Deividas Mickunas

Modernization of company’s Freda network

Bachelor’s thesis
Engineer

2019

South-Eastern Finland
University of Applied Sciences

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)	**Degree**	**Time**
Deividas Mickunas	Bachelor of Engineering	December 2018

Thesis title

Modernization of company’s Freda network

42 pages
5 pages of appendices

Commissioned by

Supervisor

Matti Juutilainen

Abstract

The aim of this Bachelor’s degree time project was to create a new video surveillance network and expand company’s current networks with the Active Directory control system.

The company has two key entrances, out of three, to the company’s office floor that, at the time, had no security measures. It was determined that the doors would be monitored by the local security guards. The requirements for the new surveillance network were that it worked 24/7, would be able to record in the dark and send warning messages whenever movement was detected after working hours. Additionally, the distance between the two entrances was a factor when it came choosing the connection type from one camera to another.

The current network of the company was built and configured in such way that most of the company’s computers could only be controlled from the IT office. Since the building itself was large in scale there was a need of an easy access to the network’s Active Directory from key points where the IT specialists would spend most of their times. The requirements were that the new network would require low maintenance and little time to manage the networks resources around the company. These were the key elements for choosing the devices and software for the task.

The project created a new system to monitor the entrances to offices that held sensitive data all the time and to inform the security about any movement around these areas, when the company was closed. Additionally, the project also created a new Active Directory management network for IT specialists to help them be more efficient when it came to assigning resources to workers.

Keywords

Surveillance, Active Directory, Raspberry Pi, kiosk

CONTENTS

Figure and table lists

Abbreviations

AD – Microsoft Windows Server Active Directory
IP address – Computer identifier in IP network
NVR – Network video recorder
OS – computers operating system
PoE Injector – device made for distributing power via UTP cable's and ports
SSH - network protocol that defines secure client connection to a server environment using 22 (TCP) port
SSID (service set identifier) - IEEE 802.11 wireless network standard that gives network devices "network names"
Wi-Fi – wireless communication technology that allows transfer of data using wide length radio waves

1. INTRODUCTION

These days the computer network is a crucial part of every company that helps the work force and devices to communicate between one another. Be it transferring emails, documents, sharing files from one system to another, issuing commands and automated scripts. Thus, the network ensures a steady and transparent communication and communication is the universal currency that knits us together and drives our day to day operations.

According to managed it services Toronto provider PCM Canada, Computer networking is a pool of integrated computers configured to one another. Computer networks or data networks are chains of nodes linked by communication channels. The nodes receive, transmit and exchange data between endpoints. The endpoints include computer servers, mobile devices and tablets among others.

Modern networks are continually evolving, becoming more flexible, adding new features and technologies to their pool according to an article by Inspired Techs (2017). Therefore, every company needs to evolve as well, if it wishes to make best use of its computer network.

One of the main issues larger companies face today have to do with the sheer size of their network sprawl and the size of their operating work area. With personnel of hundreds and devices of thousands the IT Security personnel and network support are routinely at odds with identifying and solving the most common problems that commonly fall under performance degradation security issues categories according to an article by IT Direct (2012).

The purpose of this thesis is to find solutions for the previously mentioned large network problems for a furniture company called Freda. The thesis goals are to create an optimal surveillance system around two entrances to the office building where sensitive data is stored and to optimize IT departments efficiency when managing the network resources. The security system had to not interfere with the main network and to meet few requirements like work schedules, movement detection, night vision and warning messages. The resource management system had to be relatively easy to access for IT specialists and controlled over a browser. When not used by IT administrators the devices were to be used by other employees.

The bachelor’s thesis consists of five chapters. Chapter 1 already introduced what a computer network is, why it is important in modern company’s and what problems they face. Chapter 2 contains research elements that led to the choices regarding technologies and devices used in the project. Chapter 3 contains information about how the project was implemented. Chapter 4 contains information regarding the cost of the project in currency and time. Chapter 5 concludes the thesis paper with suggestions for improving the project in the future.

2. BACKGROUND STUDY

This chapter contains the study behind the choices of devices and methods used to complete the thesis. Additionally, there will be device comparison and a short introduction as to why medium to large companies need an Active Directory in their network.

2.1. Surveillance system technologies

When it comes to implementing new video surveillance there are plenty of methods and technologies that can be used to install the system according to surveillance security company Intervid Africa (2019). The three main methods are the type of the system, type of cabling and type of the network.

The most popular surveillance systems are an IP system and an analog system. The analog system is usually used in small business where the distances between the cameras and the recording device are short. Furthermore, the analog system can only support up to 32 devices and is limited for scalability. The IP system bases on giving the connected devices their own IP addresses and even power them on through an ethernet cable (PoE). This allows for a single recording device to have hundreds of cameras connected to it via the use of switches according to an article by CableOrganizer (2019).

The choices when it comes to cabling between devices are between fiber cables and cat series cables. The fiber cables, according to Mailheau (2019), use light technology to transmit data from one point to another, giving it the edge over cat cables when it comes to speed and safety from outside interferences. However, using light to transmit data means that the data cables themselves are made from glass, and unlike regular copper, glass cables are much more expensive and are limited by how much you can bend and twist the cable before ruining the connection. Meanwhile cat series cables, while still slower than fiber, are advancing rapidly when it comes to increasing their bandwidth and security like the cat7 cables that can support 100Gbps speed. Comparing the two cabling technologies fiber is better for long range, high speed connection, while cat category cables are best used around offices and factories. (Mailheau 2019.)

The options for the network itself are between having a wired network or a wireless one. According to an article by Goodman (2019) a wireless network comes with its benefits and drawbacks. What is great about a wireless network is that, since it doesn’t depend on ports for connection, it’s great for the convenience of the end user and scalability of the company, since routers and access points can be connected by any device supporting Wi-Fi. This technology saves a lot of labor and mitigates the complexity of the network. Nevertheless, the wireless network has its flaws, one of them being that the connection between devices is based on radio signals. These signals have limited range, becoming weaker the farther the end user is from the router and they can be blocked by thick walls and other devices that use radio signals and create noise around the connection area.(Goodman 2019.)

As mentioned in the previous paragraph various devices, that have some sort of wireless connection to one another can create noise. In Daniels (2012) book the noise is explained as an interference between two radio signals. Since the signals are high frequency sounds, they can collide with one another and mess up one another’s streaming data. To avoid that signal channels were created which transfer data at different frequencies, overlapping the signals. And depending on in which country you live there are different numbers of said channels, since the government always reserves a few frequencies for communications such as radio and defense. Additionally, one antenna company has even created their own airMAX technology that uses a non-conventional signal protocol Ubiquiti TDMA (Time Division Multiple Access) that provides greater noise immunity and performance.

2.2. Antenna alternatives

According to a guide by Radvan (2009) there are three types of antenna categories available for wireless connections:

- Omnidirectional
- Semidirectional
- Highly-directional

Omnidirectional antennas are designed to radiate a signal in all directions. An antenna of this type is an attempt to provide general coverage in all directions. This is the most common type found for client adapters and access points, as in these situations, good coverage in a general spherical area around the antenna is desirable.

Semidirectional antennas are designed to provide specific, directed signal coverage over large areas.

Highly directional antennas are used for point-to-point links; for example, between two buildings. They radiate a very narrow beam over a long distance and are often used for dedicated links. (Radvan 2009.)

Additionally, Radvan’s (2009) guide also specifies that antennas can also work in different modes: infrastructure or adhoc. The infrastructure uses wireless access points, like a regular household router that is a central device to manage connections between clients. This mode type can benefit from ACLs and firewalls. Adhoc, on the other hand, establishes connections between devices without the use of a central point to manage all the data transfers. This technology is also known as peer-to-peer connection that require no outside service providers to establish communication between devices.

Furthermore, the guide also discusses how newer and newer protocols are introduced on Wi-Fi devices to ensure to safety of wireless connection. It also gave tips for using WPA2 (Wireless Protected Access) certificates with AES (Advanced Encryption Standard) to further increase the security of networks. (Radvan 2009.)

2.3. Camera analysis

According to articles by Wilson (2015), Prajapati (2018) and Lou (2019) there are more than a handful of camera types on the market that have their own unique features. Among the most known types are the dome CCTV, bullet CCTV, network/IP CCTV day/night CCTV.

The dome CCTV cameras get their name from their shape where the camera is hidden underneath a one-way see-through glass, making it difficult to tell the direction that these cameras are facing, and thus are ideal for deterring criminals. These domes also have a subcategory that is speed dome CCTV cameras that also give the operators the ability to move the cameras’ field of vision.

The bullet CCTV cameras have a long, cylindrical, and tapered shape, similar to that of a "rifle bullet", often used in applications that require long distance viewing. Unlike the dome cameras these surveillance devices were solely created to capture images from a fixed location, pointing at a particular area.

The network/IP CCTV cameras, both hardwired and wireless, transmit images over the Internet or ethernet cables in a local network, often compressing the bandwidth so as not to overwhelm the traffic. These cameras are getting more and more popular among companies with developed computer network, since they are easy to integrate into the system and can scale alongside the business needs.

The day/night CCTV cameras are specified to work in either normal or poorly lit environment. These cameras are ideal for outdoor surveillance since they have a wide dynamic range to function in glare, direct sunlight, reflections and strong back light 24/7.
(Wilson 2015; Prajapati 2018; Lou 2019.)

Additionally, Webster's (2012) book about surveillance suggested that a good security practice when installing new surveillance devices is to buy the NVR (network Video Recorder) from the same manufacturer. That action would mitigate the possibility of a conflict taking place between the security devices.

2.4. Security network solution

Based on the previously covered studies it was determined that the following technologies, methods and devices will be used to complete the surveillance network project:

- Directional Wi-Fi antennas to establish connection between NVR and the farthest camera
- New network for the security overlapping with the existing company network
- IP bullet CCTV cameras with integrated features
- NVR from the same manufacturer as the cameras with integrated features

The Wi-Fi connection will be used, because the distance between the NVR on one camera (the left red X in Figure 2) barely goes over the 100 meter mark, meaning that, if it was connected with a cat category cable it, would require a switch somewhere in the middle to boost up the signal. Otherwise, the quality of the data transfer would suffer. Additionally, it would save the cost of labor and equipment as the IP antennas are quite easy to setup. Furthermore, the roof of the office area (highlighted in Figure 1) is clear of any structures, providing a perfect vision for directional antennas.

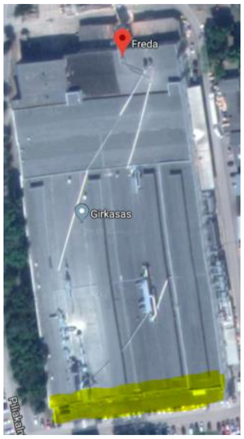


Figure 1. Satellite view of the company's Freda building

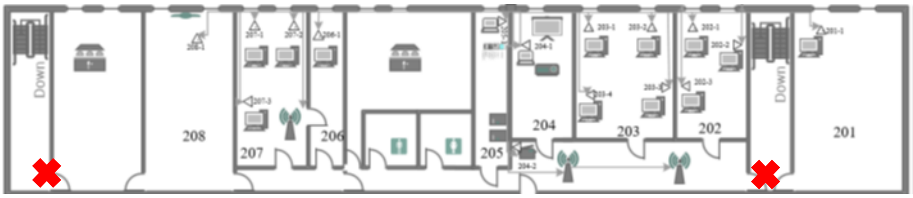


Figure 2. Camera positions

The previous decision is further supported, since the new surveillance system cannot be integrated into the existing network. The reasons behind this are to avoid a bigger network sprawl, IP address mix up for the new devices and to prevent any data overload and bottle necks. This way the video recording will be reliable, of high quality and uninterruptable. Taking all the requirements into consideration the antennas were chosen from the following three:

Figure 3. TP-LINK outdoor wireless antenna

Table 1. TP-Link antenna specification

Power:	Passive PoE 24V, 1.0A Max
Gain:	8.0 dBi
Network interface:	(1) 10/100 Ethernet port
Processor:	Qualcomm Atheros 560MHz CPU, MIPS 74Kc
Operating memory:	64MB DDR2 RAM, 8MB Flash
Frequency:	2.4 GHz
Work frequency:	2.4~2.483GHz
Supported distance:	5+ km

Figure 4. Ubiquiti NanoStation M Loco M2

Table 2. M2 antenna specification

Power:	Passive PoE 24V, 0.5A
Gain:	8.5 dBi
Network interface:	(1) 10/100 Ethernet port
Processor:	Atheros MIPS 24Kc, 400 MHz
Operating memory:	32 MB SDRAM, 8 MB Flash
Frequency:	2.4 GHz
Work frequency:	2412-2462 MHz
Supported distance:	5+ km

Figure 5. Ubiquiti NanoStation M5

Table 3. M5 antenna specification

Power:	Passive PoE 24V, 0.5A
Gain:	14.6-16.1 dBi
Network interface:	(2) 10/100 Ethernet port
Processor:	Specs Atheros MIPS 74Kc, 560 MHz
Operating memory:	64 MB DDR2, 8 MB Flash
Frequency:	5 GHz
Work frequency:	5170-5875 MHz
Supported distance:	15+ km

The specifications mate it clear that M5 model antennas would be ideal for fast, large data transfer between points needed for high resolution video streaming. But the antenna itself can only work at a 5GHz frequency, meaning that, if there was an outside noise that would interfere with the signal, there would be a risk of losing a lot of data due to the high working frequency. And while all the antennas support the new airMAX technology, they still aren’t immune to outside interference. Not to mention that the company itself already had M2 type antennas from previous project and was looking to cutting down unnecessary costs.

The decision behind using the bullet IP camera based on the fact that the company had plans to further expand the new surveillance in the future, and for a growing company the best solution for video security are the IP cameras. Plus, the bullet cameras themselves come with all sort of features like night vision, motion sensors and sound. Figure 6 shows how this camera looks like

Figure 6. Hikvision bullet camera

The choice came between three types of cameras: HIKVISION, DS-2CD2085FWD-I F4 (ref. as Hik1), Hikvision DS-2CD2455FWD-IW F2.8 (ref. asHik2) and Hikvision DS-2CD2442FWD-IW F2.8 (ref. as Hik3).

Hik1 camera has an 8-megapixel camera and a night vision mode that can see up to 30 meters in the dark. It also has the following features: intrusion detection, motion detection, line crossing detection, face recognition and object removal/appearance. The camera’s total price is EUR 189.99.

Hik2 camera has a 4-megapixel camera and a night vision mode that can see up to 10 meters in the dark. It also has the following features: intrusion detection, motion detection, line crossing detection, face recognition and object removal/appearance, integrated speakers and a microphone. The cameras total price is EUR 161.88.

Hik3 camera has a 5-megapixel camera and a night vision mode that can see up to 10 meters in the dark. It also has the following features: intrusion detection, motion detection, line crossing detection, face recognition and object removal/appearance, integrated speakers and a microphone. The cameras total price is EUR 122.64.

Based on the product features the best optimal IP camera would have been the H3 type due to its integrated features, relatively high-quality camera and the lowest cost of all the other cameras. But the company had already spare H1 type cameras from a previous project, they were used instead.

Finally, the NVR itself was recommended from the shop that provided the cameras. HikVision DS-7604NI-K1, 4 channel IP NVR, 4K resolution NVR was relatively cheap in price and it had a user friendly interface alongside various features like setting up working schedules for the cameras, creating warning rules and giving the operators a warning in case a connection between the NVR and the camera would suddenly disappear. With these choices the new surveillance system was ready to be installed.

2.5. Active Directory analysis

According to Jacoberger's (2014) article Active Directory (AD) is a system on a single device that allows the user to control the entire computer network connected to the said device. With the help of AD the devices to the network connected on the local network can become aware of each others' existence and are able to share files and data with one another, allowing access to one device using another. Furthermore, according to Heckman (2017) the use of AD allows the company to more efficiently manage user passwords, create authentication policies, create work groups and combat human errors. In terms of password management the administrator can manage complexity, length, expiration and other settings of all user passwords. This ensures that every employee complies with the company's security standards. With work groups all the users in the network can be assigned into appropriate groups that have the rights and permissions needed for the users to access data or resources. Authentication policies ensure that stored data can only be accessed by users allowed to do so. The AD can combat human errors, by using the *least privileged* method that can be used on workers who are computer illiterate and may delete or modify a file they were not supposed to. This also helps prevent clueless users from infecting sensitive data and files with viruses. (Heckman 2017.)

Now while the only method to install Active Directory on the network is to set up a server, this only helps the company by introducing new features and systems to use. According to an article by Sanassi CISSE (2017) with Windows server the networks security can be greatly increased by securing administrator credentials, implementing new attack detection features and isolating applications. Among all that, the server itself can improve the scalability and performance of the whole network grid by virtualizing new workplaces, using Hyper-V technologies to massively create new virtual devices from a template, creating backups, setting up update and control policies and so on. Additionally, new ways of managing AD than just from the server are making their way into the market. The only known other way to remotely control AD was through a remote connection to the server, but today there is software that use LDAP to allow full control of AD over a browser. Not to mention this software comes with its own features like creating reports about AD and having the option to create rule-based account creation and modification templates.

2.6. Single-board computer analysis

By Beal's (2019) definition a single-board computer is a small device that work as a regular computer but is built upon single circuit boards. A device like that often works without a conventional cooling fan due to its low power consumption. Nevertheless, these microcomputers are developing each day. According to an article by Paul (2018) most of the microcomputers nowadays run on Linux based open source operating systems, meaning that not only the microcomputer hardware is cheap, but the necessary software is free as well. And with advancing technologies and more powerful processors the single-board computers become ideal for menial tasks and network development.

2.7. Resource management system

Based on the analysis it was determined that the following technologies, methods and devices will be used to complete the resource management system:

- Raspberry microcomputer will be set up as a kiosk
- The microcomputers will have AD control software installed that will allow them to access AD though a web browser

Since it was planned to have the system installed in the furniture factory, the choice to use a single-board computer based on the fact that it consumed low power and required low maintenance. Additionally, in a busy factory size means a lot and since microcomputers are small there won't be a problem to find a place to set them up. Furthermore, for the task the device doesn't need to be a powerful one.

For the web-based AD controller it was determined that the previously mentioned computers will be also turned into an internet kiosk for regular employees to use. The kiosk work mode would render the tinkering of the device by the regular workers while supporting access to the company's AD for the IT administrators.

For this project the company had spare Raspberry Pi 3 computers as for the AD controller we had to choose from three: ADManager Plus, WebActiveDirecotry and GroupID. All of them give access to AD through a web browser. However, WebActiveDirecotry and GroupID have additional authentication features. But unlike ADManager Plus they don't have a live tech support. Additionally, because ADManager has more detailed report system and a better price range for a mid-sized company like Freda it was the chosen software for the project.

3. PROJECT IMPLEMENTATION

This chapter explains step by step the implementation of the project, what methods were used, how the software was installed, devices built and configured and how many devices the project required.

3.1. Company's network infrastructure

The very first step of the project was to get to know the company's internal network structure, which mainly consisted of the network's logical plan, physical plan and IT rack. That allowed figuring out if the network itself could expand itself with new devices.

3.2. Company’s network logical plan

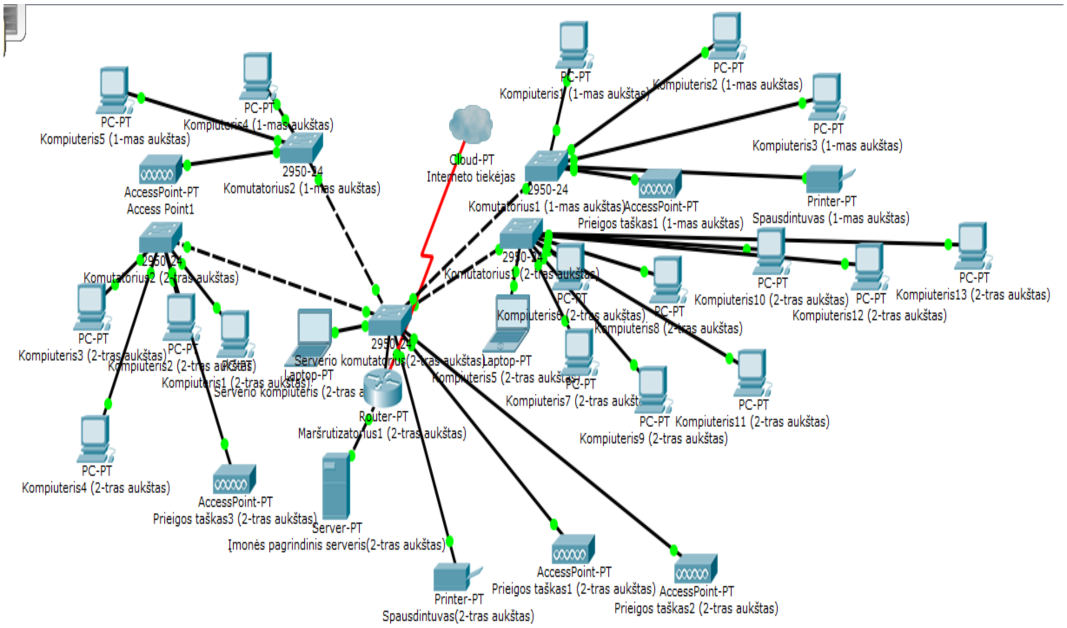
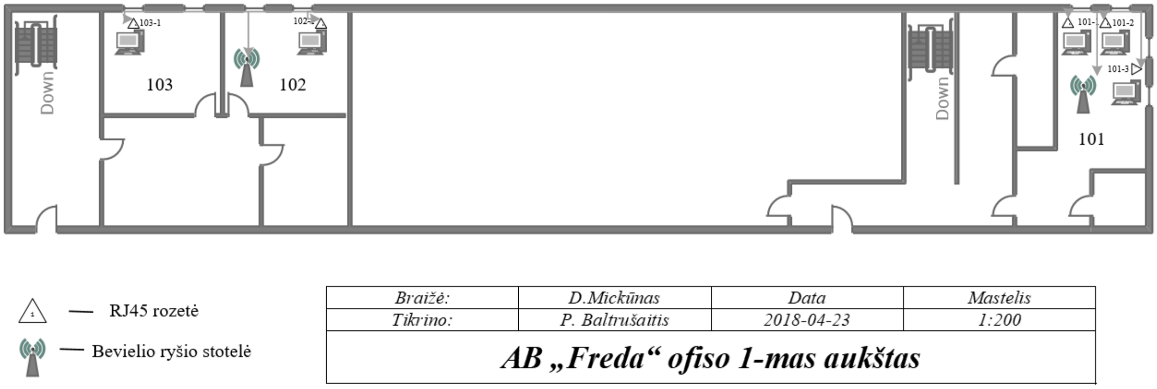

PC-PT
Kompiuteris5 (1-mas aukštas)
PC-PT
Kompiuteris4 (1-mas aukštas)
2950-24
Komutatorius2 (1-mas aukštas)
AccessPoint-PT
Access Point1
2950-24
Komutatorius2 (2-tras aukštas)
PC-PT
Kompiuteris3 (2-tras aukštas)
PC-PT
Kompiuteris2 (2-tras aukštas)
PC-PT
Kompiuteris1 (2-tras aukštas)
PC-PT
Kompiuteris4 (2-tras aukštas)
AccessPoint-PT
Prieigos taškas3 (2-tras aukštas)
Laptop-PT
Serverio kompiuteris (2-tras a
2950-24
Serverio komutatorius(2-tras aukštas)
Router-PT
Maršrutizatorius1 (2-tras aukštas)
Server-PT
Įmonės pagrindinis serveris(2-tras aukštas)
Printer-PT
Spausdintuvas(2-tras aukštas)
Cloud-PT
Interneto tiekėjas
PC-PT
Kompiuteris1 (1-mas aukštas)
PC-PT
Kompiuteris2 (1-mas aukštas)
PC-PT
Kompiuteris3 (1-mas aukštas)
2950-24
Komutatorius1 (1-mas aukštas)
AccessPoint-PT
Prieigos taškas1 (1-mas aukštas)
Printer-PT
Spausdintuvas (1-mas aukštas)
2950-24
Komutatorius1 (2-tras aukštas)
Laptop-PT
Kompiuteris5 (2-tras aukštas)
PC-PT
Kompiuteris6 (2-tras aukštas)
PC-PT
Kompiuteris7 (2-tras aukšt
PC-PT
Kompiuteris8 (2-tras aukštas)
PC-PT
Kompiuteris9 (2-tras aukštas)
PC-PT
Kompiuteris10 (2-tras aukštas)
PC-PT
Kompiuteris11 (2-tras aukštas)
PC-PT
Kompiuteris12 (2-tras aukštas)
PC-PT
Kompiuteris13 (2-tras aukštas)
AccessPoint-PT
Prieigos taškas1 (2-tras aukštas)
AccessPoint-PT
Prieigos taškas2 (2-tras aukštas)

Figure 7. Logical plan

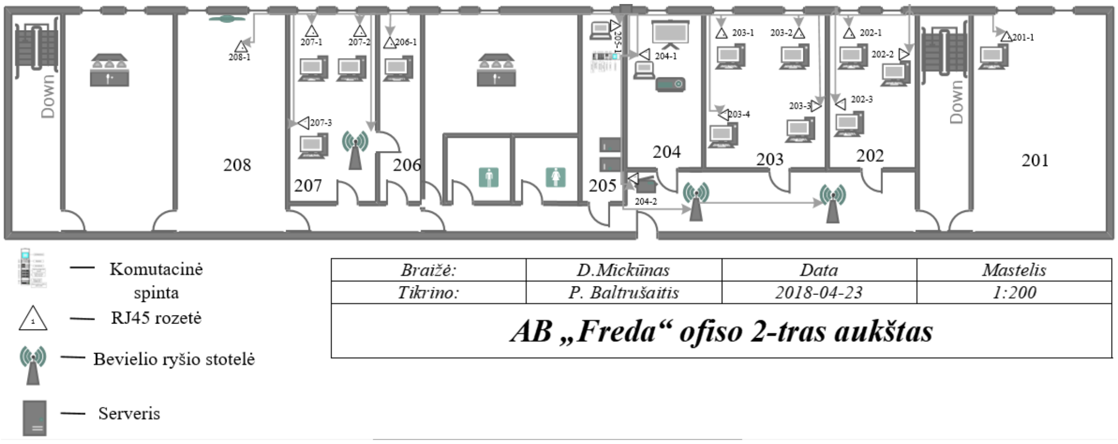
The plan indicates that all devices are connected to the company server (server network) and that every office had its own switch giving connection to the end devices. These switches were more than enough for the offices, so they were able to support additional devices.

3.3. Company’s network physical plan



Braižė:	D.Mickūnas	Data	Mastelis
Tikrino:	P. Baltrušaitis	2018-04-23	1:200
AB „Freda“ ofiso 1-mas aukštas			

Figure 8. 1st floor plan



Braižė:	*D.Mickūnas*	*Data*	*Mastelis*
Tikrino:	*P. Baltrušaitis*	*2018-04-23*	*1:200*
AB „Freda“ ofiso 2-tras aukštas			

Figure 9. 2nd floor plan

The physical plan showed how the cables are routed through the building and precise location of every end device in the area. The plan helped decide which spot would be ideal for the expansion as not to cramp the offices or set up in an area that is not meant for electronic devices.

3.4. IT rack

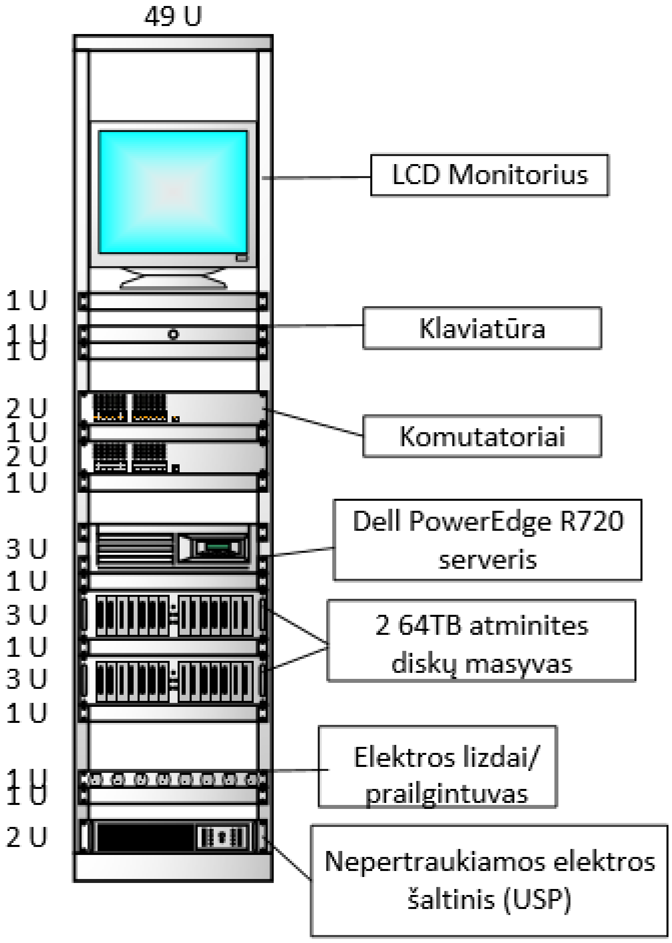

49 U
1 U
1 U
1 U
2 U
1 U
2 U
1 U
3 U
1 U
3 U
1 U
3 U
1 U
1 U
1 U
2 U
LCD Monitorius
Klaviatūra
Komutatoriai
Dell PowerEdge R720 serveris
2 64TB atminites diskų masyvas
Elektros lizdai/ prailgintuvas
Nepertraukiamos elektros šaltinis (USP)

Figure 10. Company's IT rack

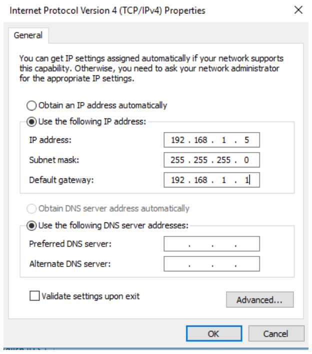
The rack was fully developed to support and provide for the company's needs, with more than enough resources and space to scale the network and add a few more end devices.

3.5. Company's network expansion

From the information gathered in the previous points the conclusion is that the network is capable of scaling and adding new, configured end devices to it without much of a drawback when it comes to space and connectivity.

3.6. New surveillance network installation and configuration

To establish video surveillance, we first had to ensure that the connection between the two Wi-Fi antennas that we have is stable. For that task we had to configure one antenna to be an access point and the other to be a station. We started off by firstly connecting one of the antennas to a local laptop and changing the computer's IP address so they would be in the same subnet (in this case it's 192.168.1.x) as the antenna, so that a direct connect to it could be established. The process of it can be seen in Figure 11.


Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 5

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

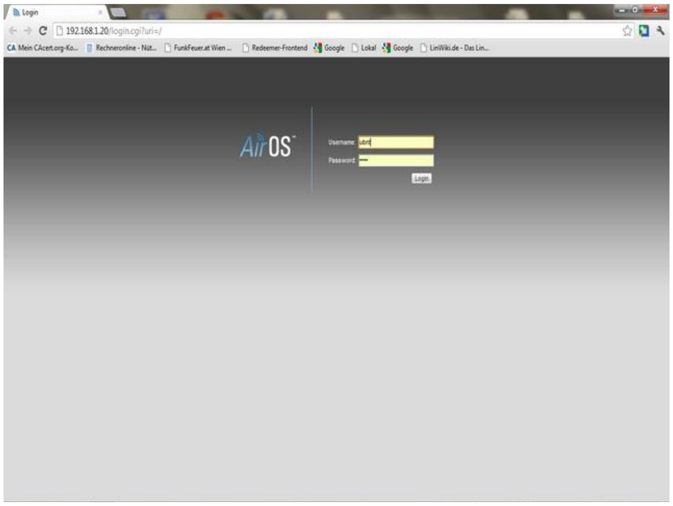
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 11. NIC configuration

After doing the first step, the second step was to open a browser on the laptop and enter the antenna's IP address (in the instruction manual it was 192.168.1.20) into the search bar. Doing that opened the login screen to the device's configuration controls. And since we had reset both antennas, their logins were set back to factory defaults, which were *ubnt* for username and password as shown in Figure 12.

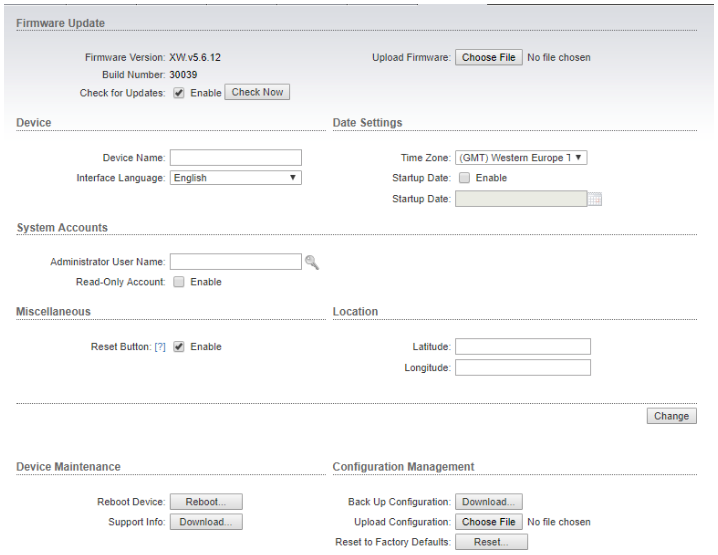

192.168.1.20/login.cgi?uri=/

Username: ubnt

Password: ••••

Figure 12. Antenna Login screen

Before making any real configurations to the wireless devices, their firmware had to be updated first. For that to happen the antennas' initial firmware was saved on the laptop that was used to connect to them. The action was important to prevent the devices' total failure in case of an error during the update. After that the official new firmware was downloaded from the site described in the instruction manual. Once we had the newest firmware the devices were quickly updated from their control panel over the browser.



Firmware Update

Firmware Version: XW.v5.6.12
Build Number: 30039
Check for Updates: ☑ Enable
Upload Firmware: No file chosen

Device

Device Name:
Interface Language: English

Date Settings

Time Zone: (GMT) Western Europe T
Startup Date: □ Enable
Startup Date:

System Accounts

Administrator User Name:
Read-Only Account: □ Enable

Miscellaneous

Reset Button: [?] ☑ Enable

Location

Latitude:
Longitude:

Device Maintenance

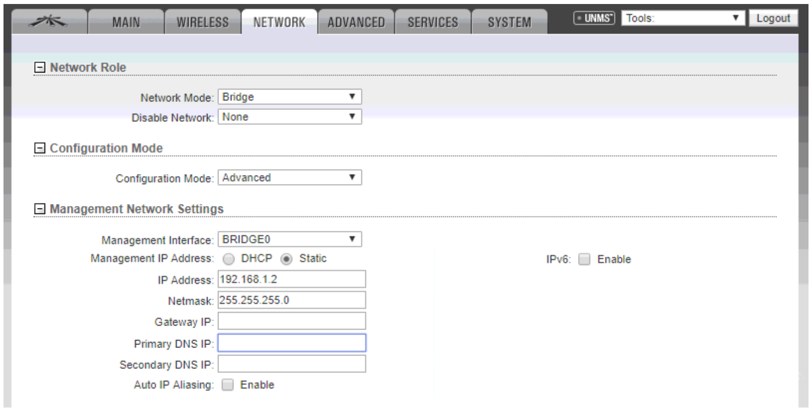
Reboot Device:
Support Info:

Configuration Management

Back Up Configuration:
Upload Configuration: No file chosen
Reset to Factory Defaults:

Figure13. Antenna System tab

Once both the devices were properly updated it was time to give each device a role in the connection. In the network tab each antenna got their own IP addresses (192.168.1.2 for access point and 192.168.1.3 for station). The network model was left in bridge mode since both devices needed to remain in the same network. After that, each of them had their default gateway set to 192.168.1.1.



⊟ Network Role

Network Mode: Bridge

Disable Network: None

⊟ Configuration Mode

Configuration Mode: Advanced

⊟ Management Network Settings

Management Interface: BRIDGE0

Management IP Address: ○ DHCP ● Static

IPv6: □ Enable

IP Address: 192.168.1.2

Netmask: 255.255.255.0

Gateway IP:

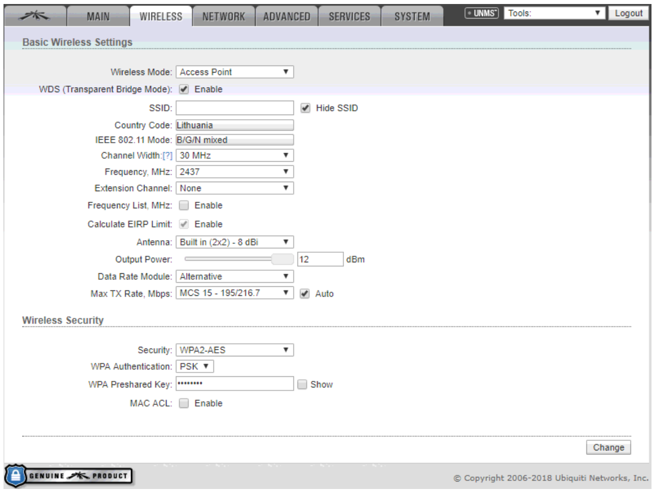
Primary DNS IP:

Secondary DNS IP:

Auto IP Aliasing: □ Enable

Figure 14. Antenna’s Network tab

After optimizing the antennas, it was time to set the wireless connection type, security and set up the password for the signal. The antenna (that will be) connected to a switch that was linked with the recording system was given access point mode, while in analog the antenna (that will be) connected directly to a camera was set to act as a station. Each device was given the same password for the signal as not to create conflict when, it comes to authenticating each other as a trusted device.



Basic Wireless Settings

Wireless Mode: Access Point

WDS (Transparent Bridge Mode): ☑ Enable

SSID: ☑ Hide SSID

Country Code: Lithuania

IEEE 802.11 Mode: B/G/N mixed

Channel Width:[?] 30 MHz

Frequency, MHz: 2437

Extension Channel: None

Frequency List, MHz: □ Enable

Calculate EIRP Limit: ☑ Enable

Antenna: Built in (2x2) - 8 dBi

Output Power: 12 dBm

Data Rate Module: Alternative

Max TX Rate, Mbps: MCS 15 - 195/216.7 ☑ Auto

Wireless Security

Security: WPA2-AES

WPA Authentication: PSK

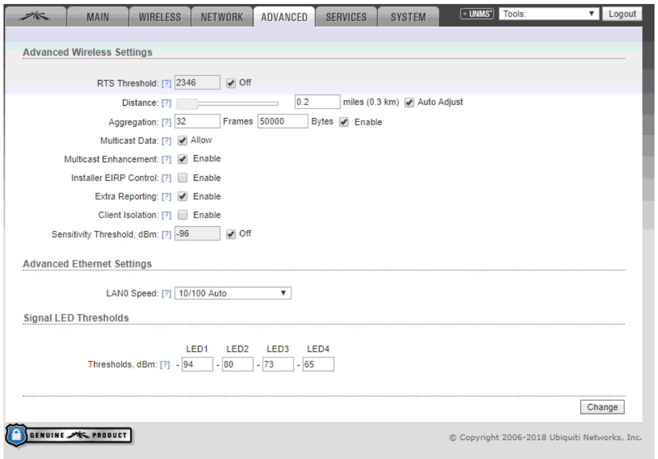
WPA Preshared Key: •••••••• □ Show

MAC ACL: □ Enable

Change

© Copyright 2006-2018 Ubiquiti Networks, Inc.

Figure 15. Antenna’s Wireless tab



Advanced Wireless Settings

RTS Threshold: [?] 2346 ☑ Off
Distance: [?] 0.2 miles (0.3 km) ☑ Auto Adjust
Aggregation: [?] 32 Frames 50000 Bytes ☑ Enable
Multicast Data: [?] ☑ Allow
Multicast Enhancement: [?] ☑ Enable
Installer EIRP Control: [?] □ Enable
Extra Reporting: [?] ☑ Enable
Client Isolation: [?] □ Enable
Sensitivity Threshold, dBm: [?] -96 ☑ Off

Advanced Ethernet Settings

LAN0 Speed: [?] 10/100 Auto

Signal LED Thresholds

	LED1	LED2	LED3	LED4
Thresholds, dBm: [?]	- 94	- 80	- 73	- 65

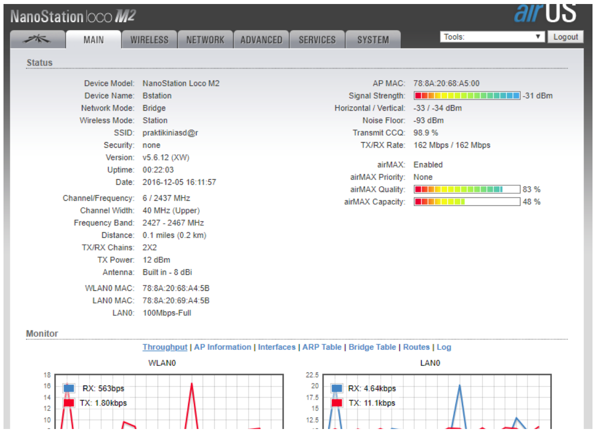
Change

© Copyright 2006-2018 Ubiquiti Networks, Inc.

Figure 16. Antenna’s Advanced tab.

To further increase the security of the connection in the *Wireless* tab both antennas were given a name (SSID) that were hidden to prevent anyone from accessing the devices with a wireless connection. Then moving to the *Advanced* tab, the distance between the devices was set to 200m, the distance between their planned locations, so that, both devices could optimize their power by themselves. Lastly, both devices received new login information in the *Main* tab in case an unauthorized person would try to login to them with a direct link (Ethernet cable).

After all the configuration was done the connection quality between the two devices can be checked in the *Main* tab (seen in Figure 17) that displays a diagram and information about the parameters of the antenna, signal strength and bandwidth speed if there is a data transfer between the two antennas.



Status

Device Model:	NanoStation Loco M2	AP MAC:	78:8A:20:68:A5:00
Device Name:	Bstation	Signal Strength:	-31 dBm
Network Mode:	Bridge	Horizontal / Vertical:	-33 / -34 dBm
Wireless Mode:	Station	Noise Floor:	-93 dBm
SSID:	praktikiniasd@r	Transmit CCQ:	98.9 %
Security:	none	TX/RX Rate:	162 Mbps / 162 Mbps
Version:	v5.6.12 (XW)		
Uptime:	00:22:03	airMAX:	Enabled
Date:	2016-12-05 16:11:57	airMAX Priority:	None
Channel/Frequency:	6 / 2437 MHz	airMAX Quality:	83 %
Channel Width:	40 MHz (Upper)	airMAX Capacity:	48 %
Frequency Band:	2427 - 2467 MHz		
Distance:	0.1 miles (0.2 km)		
TX/RX Chains:	2X2		
TX Power:	12 dBm		
Antenna:	Built in - 8 dBi		
WLAN0 MAC:	78:8A:20:68:A4:5B		
LAN0 MAC:	78:8A:20:69:A4:5B		
LAN0:	100Mbps-Full		

Monitor

Throughput | AP Information | Interfaces | ARP Table | Bridge Table | Routes | Log

Figure 17. Antenna’s Main tab

After setting up the antennas we configured the cameras. Camera configuration is similar to antenna configuration. It, too, needs to connect to a laptop before typing the default IP address and entering the control panel login (as shown in figure 18. Username was admin and password was 12345). Once the control panel is opened, we immediately go to *Live view* to check, if the cameras are recording without any defects or errors. If everything is optimal, we proceed to the next step, which is to give the cameras their own IP addresses that are in the same subnet as the antennas and NVR, in the *Configuration* tab (shown in figure 19).

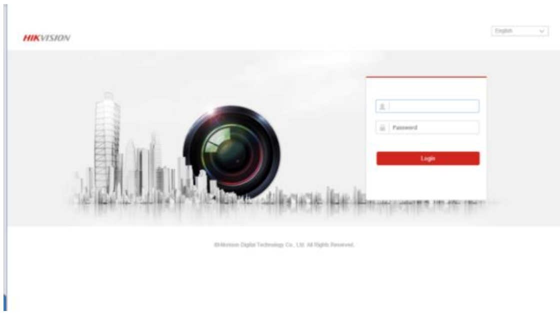
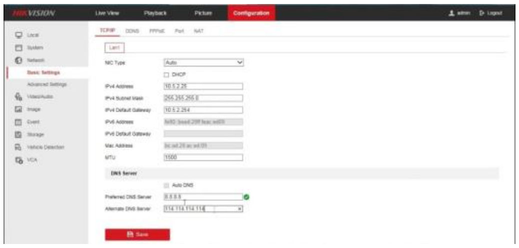

HIKVISION
English
Password
Login
©Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Figure 18. Camera’s login screen

After the quick configuration is done both cameras get new logins to prevent unwanted access from unauthorized people.



NIC Type: Auto
□ DHCP
IPv4 Address: 10.5.2.26
IPv4 Subnet Mask: 255.255.255.0
IPv4 Default Gateway: 10.5.2.254
IPv6 Address: [illegible]
IPv6 Default Gateway:
Mac Address: [illegible]
MTU: 1500

DNS Server

□ Auto DNS
Preferred DNS Server: 8.8.8.8
Alternate DNS Server: 114.114.114.114

Figure 19. Camera’s Configuration tab

The next step was NVR. Because NVR did not come with its own data storage unit, thus one needed to be installed by hand (seen in Figure 20). And before any changes could be done to the recorder, we first had to format the new disk. The process was easy since once turned on the device itself offered to format the new hard drive.

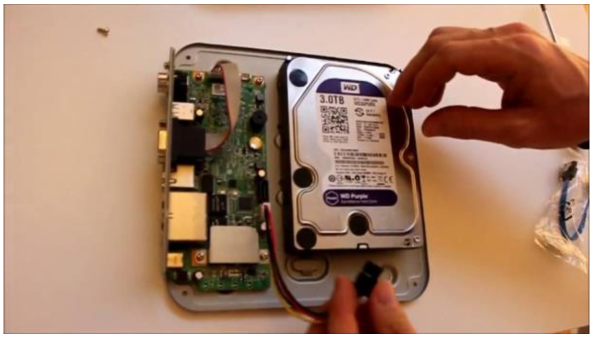
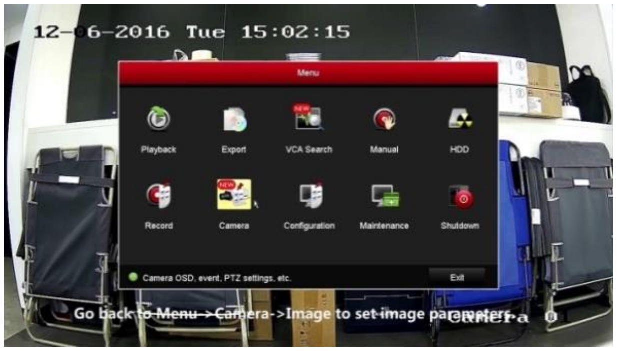


Figure 20. Hard drive installation

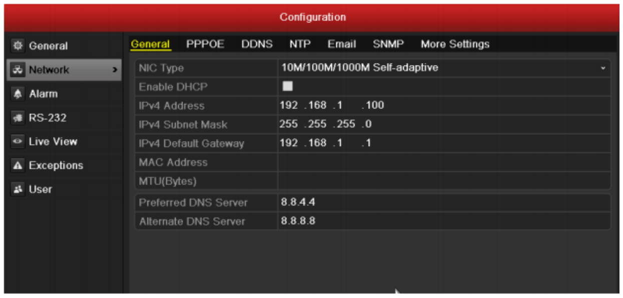
After the disk formatting the device can be properly turned on. Once booted, the device itself requires that the default login information is changed to prevent unauthorized access. Once that is done, the recorder needs to get a new IP address that is in the same subnet as the cameras and antennas and have the same gateway, so the connection could be established between all of them.



Camera OSD, event, PTZ settings, etc.

Go back to Menu->Camera->Image to set image parameters

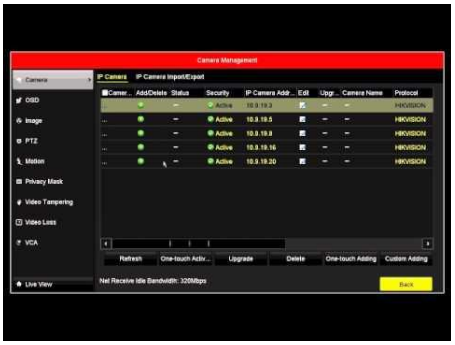
Figure 21. NVR main menu



NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	□
IPv4 Address	192 .168 .1 .100
IPv4 Subnet Mask	255 .255 .255 .0
IPv4 Default Gateway	192 .168 .1 .1
MAC Address	
MTU(Bytes)	
Preferred DNS Server	8.8.4.4
Alternate DNS Server	8.8.8.8

Figure 22. NVR configuration window

When the IP address configuration was done, we had to link cameras with the video recording system. If all the devices are in one subnet then the NVR finds and connects the cameras itself, but in case that doesn't happen it is possible to *custom add* camera IP to the list in *Camera Management* tab.



Camer...	Add/Delete	Status	Security	IP Camera Addr...	Edit	Upgr...	Camera Name	Protocol
...	●	–	Active	10.9.19.3		–	–	HIKVISION
...	●	–	Active	10.9.19.5		–	–	HIKVISION
...	●	–	Active	10.9.19.8		–	–	HIKVISION
...	●	–	Active	10.9.19.16		–	–	HIKVISION
...	●	–	Active	10.9.19.20		–	–	HIKVISION

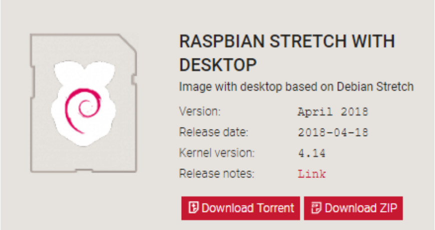
Net Receive Idle Bandwidth: 320Mbps

Figure 23. NVR Camera configuration window

Finally, after setting up and configuring all the end devices everything can be installed in their rightful places. Antennas went on to the roof of the office with special poles that provided them a clear sight with no objects blocking a direct signal to one another. Then the power injectors got plugged in and data ports between the farthest camera and antenna were connected ,so that the signal would stream the recorded video as data.

3.7. Active Directory control system installation and setup

To prepare the Raspberry computer it first needed a proper operating system (shown in Figure 24) to be downloaded from the official site Raspberry OS site. Since Raspberry single-board computers don't have any other data storage besides a memory card, it was important to make sure that the card would be formatted and then act as a boot device for the machine. For that to happen we had to use an adapter to connect the memory card to a laptop where we then used programs like *Etcher* (shown in Figure 25) and *SD Card Formatter* to perform necessary configurations to ensure smooth OS installation to the computer.



RASPBIAN STRETCH WITH DESKTOP

Image with desktop based on Debian Stretch

Version:	April 2018
Release date:	2018-04-18
Kernel version:	4.14
Release notes:	Link

Figure 24. Raspberry OS

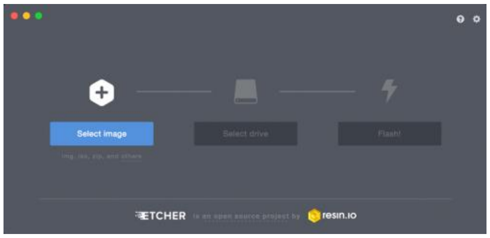


Figure 25. Etcher software

Once the card is inserted into the appropriate slot the device was then booted and by default the Pi computer started to install the OS on its own. In a few minutes the desktop of the machine appeared on the screen (seen in Figure 26), indicating a successful installation.

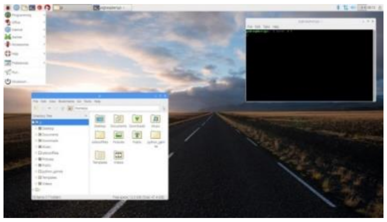
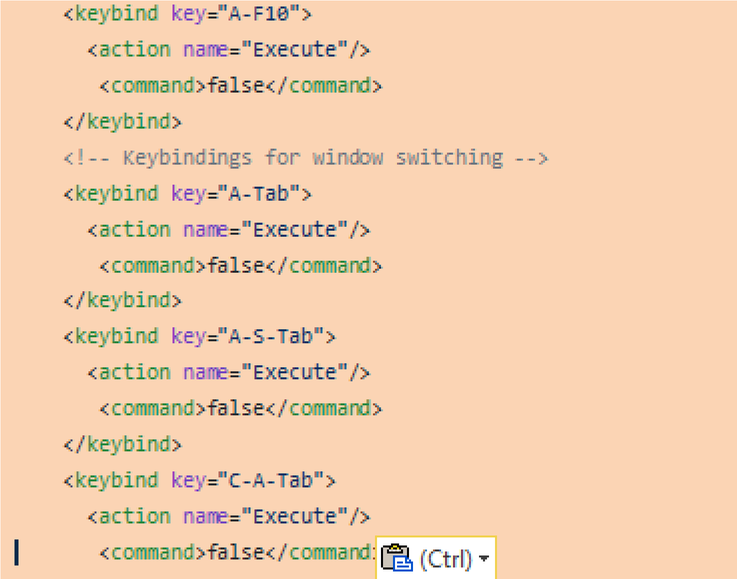


Figure 26. Raspberry desktop

Once the single-board was set for use we then had to configure it. For an interactive terminal we first had to disable all known keyboard shortcuts (key combinations involving *ALT* and *CTRL* buttons) to make sure the user wouldn't be able to get out of the kiosk mode. For that we first had to configure the device's keyboard control file, and since it was a kernel based OS we modified the needed file with the *sudo nano ~/.config/openbox/lxde-rc.xml* command in the terminal. Now this file also controlled mouse and other things, the segment of the code needed was between *<keyboard> part* and *</keyboard>*. In that code part we changed every *action name* to have the value of *execute* before adding another line below it with *<command>false</command>* that made sure any keyboard shortcut fails to work as intended. In addition, if any action name was already equal to *execute,* we simply had to change whatever was between the *command* lines to *false* (as shown in Figure 27).

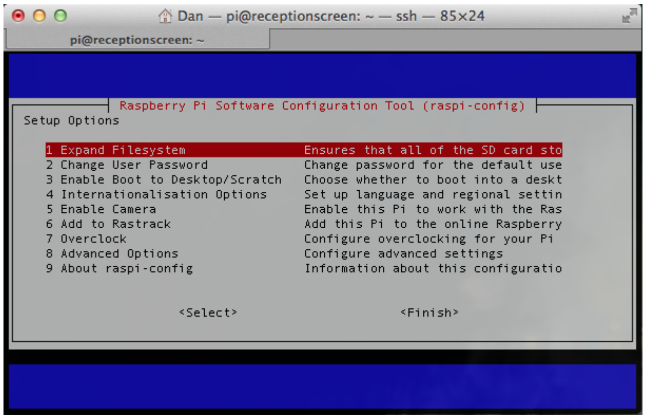


```
<keybind key="A-F10">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<!-- Keybindings for window switching -->
<keybind key="A-Tab">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<keybind key="A-S-Tab">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<keybind key="C-A-Tab">
  <action name="Execute"/>
   <command>false</command
```

Figure 27. Keyboard control file

After limiting the controls of the keyboard, we moved to configuring the computer itself, so it would work as a kiosk, that is, on startup it would launch a browser in full screen and wouldn’t let the user to anything else but use the internet. Firstly, we updated the Raspberry device with the *sudo apt-get update && sudo apt-get upgrade –y* command in the terminal.

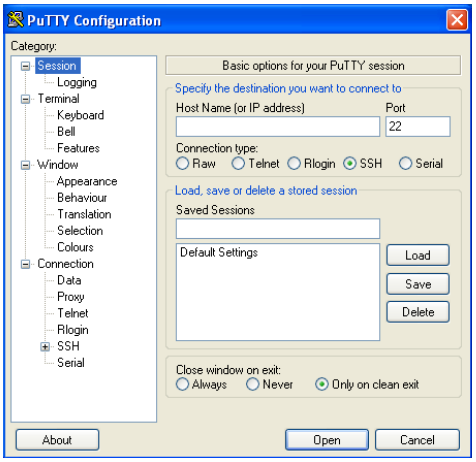
After the last step we moved on to enable SSH connection to the future kiosk. The reason behind it is that, once the computer is turned into a kiosk, it will limit any sort of other access besides access to a web browser and the internet. Since we will need to configure the device, the best way to do it would be a remote connection from another computer. For that to happen we configured the Pi computer software with the command *sudo raspi-config.* In the configuration tool (shown in Figure 28) we then activated the 22 port (SSH port).



```
Raspberry Pi Software Configuration Tool (raspi-config)
Setup Options

  1 Expand Filesystem                  Ensures that all of the SD card sto
  2 Change User Password               Change password for the default use
  3 Enable Boot to Desktop/Scratch     Choose whether to boot into a deskt
  4 Internationalisation Options       Set up language and regional settin
  5 Enable Camera                      Enable this Pi to work with the Ras
  6 Add to Rastrack                    Add this Pi to the online Raspberry
  7 Overclock                          Configure overclocking for your Pi
  8 Advanced Options                   Configure advanced settings
  9 About raspi-config                 Information about this configuratio

                <Select>                         <Finish>
```

Figure 28. Raspberry configuration window

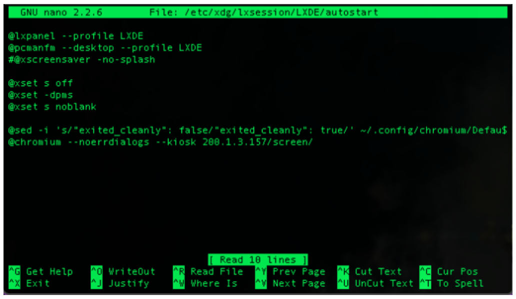
Once the SSH connection was enabled the kiosk was then connected to a laptop that had *Putty* software (shown in Figure 29) installed. The software was needed for an easy SSH access to the device that we proceeded to work on using a terminal and command lines on the laptop.



Host Name (or IP address):
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 29. Putty software

Finally, we set up the single-board computer to start up as a proper kiosk by editing the startup script in its files with the *sudo nano /etc/xdg/lxsession/LXDE/autostart* command. In the file we had to specify that the computer would not turn on its screen saver after a period of inactivity by commenting (adding # symbol in front) the *@xscreensaver -no-splash* command. The next step is to turn off the computer's sleep mode and power saving mode that includes turning off the screen after a set time of inactivity by adding the *@xset s off*, *@xset –dpms* and *@xset s noblank* commands (shown in Figure 30).



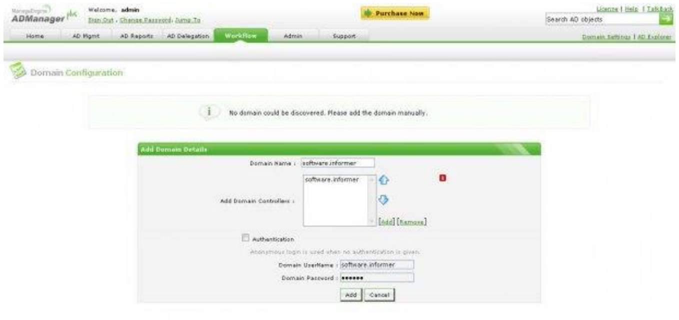
```
  GNU nano 2.2.6          File: /etc/xdg/lxsession/LXDE/autostart

@lxpanel --profile LXDE
@pcmanfm --desktop --profile LXDE
#@xscreensaver -no-splash

@xset s off
@xset -dpms
@xset s noblank

@sed -i 's/"exited_cleanly": false/"exited_cleanly": true/' ~/.config/chromium/Defau$
@chromium --noerrdialogs --kiosk 200.1.3.157/screen/







                                  [ Read 10 lines ]
^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

Figure 30. Raspberry auto start file

With the last command the kiosk opens a web browser in kiosk mode with a set default home page. Additionally, the line specified that the device mustn't show any error messages. For that to happen we simply added *@chromium --noerrdialogs --kiosk http://www.google.lt* line at the end of the script.

Once the kiosk was set we prepared the device for use. The AD control software is firstly downloaded from the official ADManager AD controller site . The program itself is called ADManager plus and allows full access and control of local Windows Server AD from a web browser from any computer that has the program installed and configured for it.

Once the controller is installed, we launch it on the device and after some time it opens up a default browser and directs the user to the control panel. From the very start the program requires to link the server domains name (shown in figure 31), in case the network has more than 1 server, before requesting to log in with a user that is already created in AD and has the rights to configure it.



No domain could be discovered. Please add the domain manually.

Add Domain Details

Domain Name : software.informer

Add Domain Controllers : software.informer

□ Authentication

Anonymous login is used when no authentication is given.

Domain UserName : software.informer

Domain Password : ••••••

Figure 31. ADManager AD Domain linking

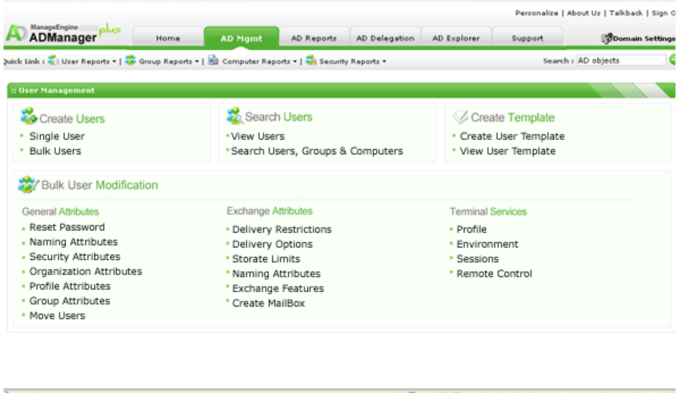


Figure 32. ADManager AD control tab

The same steps are done with any other device that needs to have a web browser access to the local AD. This software is supported by Linux, hence why they were installed and setup on the previously mentioned Raspberry Pi3 computers before they were turned into kiosks. The address for the control panel does not differ and goes by *localhost:8080* in the address bar.

3.8. Network after the project

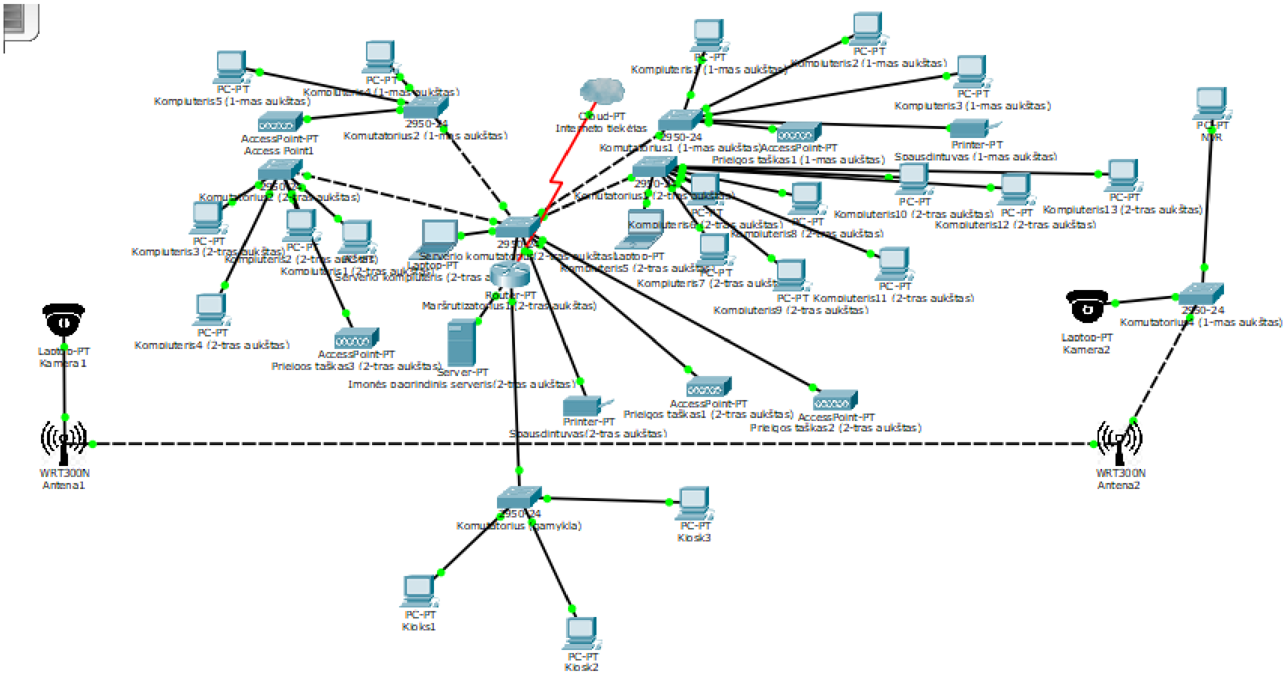

PC-PT
Kompiuteris5 (1-mas aukštas)
PC-PT
Kompiuteris4 (1-mas aukštas)
AccessPoint-PT
Access Point1
2950-24
Komutatorius2 (1-mas aukštas)
Cloud-PT
Interneto tiekėtas
PC-PT
Kompiuteris1 (1-mas aukštas)
PC-PT
Kompiuteris2 (1-mas aukštas)
PC-PT
Kompiuteris3 (1-mas aukštas)
2950-24
Komutatorius1 (1-mas aukštas)
AccessPoint-PT
Prieigos taškas1 (1-mas aukštas)
Printer-PT
Spausdintuvas (1-mas aukštas)
PC-PT
NVR
2950-24
Komutatorius2 (2-tras aukštas)
PC-PT
Kompiuteris3 (2-tras aukštas)
PC-PT
Kompiuteris2 (2-tras aukštas)
PC-PT
Kompiuteris1 (2-tras aukštas)
Laptop-PT
Serverio kompiuteris (2-tras aukštas)
2950-24
Serverio komutatorius (2-tras aukštas)
2950-24
Komutatorius1 (2-tras aukštas)
Laptop-PT
Kompiuteris6 (2-tras aukštas)
PC-PT
Kompiuteris8 (2-tras aukštas)
PC-PT
Kompiuteris10 (2-tras aukštas)
PC-PT
Kompiuteris12 (2-tras aukštas)
PC-PT
Kompiuteris13 (2-tras aukštas)
Laptop-PT
Kompiuteris5 (2-tras aukštas)
PC-PT
Kompiuteris7 (2-tras aukštas)
PC-PT
Kompiuteris9 (2-tras aukštas)
PC-PT
Kompiuteris11 (2-tras aukštas)
Router-PT
Maršrutizatorius1 (2-tras aukštas)
PC-PT
Kompiuteris4 (2-tras aukštas)
AccessPoint-PT
Prieigos taškas3 (2-tras aukštas)
Server-PT
Imonės pagrindinis serveris(2-tras aukštas)
Printer-PT
Spausdintuvas(2-tras aukštas)
AccessPoint-PT
Prieigos taškas1 (2-tras aukštas)
AccessPoint-PT
Prieigos taškas2 (2-tras aukštas)
Laptop-PT
Kamera1
Laptop-PT
Kamera2
2950-24
Komutatorius4 (1-mas aukštas)
WRT300N
Antena1
WRT300N
Antena2
2950-24
Komutatorius (gamykla)
PC-PT
Kiosk3
PC-PT
Kioks1
PC-PT
Kiosk2

Figure 33. Company’s logical plan after the project

The company’s network after the project has three new devices connected to the already existing server network, since all of them need a direct link to the server to run the AD controller properly. The network also has a new separate network next to the server network, dedicated for the CCTV. That way any bottle neck for data, interference and load on the cables is separated from the security footage.

3.9. Local estimate

Table 4. Local estimates

Name	Unit of measurement	Amount
Cat5 B category cable	m.	500
RJ45 plugs for Cat5 cables	unit	100
Protection for RJ45 plugs	unit	100
Antenna’s	unit	2

Camera’s	unit	2
Video recording system	unit	1
Raspberry Pi3 computer	unit	3
PoE injector	unit	4
„Dell“ computer	unit	1
Operating system	unit	3
Active Directory control software	unit	1
Setup work	h.	217,5

This local estimate has all the information about how many devices, parts, hardware, software and work hours were needed for the project. It will later on be used in finance part of the document to calculate approximate cost of the whole task.

4. FINANCIAS

This financing part of the project introduces the exact values of price, labor and equipment.

4.1. Equipment requirements

Table 4. Equipment requirement

Name	**Amount**	**Unit of measurement**
1. Hardware		
1.1. Cameras	2	unit
1.2. UTP cables	500	m
1.3. Network video recorder	1	unit
1.4. Antennas	2	unit
1.5. Cable head protectors	100	unit
1.6. UTP cable heads	100	unit
1.7. Computers	4	unit
1.8. PoE injectors	4	unit

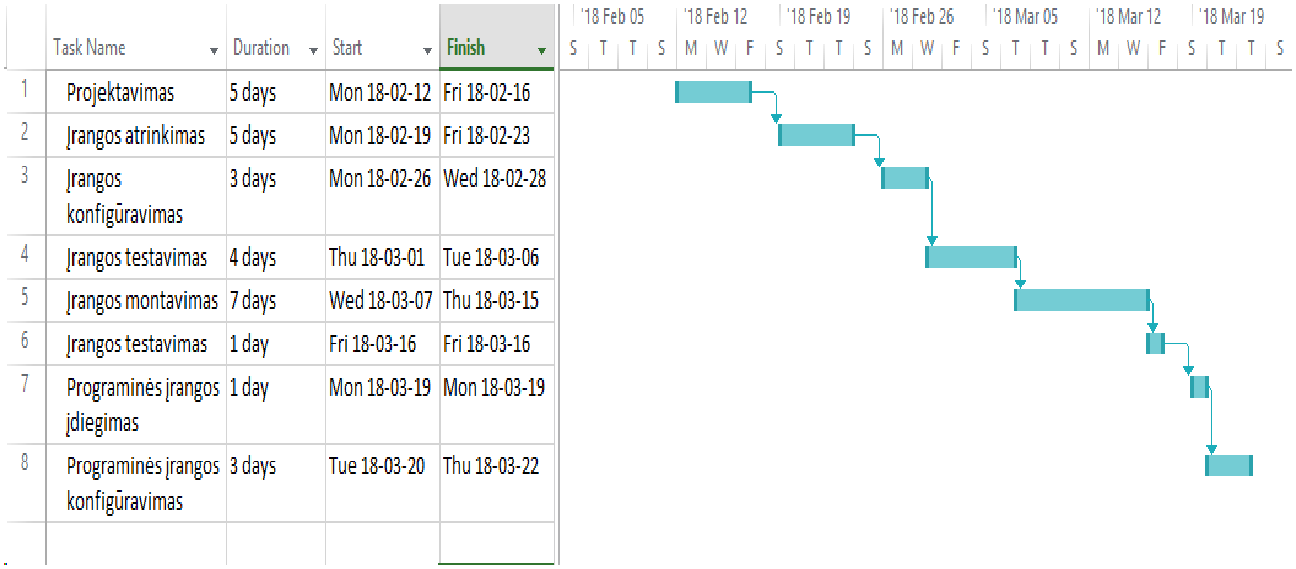
2. Software		
2.1. Active Directory controller	1	unit
2.2. Operating system	1	unit

4.2. Hardware and software estimate

5. Table 5. Equipment price

Name	**Price, euro (€)**	**Unit of measurement**	**Amount**	**Total, euro (€)**
1. Hardware				
1.1. 8-megapixel IP camera HIKVISION, DS-2CD2085FWD-I F4	**189,99**	unit	**2**	**379,98**
1.2. CAT5 UTP cable	**0,45**	m.	**500**	**225,00**
1.3. HikVision DS-7604NI-K1, 4 channel IP NVR, 4K resolution NVR.	**161,88**	unit	**1**	**161,88**
1.4. Ubiquiti nanostation locom2 antennas	**35,27**	unit	**2**	**70,54**
1.5. Cable head protectors, 4,8 x 290 mm	**0,05**	unit	**100**	**5,00**
1.6. UTP cable heads	**0,13**	unit	**100**	**13,00**
1.7. Computer „Dell“	**349,00**	unit	**1**	**349,00**
1.8. Raspberry Pi 3 microcomputer	**69,00**	unit	**3**	**207,00**
1.9. POE-12V48 Power Over Ethernet for IP Camera, PoE Midspan Injector	**29,99**	unit	**4**	**119,96**
2. Software				
2.1. ADManager	**496,16**	unit	**1**	**496,16**
2.2. Windows 7 „Professional“	**44,98**	unit	**1**	**44,98**

5.1. Projects work diagram (Gnatto diagram) and work hours



	Task Name	Duration	Start	Finish
1	Projektavimas	5 days	Mon 18-02-12	Fri 18-02-16
2	Įrangos atrinkimas	5 days	Mon 18-02-19	Fri 18-02-23
3	Įrangos konfigūravimas	3 days	Mon 18-02-26	Wed 18-02-28
4	Įrangos testavimas	4 days	Thu 18-03-01	Tue 18-03-06
5	Įrangos montavimas	7 days	Wed 18-03-07	Thu 18-03-15
6	Įrangos testavimas	1 day	Fri 18-03-16	Fri 18-03-16
7	Programinės įrangos įdiegimas	1 day	Mon 18-03-19	Mon 18-03-19
8	Programinės įrangos konfigūravimas	3 days	Tue 18-03-20	Thu 18-03-22

Figure 34. Project’s time diagram (Gnatto diagram)

Table 6. Work time

Jobs	**Hours spent (h)**
Projection	37.5
Device selection	37.5
Device configuration	22.5
Device testing	30
Device setup	52.5
Device testing	7.5
Software installation	7.5
Software configuration	22.5
Total:	217.5

Gnatto diagram showcases precise timeline of the project (duration of workdays and in what weeks the project took place) as well as indicating the workflow.

5.2. Project developer’s labor costs

1. Calculation of hourly rate:

Deividas monthly pay (before taxes (euro) / 21 workdays (on average) / 7,5 work hours = hourly pay (euro)

Deividas monthly pay (before taxes) = **EUR 700**

1 200 (euro) / 21 (workdays) / 7,5 (work hours) = **EUR 4.44**

2. Brutto pay, regarding project preparation time:

Hourly pay (EUR) x project execution time (val.) = costs of the project developer (EUR)

4,44 (euro) * 217 (val.) = **EUR 963.48**

3. Calculation of costs of the project developer:

Project developer salary costs + employer social security contributions (30,98%) + Employer's contributions to the guarantee fund (excluding state budget institutions, municipal budget institutions) – (0,2 %)

963,48 + 298,49 + 1,93 = **EUR 1263.90**

4. Netto pay calculation:

Deividas pay, regarding project preparation time – income tax (15%) –health insurance (6%) – pension (3%))

963,48 – 144,52 – 86,71 = **EUR 752.25**

5.3. Projects estimate

6. Table 7. Projects estimate

Nr.	**Name**	**Price, euro (€)**
1	**Project implementation costs**	
1.1.	Hardware	**1531.37**
1.2.	Software	**541.14**
1.3.	Salaries	**1263.90**
Total:		**3336.41**
2	**Projects monthly upkeep**	
2.1.	Hardware	**351 / 1 a month**
2.2.	Software	**41.35 / 1 a month**

2.3.	Salaries	**700 / 1 a month**
Total:		**1092.35 / 1 a month**
3.	**Administrative costs (10%)**	**333.64 + 109.23/ 1 a month**
Projects total:		**3670.05+ 1201.58 / 1 a month**

Pricing of the project to the customer will be EUR 3670.05 initially and EUR 1201.58 every month. Out of the initial cost EUR 2072.51 were used on the project’s hardware and software while EUR 1263.90 were paid in salaries.

7. CONCLUSIONS

The goal of the thesis was to create a new surveillance network and new resource management of the networks Active Directory using web browser interface.

The security solution was implemented using IP cameras with built in motion sensors and night vision capabilities. Additionally, for long range connection between the devices a Wi-Fi connection was used with antennas that were able to handle the high data stream requirements and mitigate security risks such as unauthorized connection to the signal or even signal jamming. Furthermore, the whole network itself was relatively cheap, providing a 24/7 surveillance, that increase the response time of local security guards in case of a break in and provide information (appearance, face, gender, etc.) about possible intruders in case of unauthorized access for recognition.

The resource management solution was implemented using Active Directory control software and single chip Raspberry single-board computers. The computers were configured to work as internet Kiosk so that other employees besides IT administrators could use the devices for personal use without the risk of them doing their own configurations on the Kiosk. This solution allowed for an easier access to the company’s Active Directory for IT specialists, mitigating the down time of resource allocation or user account management.

However, both solutions still have room to improve. The surveillance system itself could be improved by implementing a video stream to the security guards' smart phones using single-board computer and a mobile app.

The resource management system while useful for the IT department has lost a layer of security. The system could be improved by a multifactor authentication whenever someone would try to access to the control panel on the browser.

In conclusion, the new created systems were functional and tackled the problems the company faced. Furthermore, both technologies can be used further to increase reliable surveillance over long distances around the factory and easier access to resource management. None the less both systems can be improved security wise.

REFERENCES

airMAX team. 2019. Ubiquiti airMAX. Available at: https://www.doubleradius.com/Ubiquiti-AirMAX.html [Accessed 22 March 2019]

Bensky, Alan. 2008. Wireless Positioning Technologies and Applications. Available at: https://kaakkuri.finna.fi/Record/nelli29_mamk.1000000000534004 [Accessed 5 December 2018]

Brooks, Charles J., Grow, Christopher, Craig, Philip, Short, Donald. 2018. Cybersecurity essentials. Available at: https://kaakkuri.finna.fi/Record/kaakkuri.224229 [Accessed 25 January 2019]

CableOrganizer.com team. 2019. Security: IP Cameras vs. Analog Cameras. Available at: https://www.cableorganizer.com/learning-center/articles/ip-cameras-vs-analog-cameras.html [Accessed 15 April 2019]

Clines, Steve, Loughry, Marcia. 2008. Active Directory for Dummies Available at: https://kaakkuri.finna.fi/Record/nelli29_mamk.1000000000539678 [Accessed 20 November 2018]

Heckman Robert. 2015. Hesitant About Active Directory? This Is Why Your Company Needs It. Available at: https://www.liveconsulting.com/news/hesitant-about-active-directory-this-is-why-your-company-needs-it [Accessed 18 December 2018]

Inspired Techs. 2017. The Main Benefits of Computer Networking in 2017. Available at: https://www.inspiredtechs.com.au/computer-networking/ [Accessed 30 March 2019]

Intervid team. 2019. CCTV Surveillance Options & Techniques. Available at: https://www.intervid-africa.co.za/blog/cctv-surveillance-options-techniques [Accessed 8 April Sep 2019]

Jacoberger Tom. 2014. How Does Active Directory Work? Available at: https://blog.tcitechs.com/blog/active-directory-work/ [Accessed 21 January 2019]

Jacoberger Tom. 2014. What is Active Directory? Why Does My Company Need It? Available at: https://blog.tcitechs.com/blog/active-directory-company-need/ [Accessed 21 January 2018]

Joe Wilson. 2015. What Type Of CCTV Camera Should I Buy? Available at: https://www.sonitrolwesterncanada.com/blog/what-type-of-cctv-camera-should-i-buy [Accessed 2 March 2018]

Luo Flora. 2019. CCTV Camera Types, Features, Uses, Price & Best Picks. Available at: https://reolink.com/cctv-camera-types/ [Accessed 23 April 2019]

Mailheau Rita. 2019. The Cable War: Copper vs. Fiber. Available at: https://www.versatek.com/blog/cable-war-copper-vs-fiber [Accessed 5 March 2019]

Paul Goodman. 2019. Wireless Network vs Wired Network: Advantages and Disadvantages. Available at: https://turbofuture.com/computers/Wireless-Network-vs-Wired-Network-Advantages-and-Disadvantages [Accessed 14 February 2019]

Prajapati Vinay. 2018. 10+ Different Types of CCTV Cameras and Their Purpose. Available at: https://www.techprevue.com/cctv-cameras-different-types-purpose/ [Accessed 3 December 2018]

Sanassi CISSE. 2017. Benefits of Windows Server 2016 for businesses. Available at: https://www.supinfo.com/articles/single/6411-benefits-of-windows-server-2016-for-businesses [Accessed 9 February 2019]

Steele Carmen. 2019. Why is Computer Networking Important? Available at: http://www.digitaldividecouncil.com/why-is-computer-networking-important/ [Accessed 2 May 2019]

Vangie Beal. 2019. SBC - single-board computer. Available at: https://www.webopedia.com/TERM/S/sbc_single_board_computer.html [Accessed 12 April 2019]

Webster, C.W.R, Töpfer, E., Webster, C. William R. 2012. Video Surveillance: Practices and Policies in Europe. Available at: https://kaakkuri.finna.fi/Record/nelli29_mamk.2670000000326838 [Accessed 29 February 2018]

Wong, K. Daniel, John Wiley & Sons. 2012. Fundamentals of Wireless Communication Engineering Technologies. Available at: https://kaakkuri.finna.fi/Record/nelli29_mamk.2670000000138102 [Accessed 3 March 2018]

Official Raspberry Operating system download site: *https://www.raspberrypi.org/* [Accessed 9 March 2018]

Official ADManager AD controller site: *https://www.manageengine.com/* [Accessed 10 March 2018]

APPENDIX

Keyboard shortcut file (the edited part):

```
<keyboard>
  <chainQuitKey>C-g</chainQuitKey>
  <!-- Keybindings for desktop switching -->
  <keybind key="C-W-Left">
    <action name="DesktopLeft">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
  <keybind key="C-W-Right">
    <action name="DesktopRight">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
  <keybind key="C-W-Up">
    <action name="DesktopUp">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
  <keybind key="C-W-Down">
    <action name="DesktopDown">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
  <keybind key="W-S-Left">
    <action name="SendToDesktopLeft">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
  <keybind key="W-S-Right">
    <action name="SendToDesktopRight">
      <dialog>no</dialog>
      <wrap>no</wrap>
    </action>
  </keybind>
```

```
<keybind key="W-S-Up">
  <action name="SendToDesktopUp">
    <dialog>no</dialog>
    <wrap>no</wrap>
  </action>
</keybind>
<keybind key="W-S-Down">
  <action name="SendToDesktopDown">
    <dialog>no</dialog>
    <wrap>no</wrap>
  </action>
</keybind>
<keybind key="W-F1">
  <action name="Desktop">
    <desktop>1</desktop>
  </action>
</keybind>
<keybind key="W-F2">
  <action name="Desktop">
    <desktop>2</desktop>
  </action>
</keybind>
<keybind key="W-F3">
  <action name="Desktop">
    <desktop>3</desktop>
  </action>
</keybind>
<keybind key="W-F4">
  <action name="Execute"/>
   <command>false</command>

  </action>
</keybind>
<keybind key="W-d">
  <action name="Execute"/>
   <command>false</command>
  </action>

<keybind key="C-A-d">
  <action name="Execute"/>
   <command>false</command>
  </action>

<!-- Keybindings for windows -->
<keybind key="A-F4">
  <action name="Execute"/>
   <command>false</command>
  </action>
```

```
</keybind>
<keybind key="A-Escape">
  <action name="Execute"/>
   <command>false</command>

    </action>
</keybind>
<keybind key="W-Menu">
  <action name="ShowMenu">
    <menu>client-menu</menu>
  </action>
</keybind>
<keybind key="W-t">
  <action name="ToggleDecorations"/>
</keybind>
<keybind key="A-F10">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<!-- Keybindings for window switching -->
<keybind key="A-Tab">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<keybind key="A-S-Tab">
  <action name="Execute"/>
   <command>false</command>
</keybind>
<keybind key="C-A-Tab">
  <action name="Execute"/>
   <command>false</command>
  </action>
</keybind>
<!-- Keybindings for running applications -->
<keybind key="W-e">
  <action name="Execute">
    <startupnotify>
      <enabled>true</enabled>
      <name>PCManFM</name>
    </startupnotify>
    <command>pcmanfm</command>
  </action>
</keybind>
<!--keybindings for LXPanel -->
<keybind key="W-r">
  <action name="Execute"/>
   <command>false</command>
   </action>
  </keybind>
  <keybind key="A-F2">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="C-Escape">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <!-- User Keybindings -->
  <keybind key="W-space">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="F11">
   <action name="Execute"/>
    <command>false</command>
   </action>

  <keybind key="A-Print">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="C-Print">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="S-Print">
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="W-f">
   <!-- Force the flash plugin to release keyboard focus
        http://awesome.naquadah.org/wiki/Workaround_plugins_that_steal_the_keyboard_focus
    -->
   <action name="Execute"/>
    <command>false</command>

   </action>
  </keybind>
  <keybind key="W-p">
    <action name="Execute"/>
     <command>false</command>

    </action>
  </keybind>
  <!-- Launch Task Manager with Ctrl+Alt+Del -->
  <keybind key="A-C-Delete">
    <action name="Execute"/>
     <command>false</command>

    </action>
  </keybind>
  <keybind key="C-A-Escape">
    <action name="Execute"/>
     <command>false</command>

    </action>
  </keybind>
  <keybind key="XF86ScrollDown">
    <action name="Execute"/>
     <command>false</command>
    </action>

  <keybind key="XF86ScrollUp">
    <action name="Execute"/>
     <command>false</command>
    </action>

</keyboard>
```