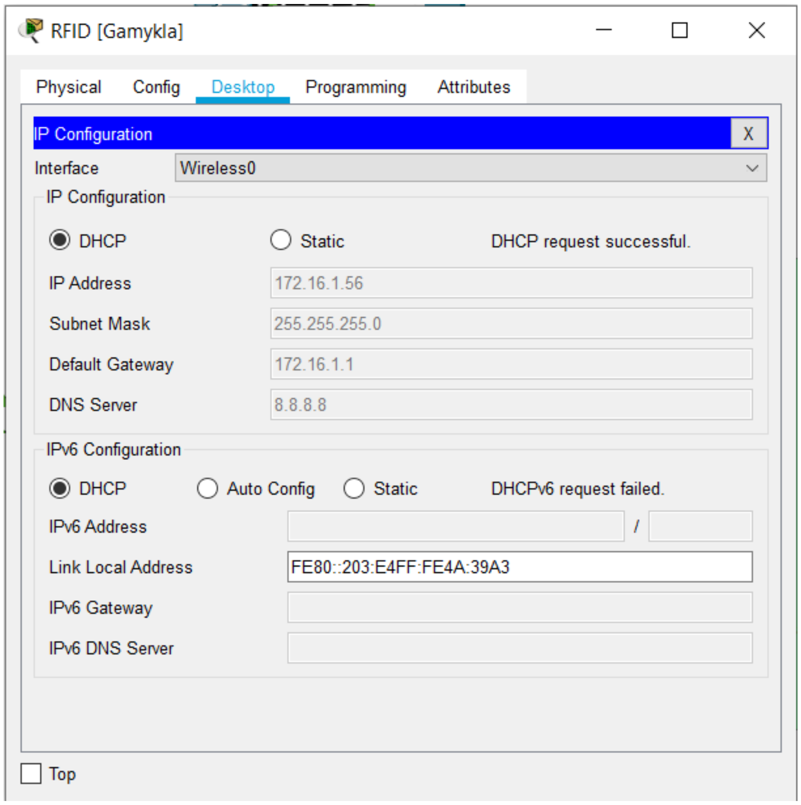
Next, we test the ACL that prevents external devices from accessing devices on subnet 172.16.2.0, i.e., all network cameras. All attempts to do so shall be recorded.



```
Router#show IP NAT translations
Pro  Inside global      Inside local       Outside local
Outside global
icmp 11.11.11.11:5      172.16.1.50:5      8.8.8.8:5
```

Figure 35 Testing the performance of the NAT

Finally, we check if NAT is working. This converts all outgoing internal IP addresses into a single external address. We can see that our internal address is successfully converted into an external address.



RFID [Gamykla]

IP Configuration X

Interface: Wireless0

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address: 172.16.1.56

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.1.1

DNS Server: 8.8.8.8

IPv6 Configuration

● DHCP ○ Auto Config ○ Static DHCPv6 request failed.

IPv6 Address: /

Link Local Address: FE80::203:E4FF:FE4A:39A3

IPv6 Gateway:

IPv6 DNS Server:

□ Top

Figure 36 Testing the performance of DHCP

Finally, we verify that the DHCP network is working and that the network devices are getting a dynamic address.

5. CONCLUSION

The analysis of the current situation has shown that the existing wireless network of the warehouse does not meet the needs, covers only part of the premises, works unreliably; outdated equipment used for video surveillance provides under-resolution imagery, stalling, and does not cover all desired locations.

So, to fix these issues, we chose these devices:

- UniFi 16- and 24-port switches that support PoE functionality on all ports
- UniFi AP AC-LR, which perfectly covers the entire desired territory
- Dahua 5MP IP cameras that convey good quality image and have motion sensors
- Dahua NVR device that supports up to 16 cameras and has a good enough image compression rate.

A new warehouse wireless network has been designed to provide a reception of at least –60 dBm and a transmission speed of at least 50 Mbps in all rooms at a frequency of 2.4GHz. Chosen hardware is relatively new, is up to date with its technologies and is constantly getting software updates. A new video surveillance network has been designed to ensure full monitoring in old and new premises and a non-stop system that stores recorded information for up to 60 days.

These upgrades in both network devices and video surveillance should last quite some time or at least until new constructions works or plans to expand even further. Nonetheless, new AP additions should not affect the current upgraded network.

This project implementation is estimated at **11,227.14** euros. This includes workforce pay, cabling, hardware, cabinets etc. Only equipment will cost **9,100** euros. It will take approximately **152 hours** to complete and bring around **1,300** euros of profit.

REFERENCES

1. Colbach, G. (2019). • The WI-FI Networking Book: WLAN Standards: IEEE 802.11 B/g/n, 802.11n, 802.11ac and 802.11ax. *[Wireless network standards]*

2. Cunningham, A. (2018). What Is a Network Switch, and Do You Need One? Retrieved from https://www.nytimes.com/wirecutter/blog/what-is-a-network-switch/ *[differences between managed and unmanaged switches]*

3. Donahue, G. A. (2011). Connecting VLANs. In Network Warrior. [VLAN connection]

4. Karris, S. T. (2008). NETWORK'S design and management. Fremont, CA: Orchard Publications. *[types and features of network cables]*

5. Klimavičius, G. (2018). Vaizdo stebėjimo sistemos projektas: Bakalauro darbas. Kaunas: Kauno technologijos universitetas. Prieiga per eLABa – nacionalinė Lietuvos akademinė elektroninė biblioteka. *[Differences between NVR and DVR]*

6. Martins, C. (2019, February 15). How to connect multiple IP cameras to a computer (step-by-step). Retrieved from https://learncctv.com/multiple-ip-cameras-to-a-computer/ *[Connecting IP cameras]*

7. SafeSite Facilities Ltd. (n.d.). Retrieved June 01, 2020, from https://www.safesitefacilities.co.uk/knowledge-base/internet-protocal-cameras-how-do-they-work *[How IP cameras work]*

8. *https://dl.ubnt.com/datasheets/unifi/UniFi_PoE_Switch.pdf [UniFi 16 port switch technical features]*

9. *https://dl.ubnt.com/datasheets/unifi/UniFi_AP_DS.pdf [UniFi AP Technical Features]*

10. *http://www.equinox.lt/sandelio-valdymas/sandelio-valdymo-sistema-vision/ [EQUINOX Server]*

11. *https://www.dahuasecurity.com/asset/upload/product/20180824/DHI-NVR5816-5832-5864-4KS2_Datasheet_20180824.pdf [Features of NVR]*

12. *https://www.dahuasecurity.com/products/productDetail/19977?us [Features of IP camera]*

13. *https://www.youtube.com/watch?v=kjUa0UjZBYQ [Comparison of the quality of IP cameras]*

14. *https://reolink.com/cctv-camera-types/ [Types of IP cameras]*