Edvinas Andriukaitis

MODERNIZATION OF COMPUTER NETWORK IN A COMPANY

Bachelor's thesis

Bachelor of Engineering

Degree Program in Information Technology

2023

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor or Engineering
Author(s)	Edvinas Andriukaitis
Thesis title	Modernization of computer network in company
Commissioned by	Matti Juutilainen
Year	2023
Pages	66 pages, 1 pages of appendices/1 appendix page
Supervisor(s)	Matti Juutilainen

ABSTRACT

The aim of the thesis was to prepare a project for the modernisation of the computer network in a company, the project also includes the implementation of a video surveillance system. Upgrading of the company's IT infrastructure and workstations to improve work efficiency and reduce the "stress" experienced by employees as a result of computer malfunctions. After analysing required data about the routers, switches, IP surveillance systems, protocols and other necessary articles the project was implemented. The results after the implementation were: The company’s computer equipment and network were updated, and a video surveillance system was installed. These works have increased the stability of the computer network and improved cyber security, as a firewall solution has been installed and equipment has been updated to meet today’s requirements. Employee work productivity has increased.

Keywords: PoE, OS, IT, CPU, VPN, LAN, NVR, SSH, DHCP, IP, Wi-Fi, UDP, DNS, NAT, GDPR, ACL.

CONTENTS

Abbreviations

ACL – it is a set of rules that allow or deny access to a computer network.

CPU – it is a computer system that controls the interpretation and execution of instructions.

DHCP – it is a network protocol that allows to configure network devices on an IP network.

DNS – it is a naming system for computers, services and other resources in the internet.

GDPR – General Data Protection Legislation.

IP – it is a set of rules for communication over the internet.

IT – it is the use of computers, storage drives, networking devices and other physical devices.

LAN – it is a form of a network in a certain location with computers linked together.

NAT – it is the process that maps an internet protocol address to another by changing the header of IP packets via router.

NVR – it is a computer system that includes a software that records a video in a digital format to a disk drive.

OS – it is a program that is loaded into the computer by a boot program, it manages all other applications.

PoE – it is a technology that allows to power up devices using Ethernet cables.

SSH – it is a network protocol that enables two computers to communicate.

UDP – it is a communication protocol that is used across the internet for video playback, DNS lookups or other sensitive matters.

VPN – it is technology that provides users with an opportunity to establish a protected network connection when using public networks.

Wi-Fi – it is a wireless networking technology that uses radio waves to provide wireless internet access.

1 INTRODUCTION

Many companies nowadays are still using computer networks that were designed a long time ago. As the time passed the solutions and technologies that were cutting edge yesterday is considered outdated today. That is why many companies is in need for a computer network modernization. Today almost all of the companies data is being stored either in cloud-based storage solutions or local data servers. Old network equipment cannot cope with data streams that is increasing day by day. That is why companies should renew their outdated computer networks not only for the efficiency, but also for reliability, security, computing power and availability to add more storage space.

The need of overhaul of a company's office provided an opportunity to upgrade the outdated existing technologies and equipment. Some of the equipment that is still usable will be moved to the renovated premises. After the upgrades of the equipment, the work will be significantly more productive, and the IT administrator's work will become easier.

Most of the company's computer equipment is already outdated, and the part that is still usable is very slow because it is overloaded with redundant information. There are 13 computers in the computer network, which specifications (see Table 1) fall short of the requirements, for example the OS must be Windows 10, because other older versions are no longer supported by Microsoft. The motherboards must have more connections, for the peripheral devices. The processors must be significantly more efficient than the current ones. The benchmark index of the current computers in the company according to the Passmark testing program is 2867, which is quite a good number for a computer of 2014, but according to current estimates and future plans, the requirements for the processor index of new computers are about 9000. The loads of the programs that are used by the engineers and designers are too high for those computers. Existing computers are very slow when they are turned on. Usually it takes about one minute, and upgrades would cut that time by more than half. The reaction to program launches is also very slow. Applications should load in 10-15 seconds, but now they load in 1,5 minutes. Also, OS used on company's computers are no longer supported by the vendor.

Operating systems such as Windows 7 or Windows 8 no longer receive security and stability updates from Microsoft. The current internet plan provides company with 100 Mbps, which was enough for the former number of employees. After the company's overhaul with the increase in the number of the employees and the appearance of the IP video surveillance system, the need for the internet connection will become significantly greater. At the moment, during the internet speed test using the "Speedtest" application, or performing simple "ping" command using Windows command prompt to Lithuanian web pages, the delay is about 3 ms. With the increase in the number of workplaces in the company and taking into account the loads placed on the network by the IP surveillance system we can confidently say that with the current internet plan, the delay would be more than 5 ms, and the requirement is to have <= 1 ms delay. When upgrading old and creating new workplaces, as well as updating computer and network equipment, there is a need to redo the existing computer network plan. In order to increase security of inventory, documents, employees and their personal belongings, there is a need for IP video surveillance system. The pandemic has taught the company to work more "flexibly". Therefore, in order to give employees, the opportunity to work remotely, the company needs a secure remote connection to the company's internal resources.

Table 1 Computers being used in company

Computer	Lenovo ThinkCentre M710 SFF
CPU model	Intel Core i3-4150 T
Operating system	Windows 8
Graphics card	Intel HD Graphics 4400
Chipset	Inter Q87
Random Access Memory	4 GB 1333 MHz
Storage memory	HDD 500 GB
CPU Passmark index	2867
Maximal power consumption	210 W

The main objective is to prepare a project for the modernization of the company’s computer network, which includes the installation of the company’s security system.

The main tasks are the following:

- Analysis of the current situation. Assess the company’s IT infrastructure and computer equipment. Determine needs for the network upgrades.
- Perform an analysis of the technologies required for the implementation of the project. Choose the most suitable technological solutions.
- Prepare IT infrastructure and workplace modernization project.
- Select the necessary equipment for the project implementation.
- Perform an assessment of the security vector of the project.
- Perform an economic evaluation of the project implementation.
- Prepare the project conclusions

2 BACKGROUND STUDY

A computer network is interconnected computer equipment that exchanges data and shares resources with each other. A geographic location often describes network, whether it is LAN (local area network) that connects computers in a defined physical space, WAN (wide area network) that can connect computers located on different continents, the best example of such a network is the internet, which connects billions of computers around the globe. Computer networks allows communication for businesses, entertainment and research purposes. The Internet, web search, video and audio sharing, online commerce, social networks, live broadcasts that connects nodes such as computers, routers, switches using optical, cooper cables or wireless signals. These connections allow network devices to communicate and share information. Networks follow protocols that define how communications are sent and received and without them it would simply be impossible. Each device on a network uses an Internet protocol, or IP address which uniquely identifies the device and thus ensures that other device can recognize it. What is computer networking? (Amazon).

2.1 NAT

NAT (Network Address Translation) is a protocol that allows a single IP address to represent a whole group of computers. NAT technology is often works in a router or firewall to assign a public IP address to computers within a private network. The purpose of NAT is to "conserve" IP addresses. This is because the availability of public IP addresses is reaching its capacity [Network Address Translation].

2.2 DHCP

DHCP is a protocol used by clients and servers for the automatic assignment of network addresses when clients move between networks, or static entries for clients who require the same network address. DHCP is essentially an automated and centralized management tool used by network administrators to provide more reliable IP address configuration and to reduce the workload [Dynamic Host Configuration]. When you connect a device to the computer network, the device needs an IP address. This request is sent to the DHCP server, and an address is then assigned to the device by the server. After assigning the IP address, the DHCP server controls the use of the IP address and recovers it when the machine turns off. DHCP parameters are also provided by these servers. These parameters describe options such as:

- A default gateway
- A subnet mask
- A DNS server

2.3 ACL

A network access control list (ACL) is made up of a set of rules that either allow or deny access to a computer environment. In a sense, an ACL is like a private, exclusive club. You can only enter if you are on the guest list. There are two main types of ACLs: File System ACLs and Network ACLs. A file system access control list acts as a set of rules that manages access to a directory or a file. Access to a network is managed by the Network Access Control List. These lists tell switches and routers what type of traffic is allowed to interface with the network. It also tells them what each user or device is allowed to do when they are on the network. Some of the benefits of the use of ACLs are Easier to identify users, performance and control users [What is a Network Access Control List?]

2.4 PoE

PoE (Power over Ethernet) - is the technology that allows power and data to be transmitted over twisted pair Internet cables to wireless access points, IP cameras, VoIP phones and other devices. This makes it easier to physically deploy network devices without the need for additional power cables for each device that supports PoE [Power over Ethernet] technology, as a single RJ-45 cable can provide both data connectivity and power to the devices.

2.5 VPN

One more technology that is used by most of the companies or even users are VPN (Virtual Private Network). More than 30% of the world's Internet users rely on virtual private networks for security and privacy. A business VPN primarily protects the information that employees send and receive over the Internet. It also protects the Internet connection from unauthorized intrusion. It allows users to browse securely from wherever they are accessing the Internet by providing full encryption of Internet connections. Once encrypted data is private. It is protected from spoofed Wi-Fi connections, hackers, governments or competitors.

Some of the benefits of a VPN are:

- Improved safety
  Secure Internet connections with firewalls and anti-virus software are not completely immune to hackers. Antivirus software protects your information from about 75% of common malware and viruses. A VPN service can solve this problem because a regular internet connection is not very secure or encrypted. It protects sensitive customer information, internal documents, communications and other trade secrets by encrypting all data transmissions.
- Sharing data securely
  Sharing data securely between groups, colleagues and people outside the company is one of the most useful uses of a VPN. Depending on a company's choice of VPN service, a private network can encrypt not only the Internet connection to the internal computer network, but also the connection to the outside world.
- Remote access to data
  The Virtual Private Network service allows you to more securely connect remotely to your organisation's secure server and access the data you require. Because this connection is direct encrypted, data is protected from prying eyes. A business VPN service is a great choice for companies that are looking to improve their security and provide their employees with the ability to access information from home or other remote locations.

- Avoidance of international censorship
  Traveling to countries that censor the web, blocking various online portals and social networks can prevent employees from working effectively remotely. Many VPN providers offer the ability to choose the location of the virtual network, thereby circumventing the system of the country in question.
- Set-up and costs
  These solutions usually take a lot of time, energy and effort to integrate into an existing computer network. If the network is new, things are a little easier.
- Management and operations
  An organisation should have a person or team responsible for maintaining and managing the system if it is not using a managed VPN service. The secure and stable operation of this system is of the utmost importance, both for the employees and for the customers. Company and customer data is priceless. It is therefore extremely important to protect it. According to a report in the New York Times by Craig Newman, companies can save up to 47% of the costs associated with a data breach through risk management, the use of encryption and employee training. A VPN solution is the ideal solution for any business that deals with sensitive data in one way or another, as it will help to ensure that this data is protected. As a result, the installation of a VPN service in the computer network is a decision worth making.

2.6 VLAN

A Virtual Local Area Network (VLAN) is a virtual connection that links together a number of devices and network nodes that are on different LANs to form a logical network. VLANs are most commonly configured on a switch. A virtual local area network can be spread across a number of switches, with each VLAN being treated as a separate subnet or broadcast domain. VLAN offers a number of benefits such as simplified administration, increased performance, greater flexibility and much more.

2.7 GDPR

The General Data Protection Regulation (GDPR), adopted by the European Parliament and the Council in 2016, sets out the requirements that must be followed by organizations in relation to the collection, storage and management of individuals' data. All European organizations that deal with EU residents in one way or another are subject to the regulation.

Cyber security is perhaps the biggest and most important aspect of the GDPR. The protection of people's private data stored on a company's physical servers is quite vulnerable. This type of server is highly susceptible to hacking or cyber-attacks. Both physical and software protections must be in place to avoid this. Server room is always under surveillance.

- A lockable server racks.
- Physical firewall.
- Virtual Private Network (VPN).
- Backups are made.
- Unauthenticated users have no access to the company network.
- Users can only see information they are authorized to see.
- Password encryption using WPA2 or WPA3 protocols.
- Record regular software updates that fix stability or vulnerability issues.
- MAC address filtering.
- Monitor and educate employees about cyber threats and how to protect against them.

To ensure your business is GDPR compliant, you can contact professionals who advise businesses on GDPR issues. These organisations will carry out an assessment of the current situation and provide guidance on how to further ensure the security of sensitive data. If the current situation is not satisfactory, they can also implement a range of solutions to improve the current situation.

Breaches of the GDPR can result in administrative fines. These fines must be effective, proportionate and dissuasive. Thus, the fine may be up to 2-4 percent of the total annual worldwide turnover of the preceding financial year, or up to 10,000,000 - 20,000,000 euros. It should be noted that these are maximum fines, but the lower limit of the fines may be any numerical expression of the minimum amount [Fines and other sanctions following the application of the GDPR].

A closer look at the computer network equipment used in the company would suggest that it is not bad and is still good enough to continue using it. The Lithuanian National Cyber Security Centre warns in its report of the security threats posed by Russian software. It urges people to pay attention to hardware and avoid Russian-made equipment. Users are also advised to disable any online components linked to Russia. These can be used to collect confidential information and perform other malicious activities. Back in 2019, a study of the National Cyber Security Centre [analysis of D-Link products] found that devices have “YandexDNS” and “SkyDNS”, owned by Russian companies installed by default. YandexDNS logs all user requests, which allows it to identify IP address of the users the country of the user, the time of the request and the addresses that user visits. This long-term monitoring of people helps to determine with a which degree of accuracy the behaviour of a person in cyberspace and, in certain cases, to identify the person. In addition, there is another DNS service called “SkyDNS”, which provides DNS and DNS filtering services. [Russian-origin software components pose security threat].

2.8 Situational analysis

The company that is being overhauled is engaged in the production of precast reinforced concrete. It has branches in many European countries. As production expanded, there was a need to reconstruct company’s existing office building and update computer and network equipment. The object that is being renovated is located in city of Kaunas, Lithuania where computer network will be reorganized and the number of workplaces will be increased.

2.8.1 Computers used in the company

The Lenovo ThinkCentre M710 SFF computers currently used in the company (see Table 1) are physically obsolete. The components that these devices have struggles to cope with ongoing tasks and application loads. As the number of types of products produced by the company increases and as the production volume expands the software that is being used to design cannot keep up. So new modelling programs should be installed. The technical requirements of these programs are too high for the current equipment. Programs such as AutoCAD requires at least 1 GB of video memory which integrated graphics card cannot offer. It does not have its own dedicated memory to use, so that puts even more strain on the computer's RAM.

For specific positions that work with design and modelling a physical graphics card could be installed, but this would only partially correct the situation, since other computer components are nor powerful enough. Lack of RAM, processor, hard disk, these parts of the computer are the most outdated and reduce work performance. Currently the company's processors are clocked at 3 GHz, which are sufficient for minimal operation of SolidWorks program but it needs 4 or more GHz to run in optimal modes. The processor is involved in the rendering of structural assemblies and models, which takes significantly longer with a low clock frequency than with higher one, the difference could be up to 2-3 minutes or even more. AutoCAD requires 16 GB of RAM to run smoothly and the current system only has 4 GB of 1333 MHz memory. The hard disk is responsible for the speed of saving and opening the files. The speed of the HDD is significantly slower than the new SSD or the latest generation of PCIe NVME drives. HDD drives transfer data at an average speed of 30-150 MB/s, SSD drives at around 500 MB/s and NVME drives at 300-3500 MB/s these figures may vary by the manufacturer or model, but the trend shows that the difference between these disks is major. Therefore, a decision was made to replace the computers with new ones that have enough memory and computing resources to perform tasks that are assigned to them.

2.8.2 Network equipment used in the company:

The company uses three routers and three switches. The specifications of these devices could be found: (see Table 2 and Table 3).

Table 2 Routers being used in company

Network device	1 Router	2 Router	3 Router
Model	D-Link DIR-2150	D-Link DIR-615S	D-Link DIR-640L
Wireless network standard	IEEE 802.11a/n/ac IEEE 802.11 b/g/n IEEE 802.11 k/v	IEEE 802.11 b/g/n	IEEE 802.11 b/g/n IEEE 802.3 IEEE 802.3u
Number of ports (RJ-45)	4	5	4
Throughput	2100 MB/s	300 MB/s	300 MB/s
SFP+	-	-	-
Multiple SSID	+	+	+
Firewall	+	+	+
VPN server / client	+	-	+
QoS support	+	+	+
Suitable for further use? Yes / No	No	No	No

The first is the D-Link DIR-2050 router which has one 100/100/1000 BASE-T WAN port and four 10/100/1000 BASE-T LAN ports. It is equipped with four non-removable antennas that allow sending and receiving several data streams at the same time, which significantly increases the performance of the router. The firewall features on this device are pretty decent. It has NAT functionality, IPv4/IPv6 address, MAC and URL filters, which allows you to at least slightly increase the protection of your computer network. The wireless connection provided by this router ensures a speed of up to 300 Mbps at 2,4 GHz frequency and up to 1733 Mbps at the 5 GHz frequency. This router is good from the technical side, its coverage ensures wireless access in a large office area, while other two routers provide more than 95 % coverage in office premises. This device, like other D-Link devices are not reliable in terms of cyber security and therefore is not suitable for use [Software components of Russian origin pose a security threat].

The price of the D-Link DIR-615S router is about 38 euros and its maximum Internet transfer speed is 300 Mbps which is very good indicator for such a price. Some Wireless-G routers are significantly more expensive than D-Link's creation, though they only max out at 54 Mbps. The biggest shortcoming of the D-Link DIR-615S router are the lack of 1 Gbps Internet ports and USB connections, but it is an excellent choice as an entry-level router. It has a 10/100/1000 BASE-TX WAN port and four 10/100/1000 BASE-TX LAN network ports. The device can also be used as a four-port switch, allowing you to connect multiple devices to a computer network. In terms of security, this router is not a market leader, but it does have a built-in firewall. Additional security measures reduce the threat posed by hackers and Internet viruses and other dangerous software. After upgrading the Internet speed, the maximum transfer speed of this device will not allow it to use its full potential, which is why it was decided to get rid of this device.

The D-Link DIR-640L wireless router supports not only its own functions, but also the functions of a 10/100 Mbps switch, wireless access point (IEEE 802.11n), and a firewall. This small device is simply designed to be used at home or in small offices. Its performance, security is high enough and its very compact in terms of size. The DIR-640L router allows you to create a VPN and thus provide secure remote access to the main network for 24 users at the same time. The device supports IPsec, PPTP, L2TP, GRE protocols in server mode and additional advanced VPN functions can also be selected, such as: DES encryption, IKEE/ISAKMP key management. For corporate network administration this router provides some flexibility due to the ability to block employee access to certain web pages, as well to control and monitor employee activity on the network. This router is no longer usable as it will be no longer physically needed. It is also outdated and needs to be reloaded quite often because the wireless connection it provides is often unavailable.

Table 3 Switches being used in company

Network device	1 Switch	2 Switch	3 Switch
Model	D-Link GO-SW-8E/E	D-Link DGS-1008P	D-Link DGS-1210-28MP
Number of ports	8	8	28
Total bandwidth	1,6 Gbps	16 Gbps	56 Gbps
SFP+	-	-	4 ports
PoE	-	4 ports	24 ports
PoE power	-	68 W	130W
QoS support	-	+	+
Port protection	-	-	+
Mount type	Non rack	Non rack	Rack
Suitable for further use? Yes / No	No	No	No

D-Link GO-SW-8E/E switch was chosen because switches of this model have low energy consumption and relatively low market price. This switch is unmanaged, its interface speed is 10/100 Mbps. Its LED indicators provide us with information about the status and activity of the ports. The ports on this device automatically read the current internet speed and assign standards: 10 BASE-T and 10 BASE-TX and full duplex or half accordingly to ensure the maximal possible Internet speed for the device connected. This switch also supports auto MDI/MDIX interfaces, which allows this device to be connected directly to a server, router, switch or other device using a simple Straight-Through cable. The Internet speed supported by this device has been maxed out. The Internet speed in the company is currently 100 Mbps, which corresponds to the maximum speed of this device. This switch has 8 RJ-45 type ports that were partially used because not all of them were used. The D-Link GO-SW-8E/E does not have PoE (power over ethernet) functionality, which is a rather big drawback when considering whether this device is suitable for further use. This switch has Ethernet flow control functionality described by the IEEE 802.3x standard, which aims to prevent data packet loss during network congestion. Also, this device complies with the European Union’s RoHS (Restriction of Hazardous Substances Directive), which describes certain hazardous substances in the electronic equipment industry. This device is no longer usable after a network upgrade project as it supports maximum speed of 100 Mbps per port, and when the internet speed will be increased by the provider This bandwidth will not be sufficient and this switch is also unmanageable.

The company also uses a D-Link DGS-1008P switch, this unmanaged, non-rack type device has PoE ports that can provide power to devices such as: wireless access points, IP cameras, IP phones. This device takes up very little space so it is perfectly designed for home and office use. The DGS-1008P switch has 4 10/100/1000 BASE-T ports that supports IEEE 802.3 af and IEEE 802.3 protocols at which they can provide power from 15 to 30 watts. The maximum power resource of this device is 68 watts. This device can distribute 16 Gbps of data through all 8 ports. This device is no longer suitable for further use as it is unmanaged, which makes it very difficult to identify the problem in the event of a failure.

The D-Link DGS-1210-28MP is the latest generation of D-Link switches. It has 24 10/100/1000 BASE-T ports with PoE support and 4 1000 BASE-X SFP ports, which allow both fiber optic and RJ-45 connections. This device is equipped with the manufacturer’s proprietary software, the D-Link Safeguard Engine, which protects the switch against viruses and other various attacks. The 802.1X authentication port allows the use of an external RADIUS server to authenticate users. For video surveillance or IP telephony systems, the D-Link DGS-1210-28MP is the perfect choice. It features Auto Surveillance VLAN and Auto Voice VLAN, which are ideal for the systems mentioned above. This feature allows the automatic setup of video equipment or Voice over Internet Protocol (VoIP). This switch is a rack-mounted device with a maximum data transfer rate of 56 GB/s, which offers the possibility of increasing the speeds provided by the ISP, as this switch would support much higher Internet speeds than those currently available. This switch is also no longer suitable for further use as the network optimization will involve the removal of intermediate switches and the purchase of 2 managed switches, which will ensure more stable network.

2.8.3 Printing devices

The company has two types of printers in use: the Triumph-Adler 3262I and the HP LaserJet P2055dn. The first printer is relatively new. It has been on the market since 2018, so it is certainly not out of the date in terms of technology. The next printer in line is HP LaserJet P2055dn. The first printers of this model were introduced back in 2004. However, they work very well. The print speed and resolution are not inferior to current printers, and from a technical point of view, these printers are really reliable the most common problems are preventive maintenance for example, toner replacement and flushing.

Table 4 Printers being used in company

Name and model	Triumph-Adler 3262I	HP LaserJet P2055dn
Purpose and function	Copying, scanning, printing documents	Document printing
Type	Laser	Laser
Resolution	1200x1200 dpi	1200x1200 dpi
Print speed	32 ppm A4 / 17 ppm A3	35 ppm A454
Suitable for further use?	Yes	Yes

2.8.4 A diagram of the company’s network

The current layout of the company’s workstations, printers and switching hubs is shown in Figure 1. The electrical wiring required for the computer equipment is hidden in the walls, while all the network communications are in the suspended ceiling and are lowered via special troughs or through the walls into the power sockets. The internet in the office comes into the server room, where it is connected to a router, and from there everything is distributed through switches.

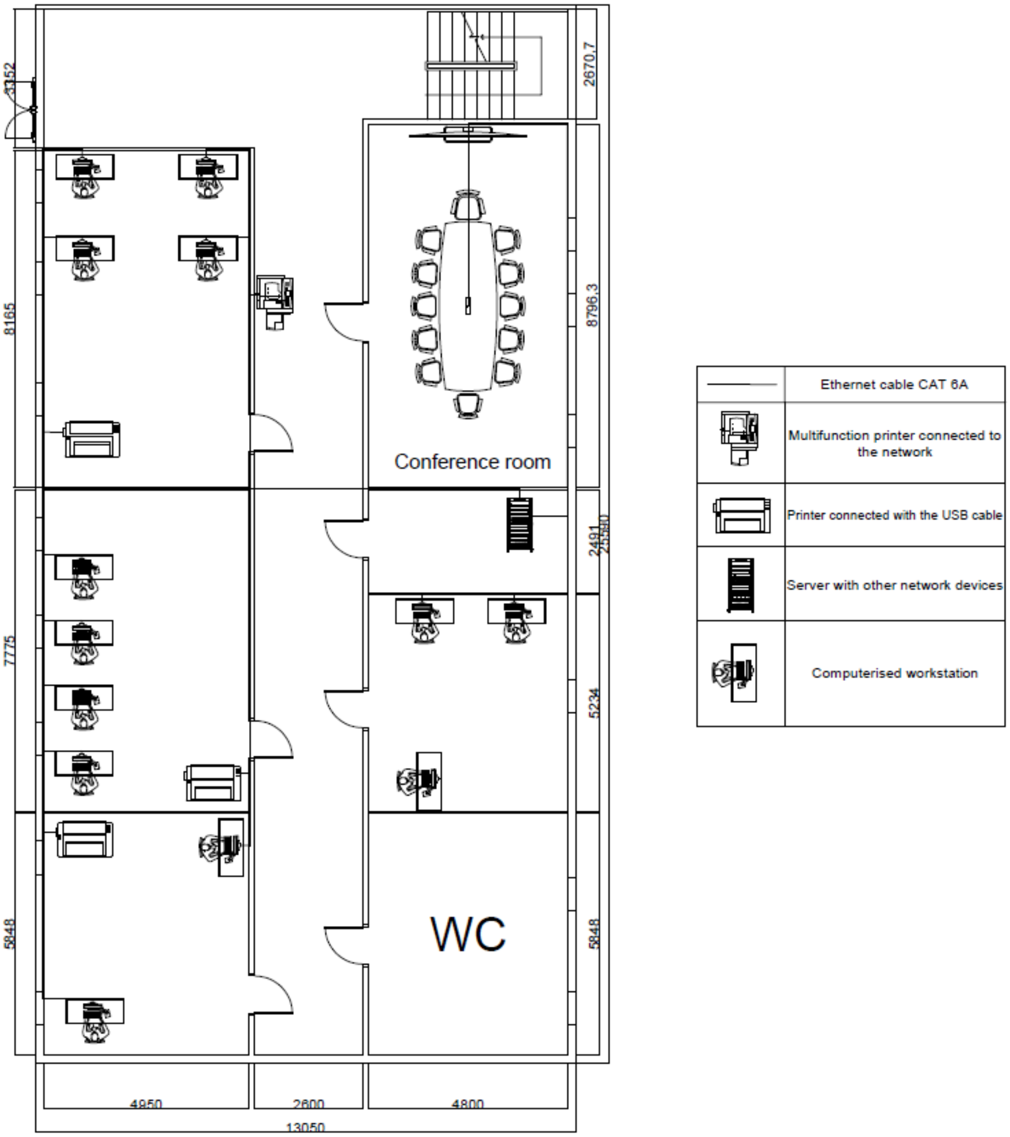


Figure 1 Map of the premises and workplaces of the company on the ground floor

Up to this point, the office space on the second floor of the company has been unfurnished and unused. However, the major refurbishment will make it ready to use. This floor will provide 20 additional workstations for designers and engineers. There will also be another conference room and a lounge/leisure area. In these workspaces, the internet connections will be installed in the wall sockets or will be dropped directly into the workstation via special troughs, and all the cable ducts will be routed above the suspended ceiling.

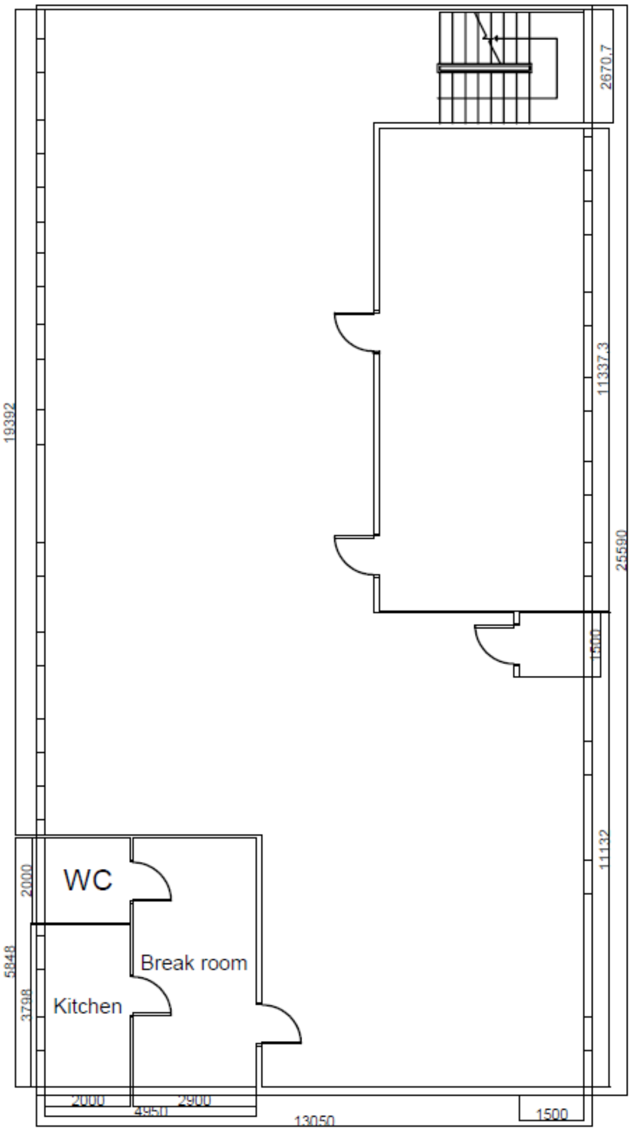


Figure 2 Map of the premises and workplaces of the company on the first floor

The company's grounds and premises are not currently monitored by CCTV cameras. However, it was decided to install them for the safety of the employees and their property. The cameras will cover the red area around the building and the blue area on the ground floor.

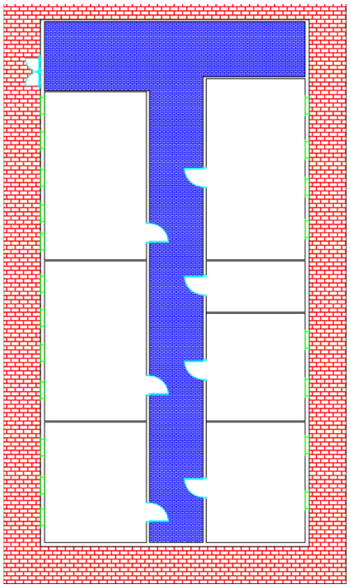


Figure 3 Zones to be covered by the IP CCTV system

2.8.5 Existing computer network topology

In the figure 4 you can find the topology that is in use right now.

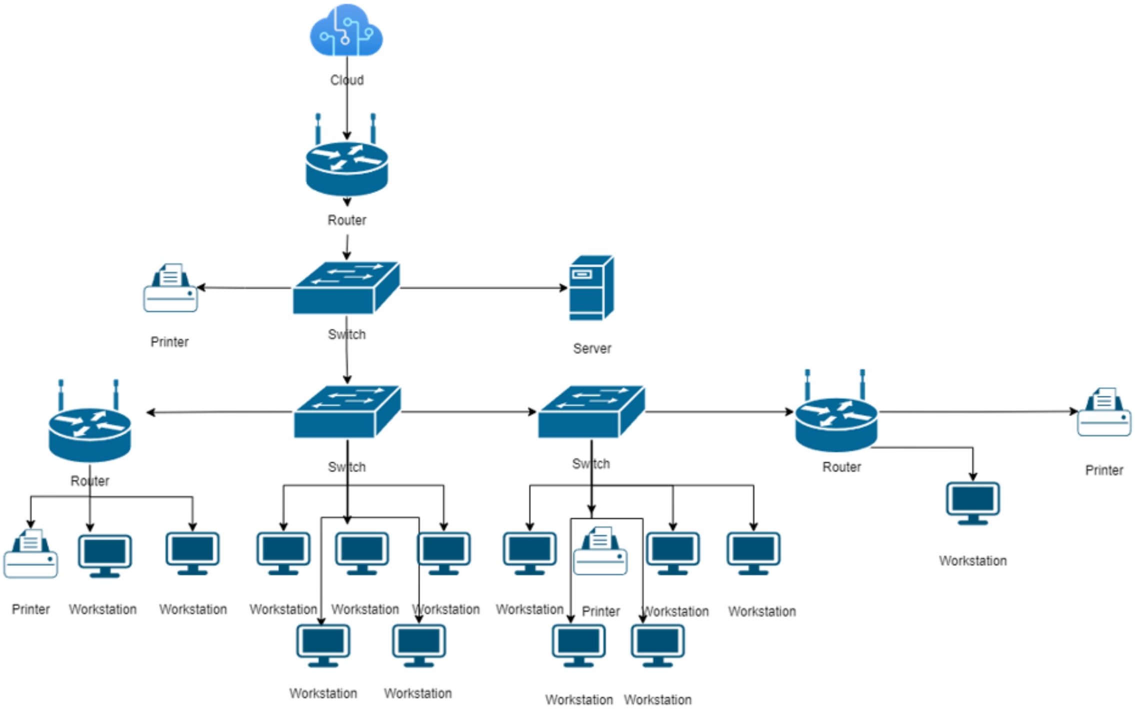


Figure 4 Topology diagram of existing computer network

3 TECHNOLOGICAL ANALYSIS

In this part analysis of the technologies is being held.

3.1 Operating systems

There are currently 13 computers on the network that are running Microsoft's Windows 8 operating system, which is no longer up to date and is no longer in compliance with security requirements. The Windows 8 operating system has been unsupported since January 2016, and Windows 8.1 will be unsupported in 2023 (Windows 8 and Office, 2020). For these operating systems, important security updates, which are particularly important today, are no longer provided by the manufacturer. Recent events are evidence of the fact that several companies' computer systems have been hacked and sensitive customer and company data has been stolen. One example is the "Cybercrime" event. 110,000 customers' details (email addresses, telephone numbers, personal codes, encrypted passwords) were exposed. "CityBee was using Microsoft's Azure Blob data storage service. "Microsoft provides the ability to secure these repositories with additional credentials, which CityBee, for whatever reason, chose not to implement," the hackers say. Researchers, hackers and programmers use what are known as DNS records, which are like a phone book that branches out to other domains that are linked to the root domain. I looked at the CNAME-type DNS records for Citybee and that was where I found the link to the Azure repository," the hacker said ["CityBee database hacker: companies never learn"]. This case is not directly related to the vulnerabilities of Windows, but the positive security features of Microsoft can certainly help to protect you against "viruses", security holes or dangerous applications that could put your data at risk. That's why it's important to upgrade an outdated OS to Windows 10 or even Windows 11, which are much safer because they receive updates and patches. These versions also have Device Guard, which checks that the application is from a trusted source and warns the user.

Table 5 Requirements for different versions of Windows

Windows version	Windows 8	Windows 10	Windows 11
Platform	x86 – x64	IA- 32, x86 – 64, ARM v7, ARM v8	x86 – 64, ARM v8
“Kernel” type	Mixed	Mixed (Windows NT kernel)	Mixed (Windows NT kernel)
Editions	4	8	7
Support	2023 year	2032 year	Unspecified
TPM support	-	v1.2 and over	v2.0

Table 6 Specifications needed for different versions of Windows

Windows version	Windows 8	Windows 10	Windows 11
Processor	1 GHz	1 GHz	1 GHz with 2 or more cores
RAM	32-bit 1 GB, 64-bit 2 GB	32-bit 1 GB, 64-bit 2 GB	4 GB
Hard disk memory	32-bit 16 GB, 64-bit 20 GB	32-bit 16 GB, 64-bit 20 GB	64 GB
DirectX	9th version WDDM 1.0	9th version WDDM 1.0	12th version WDDM 2.0
TPM	1st version	1st version	2nd version
Software	-	UEFI, secure boot	UEFI, secure boot

Choice of operating system for new computers will come down to three versions of Windows 10: Windows 10 Enterprise, Windows 10 Pro and Windows 10 Pro for Work. Windows 11 has not been chosen because not all applications in use in the company are currently supported by this version of the operating system and not all drivers, which are the means by which a computer's physical hardware interacts with software, are compatible.

3.2 Software used in the enterprise

The company uses Microsoft's 365 business solution. This solution allows the business to operate in a secure manner from any location. "Microsoft 365 Business Premium helps protect your business from a wide range of cyber threats by combining the best Office applications, efficient cloud services and comprehensive security. It includes Outlook, OneDrive, Word, Excel, PowerPoint, SharePoint, Microsoft Teams, Exchange, InTune, Microsoft Guard, Azure AD, Azure Security System.

"TeamViewer is a comprehensive remote access, manage and support solution that works on virtually all mobile platforms including Windows, MacOS, Android, iOS. With this application, you can connect to a computer or mobile device that is located anywhere in the world and use it as if you were there in person. The application allows the company's computer network administrator to remotely advise employees and, where possible, resolve problems.

3.3 Physical and software firewalls

At the simplest level, they perform the same function, but have fundamental differences: a hardware firewall is a physical entity, while a software firewall runs on a computer through an application:

Table 7 Comparison of physical and software firewalls

Firewall type	Physical firewall	Software firewall
Price	Expensive option, need to buy additional equipment	A cheap option as it can be configured on the router
Placement	Requires extra physical space	Requires no additional space
Deployment type	Complicated installation due to connection to a computer network, wiring, etc.	Easy to install

The hardware firewall acts as a sort of "guardian angel" for the physical server. It sits directly behind the router. It can be configured to analyse and filter all data packets. A physical firewall is similar to a server that filters the data traffic that is sent to and from the computer. While the user typically connects the network cable directly to the computer or server. With a hardware firewall, user is connected to the firewall that sits between the external network and the server, providing an anti-virus solution and a solid barrier against hackers.

Advantages of hardware firewalls:

- Intelligent flow control that reaches the network server
- Applies specific rules to all traffic
- Can make the work of other servers easier, e.g., can disable software firewalls that consume processor memory and power.

Every firewall setup is different, depending on how your computer network is configured. But the principle remains the same. They "stand" between your computer network and the Internet. They protect your network from cyber-attacks, viruses, and other dangers that lurk online.
Advantages of a physical firewall:

- One device for computer network management: a single physical firewall protects each computer connected to the server, reducing the time and resources required to install a software firewall on each computer.
- Security updates are applied to all computers on the network at the same time. If you change the settings on the firewall, all computers receive the updates after you save them. This helps to ensure that all of the devices on your computer network are secure.
- Protection is always on, unless it is physically disabled. The hardware firewall has no monthly payments, computer memory or malfunctions have no effect on the firewall, so there is no possibility of protection being lost and the server left dangerously unprotected.

- Better security - Hardware firewalls have their own separate operating system, which makes them less susceptible to some of the cyber-attacks that software firewalls can suffer from if a computer is compromised.
- Protection from threats that can attack the internal hard disk drives. A hardware firewall is like a physical barrier between the hard drives of a computer and any incoming malicious code that is stopped before it can cause any damage to the user's data.

Many people wonder: Can a router replace a firewall? Their assumption is that the router's security policies provide the security they need. The following security features are often provided by routers:

- Prevention of data streams that travel without a clear destination
  The router will simply drop the data if it doesn't know which host the packet is destined for. If malicious information is sent that targets the router, the data should be discarded. This is because there is no clear destination, which in this case is the host.
- Blocking certain data types
  Some routers can be configured in such a way that certain types of data can be blocked from the computer in use. This can help to ensure that hackers won't be able to use your computer to attack other devices.

However, routers do not have enough cyber security solutions. For example, if a user tries to open a malicious website, the router bypasses the malicious code on the user's computer because the user is just trying to open the website. A physical firewall, on the other hand, will block such requests, even if it is the user who wants to access the data.

Is a physical firewall the right solution for a small business? The answer is usually yes. This solution provides reliable protection while conserving computer resources. A single physical firewall can provide valuable and convenient protection for many devices because many devices share data with the server. It is also a time and effort saver for the IT staff. So, when it came to upgrading the computer network, the decision was made to purchase and install a physical firewall.

3.4 Computers used within the company

The company currently has 13 Lenovo ThinkCentre M710 SFF computers in use. The specifications are shown in Table 1. They are physically outdated and are being written off. This will require the purchase of 33 new computers, which may vary in specification depending on the role of the staff member. Laptops should be provided for administrative staff. Staff such as designers or engineers who work on drawings can be provided with both desktop or laptop computers.

3.5 Internet

The current internet speed for the company was 100Mbps, but this was too slow, according to staff complaints and the recommendations for a 10Mbps staff member in the online article [How fast should my internet be?]. With the addition of 20 new workstations, bringing the total number of workstations to 33, and the installation of IP CCTV cameras, the current 100 Mbps plan will not be enough. Therefore, a 500Mbps or higher Internet plan should be selected so that in the future, a few more workstations can have Internet access without impact on the Internet speed of other employees.

3.6 Analysis of IP CCTV camera systems

The most common IP video surveillance components are:

- IP CCTV cameras.
- A switch which connects the video surveillance system to the main computer network.
- Video recorder
- Hard disk drives

A network video recorder (NVR) is used with IP CCTV cameras and is connected to the internet for signal transmission and reception. Used by professionals in various countries around the world, this type of security surveillance system is the most advanced and appreciated. Using the Internet, you can connect to this system at any time. You can view the images or live feed on your PC, work computer, smartphone or tablet. There is also the option of download of recordings.

IP CCTV cameras have been available on the market since 1996. These cameras use a computer network or the Internet to send and receive data. An IP system must be connected to a video recorder (NVR), either via a wired or wireless computer network, in order to monitor the images, it transmits. Combining this video surveillance system with the right lighting can help to quickly identify thieves or intruders. All the necessary clues are stored on the NVR. There are also cameras on the market that can detect the presence of abandoned objects or people crossing the line. Some IP CCTV systems have the ability to detect motion. You can receive an email alert with a snapshot of the motion that triggered the alert. The maximum protection that CCTV systems can provide is an alarm function, night lighting, regular snapshots and the ability to monitor the image remotely.

3.7 Hardware subsystem

General information about the hardware being used within the company.

- The physical equipment used in the office of the company:
- 13 workstation PCs used that no longer meet specification requirements
- 13 LCD monitors in service
- Multi-function printers
- 2 switches with a wireless function and one switch without a wireless function
- 3 switches
- Simple printing devices

3.8 Information subsystem

General information about the software being used within the company.

Computer's operating system:

- Microsoft Windows 8

Document management, e-mail and more:

- Microsoft Office 365

Programmes for specific jobs:

- Citrix Workspace
- Tekla
- Scia Engineer
- DraftSight 2021
- AutoCAD 2022
- IDEA StatiCa

3.9 Result and decision

The organization’s computer network equipment is obsolete and is not fit for purpose due to cyber security weaknesses as recommended by the NCSC. The computer equipment is physically out of date and is no longer able to cope with the demands being placed on it. The facility is in need of an extension to the number of workstations, an upgrade to the computer network and an upgrade to all computer equipment. To improve security, a network of IP cameras also needs to be purchased and installed.

3.10 Object to be designed

An upgrade of the company's computer network is planned. This includes not only routers, switches and wireless access points, but also the computers themselves and their equipment. There will also be a need for a new contract with an internet service provider which will be able to offer higher internet speeds. Installing a CCTV system covering the staff car park and ground floor offices.

3.11 Purpose of the object

Smoother operation and reduced ping delays will result from the upgraded computer network. New workstations on the company's second floor will allow for the recruitment of new staff. This will increase the company's productivity. People and vehicles entering the premises can be monitored via the CCTV network.

3.12 Functions of the object

The new computers will enable them to work faster, more easily and more efficiently. An upgraded computer network will ensure better data security, and a VPN solution will be in place for home working. Surveillance of the company's territory and premises by means of an IP video camera system.

3.13 Operational requirements

- Each computer is patch-connected to the network via sockets in the walls.
- All of the computers need to be connected to a common computer network.
- A wireless access point is to be installed on both the ground floor and the first floor of the office to provide Wi-Fi access to the building.
- A switch will be installed on the second floor of the office to connect all the computers on the second floor. The device itself will be connected to another switch on the ground floor.

3.14 Requirements for the documentation of the reconstruction project

- All equipment must be supplied with full documentation, i.e.: certificates of compliance, guarantees, technical descriptions of equipment, installation and operating instructions, schematics and circuit diagrams.
- The contractor's documentation shall include all drawings necessary for the installation and operation of the equipment, i.e.: equipment layout and cabling plans, equipment connection diagrams, equipment interconnection diagrams, etc.

- All devices, equipment, apparatus, panels, cables, installation materials and products provided for in the project shall be installed, tested and coordinated according to the standards or technical specifications of their manufacturers, without prejudice to the requirements of the normative documents applicable in Lithuania.
- Technical specifications do not replace normative documents and standards applicable to the manufacture, supply and installation of equipment. They are complementary to them. Where standards or other normative documents have been approved for the manufacture and installation of equipment, these documents shall be in accordance with the requirements.
- All work, whether or not shown on the drawings or described in this document, which is reasonably considered necessary for the completion of the installation and the proper operation of the systems shall be carried out.
- All electrical wiring and cables in the room shall be of a flammable class not inferior to:
    - Evacuation routes (corridors, stairways, lobbies, foyers, entrance halls, halls, etc.) - Cca s1, d1, a1.
    - Rooms with capacity over 50 people - Dca s2, d2, a2.
    - The places in the building where the cables are laid: shafts, tunnels, technical recesses, spaces above the false ceiling, under the false floor, etc. - Dca s2, d2, a2.
- The necessary requirements and EU standards shall be met by all construction materials, network equipment, cables and installation materials used in the project. Products must have certification and approval from the VRM PAGD Fire Research Centre.

4 PROJECT IMPLEMENTATION

In this part project implementation phase and decisions of equipment will be made. Based on the analysis part and recommendations for security measures, all the network equipment needs to be changed and IT related equipment needs to be upgraded also.

4.1 Project phases

After an analysis of the current situation and input from IT and other staff, the project implementation can begin. The first phase should include placing endpoints: computers, cameras, printers, wireless access points. Based on the layout and the ports that will be needed for these devices, a wired network will be designed from the communication nodes, where the switches will be located, to the end devices. Distances must also be taken into account, and the length of the cables must not exceed the maximum limit of 100 metres. Once these steps have been taken, suitable computer networking equipment is selected with the appropriate number of ports to support 1G Ethernet and 1G Ethernet with PoE. The computers and CCTV systems are analysed and a decision is made as to which equipment should be purchased. The next step would be an analysis of Internet service provider plans and ordering of the most appropriate option. The final stage would be the installation, assembly and testing of all the systems.

4.2 Computer network planning

A new computer network plan needs to be drawn up. This will be presented to the IT specialists once all the work has been completed. It was decided to purchase 2 new switches, both with 48 ports, once all the workstations and network equipment requirements had been agreed. The reason for this decision was that the ground floor will be the connection point for all the computers, printers, wireless access point, IP CCTV cameras and the connection to the second floor. The second floor will have all the workstations, a wireless access point and a link to the first floor.

In the physical topology diagram of the computer network on the first floor, we can see where the computers, the printers and the wireless access point will be located, and how the LAN cables will be routed. From the server room switch on the first floor to the switch cabinet on the second floor, the ETHERNET cable will also be routed.

We can see where the computers and wireless access point will be located and how the LAN cables will be routed in the topology diagram of the second-floor computer network. Also, from the server room switch to the second-floor switch cabinet will be a Category 6 computer network cable.

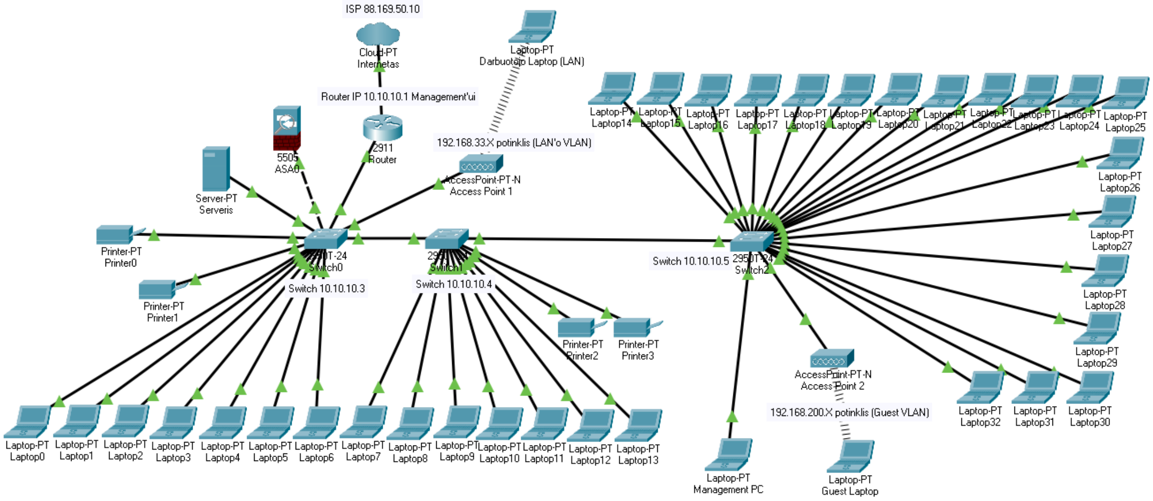


Figure 5 Diagram of the topology of the upgraded computer network

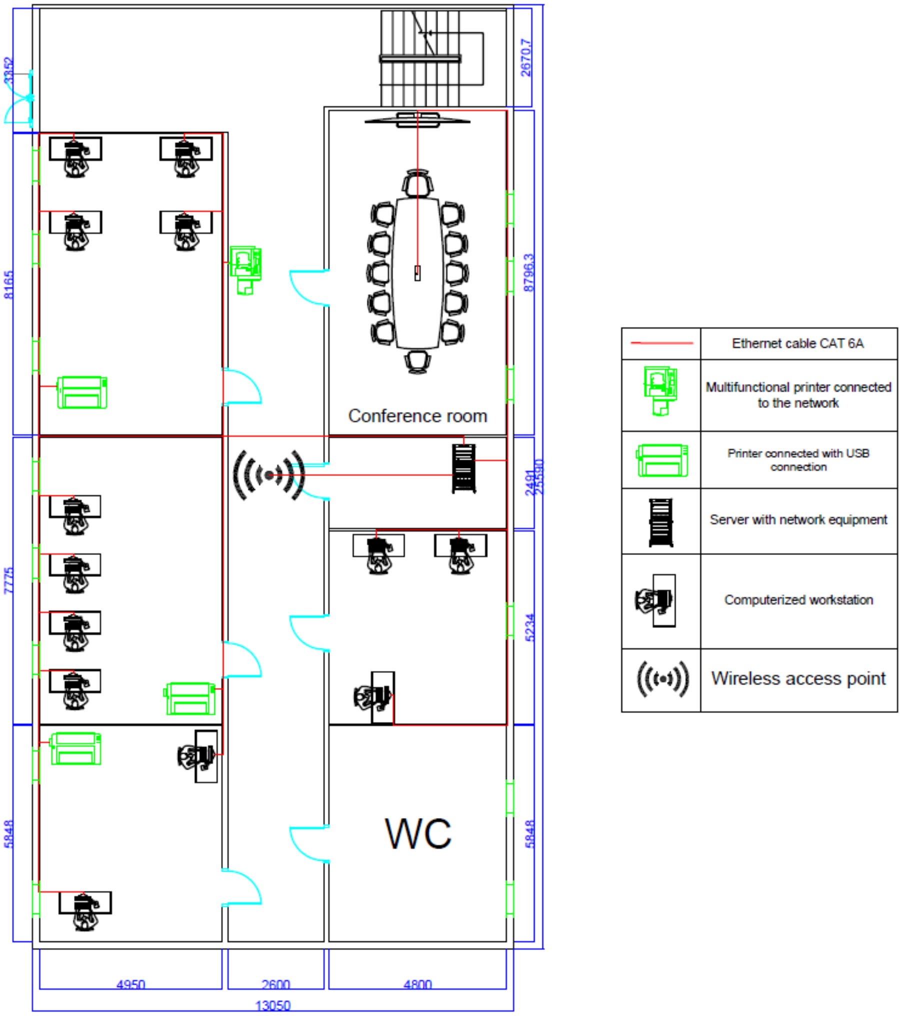


Figure 6 The layout of the renovated rooms and workplaces on the ground floor

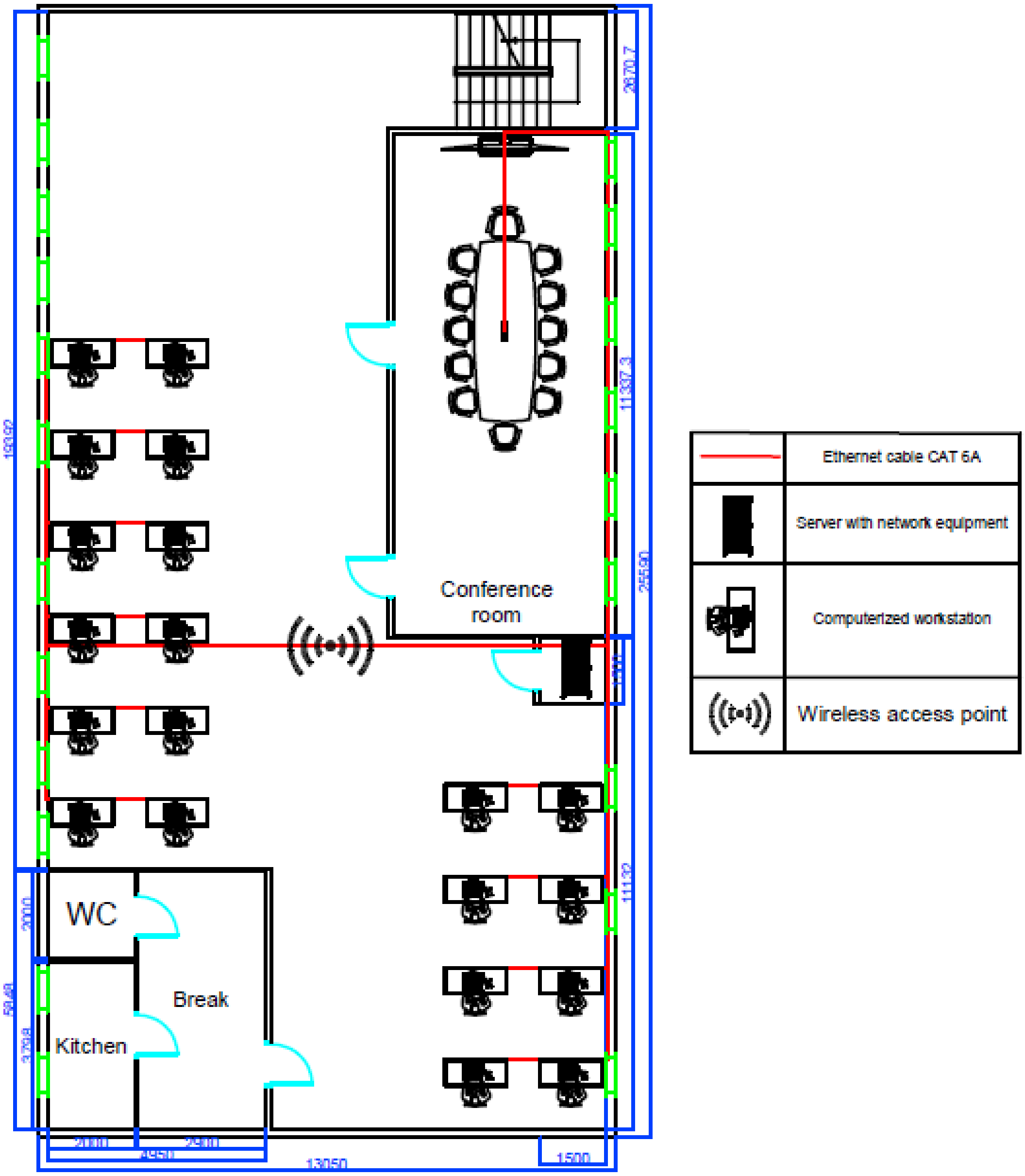


Figure 7 The layout of the renovated rooms and workplaces on the first floor

The IP addresses of the computers, printers and other equipment on the first floor and on the second floor are listed in Appendix 1. These addresses will be set for each piece of equipment. The computer addresses are automatically assigned using the DHCP protocol from the 192.168.33.1 - 192.168.33.100 range. Static IP addresses are assigned to printers, network devices and CCTV (see Appendix 1). For the following purposes: network device management, computer network, guest Wi-Fi network, virtual LANs are created.

4.3 Designing computing hardware

Based on the situational analysis the decision was made to swap the existing computers and buy additional ones.

4.3.1 A choice of computers for the designer

After analysing the parameters of the company's existing computers and the comments made by the employees, it was concluded that the equipment used so far was no longer usable. It was therefore decided to dispose of them all and purchase 33 new computers.

Table 8 Computer comparison/selection for designers

Manufacturer	Required value	DELL	DELL	DELL
Model		Precision Mobile 3561	Precision 7560	Precision 3560
CPU		Intel Core i7 - 11800 H	Intel Core i7 - 11800 H	Intel Core i7 – 1165G7
Passmark CPU index value	>= 20000	21344	21437	10557
Operating system	Windows 10 Enterprise	Windows 10 Enterprise	Windows 10 Enterprise	Windows 10 Enterprise
GPU		NVIDIA T1200	NVIDIA RTX A3000	NVIDIA T500
Passmark GPU index value	>= 7000	7882	13117	3604
Operating memory	>= 8 GB 3200 MHz	8 GB 3200 MHz	16 GB 3200 MHz	16 GB 3200 MHz
Storage	>= SSD 512 GB	NVMe SSD 512 GB	SSD 512 GB	SSD 512 GB
Price		1730 €	2642 €	1570 €

We can see that the DELL Precision Mobile 3561 and the DELL Precision 7560 meet the GPU and CPU index requirements, while the third machine does not, as shown in Figure 8. However, the price of the Precision 7560 is significantly higher than that of the Precision Mobile 3561. For these reasons, the decision was made to purchase 20 new DELL Precision Mobile 3561 laptops for designers.

4.3.2 A choice of computers for the administration

From the information in the table (Table 8), we can see that the DELL Latitude 5521 significantly outperforms its competitors in terms of Passmark benchmark scores, so the decision was made to purchase 6 of these laptops for the purchasing and sales staff, as they work with large MS Excel files and other applications. And 7 Lenovo ThinkPad E15 Gen 2 laptops for the rest of the employees, who do not need such powerful computers as they only perform the most basic tasks.

Table 9 Computer comparison/selection for administration

Manufacturer	Required value	Lenovo	DELL	HP
Model		ThinkPad E15 Gen2	Latitude 5521	ProBook 455 G8
CPU		AMD Ryzen 5 4500U	Intel Core i5 – 11500H	AMD Ryzen 3 5400U
Passmark CPU index value	>= 11000	11097	16288	11839
Operating system		Windows 10 Enterprise	Windows 10 Enterprise	Windows 10 Enterprise
GPU		AMD Radeon Graphics	GeForce MX450	AMD Radeon Graphics
Passmark GPU index value	>= 1500	1782	3751	1420
Operating memory		8 GB 3200 MHz	8 GB 3200 MHz	8 GB 3200 MHz
Storage		SSD 256 GB	SSD 256 GB	SSD 256 GB
Price		749 €	1405 €	890 €

The decision to buy laptops instead of desktop computers was taken in the context of a situation of which we are still seeing the consequences today. During the pandemic period, the majority of employees had to be teleworkers, and it is possible that future pandemics will require employees to work remotely. Laptop computers are better suited to this type of work than desktop computers. Laptops can be used as a stationary computer workstation by connecting an additional display, keyboard and mouse. In order to further increase the comfort for the employees and to ensure a sufficient number of computer connections, docking stations are connected to all the computers in the company. This allows multiple displays to be connected to computers without multiple video ports. This device also increases the number of USB ports and provides greater convenience as each device does not have to be plugged in individually, as all peripherals are ready for use with the docking station connection. Also, not all laptops are equipped to connect to a LAN, but docking station provides this.

Table 10 Docking station selection

Manufacturer	ICYBOX	ASUS	HP
Model	IB-DK2106-C	Plus Dock	USB-C Dock G5
HDMI	2 connections	1 connections	1 connections
VGA	1 connections	-	-
DVI-D	-	1 connections	-
Display port	-	-	2 connections
Connection type	USB – C	USB – C	USB – C
LAN connection	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet
USB count	3	4	2
Price	114,99 €	152,49 €	172,87 €

The ICYBOX is the cheapest option and offers all the ports you need to meet company's needs. The docking station of this model will work with all new laptops via the USB-C connection. The decision was made to purchase 33 ICYBOX IB-DK2106-C units as there was no significant difference between the other options.

Table 11 Choice of displays

Manufacturer	BenQ	AOC	DELL	HP
Model	PD2500Q	U27P2	S2722DGM	P27q G4
Reaction time	4 ms	4 ms	1 ms	5 ms
Screen resolution	2560 x 1440	3840 x 2160	2560 x1440	2560 x 1440
HD type	2K QHD	4K QHD	QHD	QHD
Brightness	350 cd/m^2	350 cd/m^2	350 cd/m^2	250 cd/m^2
Maximum refresh rate	60 Hz	60 Hz	165 Hz	60 Hz
Screen size	25 inches	27 inches	27 inches	27 inches
HDMI connections	1	1	2	1
Display port connections	1	1	1	1
Price	346,89 €	345,59 €	326,59 €	277,49 €

The company's employees do not do any photo or video editing, so screen resolution is not a very important point in the comparison of displays, so the focus is on response time, maximum refresh rate and screen size The DELL S2722DGM has the best response time and refresh rate, and is not the most expensive in terms of price, according to the available samples (see Table 10). For this reason, the decision was made to purchase these displays for all the workstations.

4.4 Designing video surveillance equipment

Based on recent activities that caused employees cars damaged the decision was made to install IP CCTV surveillance system in the company's premises. Also, for improved security and safety of workers, this system will be installed at the designed location.

4.4.1 Designing video surveillance equipment

From these four, it was decided to select the Hikvision DS-2CD2347G1-LU F 2.8 and the Dahua IPC-HDW5442TM-AS as they were similar priced and offered the best features. The other two options were ruled out because the night light was only available up to a distance of 30 metres, and the options selected offered a distance of up to 50 metres. Finally, as the price of this camera and the night colour mode it offers are well ahead of the competition, the Dahua IPC-HDW5442TM-AS was chosen. The comparison of these cameras could be found at Table 11.

Table 12 Comparing/choosing IP CCTV cameras

Manufacturer	Minimal functional requirements	Hikvision	Hikvision	Dahua	Dahua
Model		DS-2CD2347G2-L F4	DS-2CD2347G1-LU F2,8	IPC-HDW5442TM-AS	IPC-HDW2531T-AS
Magapixels	4 MP	4 MP	4 MP	4 MP	5 MP
Sensor size	1/1,8“	1/1,8“	1/1,8“	1/8“	1/2,7“
Lens size	2.8 mm	4 mm	2,8/4/6 mm	2.8 mm	2,8 mm
Power	PoE	PoE	PoE	PoE	PoE
IP rating	IP67	IP67	IP67	IP67	IP67
Angle of view	113°	113°	113°	113°	103°
Day/Night	Night light	Yes, LED light > 30 m.	Yes, colour night view	Yes, LXIP light > 50 m.	Yes, IR light > 30 m.
Resolution	2688 x 1520	2688 x 1520	2688 x 1520	2688 x 1520	2592 x 1944
Frames per second	1-25 fps	1-30 fps	1-25 fps	1-25 fps	1-20 fps
Price		240,04 €	215,81 €	199 €	160 €

4.4.2 Selection of video surveillance recorders (NVRs)

The choice of Dahua CCTV recording system is because the choice of cameras is also Dahua. Compatibility is therefore optimal. The user interface of the Smart PSS offered by this manufacturer is also more user-friendly, as the control elements and the functions offered are clearly laid out. The comparison could be seen in Table 12.

Table 13 Comparison/Choice of Video Surveillance Recorders (NVR)s0

Manufacturer	Minimal functional requirements	Hikvision	Hikvision	Dahua	Dahua
Channels	16	16	8	8	16
Maximal resolution	8 MP	8 MP	8 MP	8 MP	8 MP
PoE	8 connections	16 connections	8 connections	4 connections	8 connections
Storage	2 HDD	2 HDD	2 HDD	1 HDD	2 HDD
LAN	1 RJ 45	1 RJ 45	1 RJ 45	1 RJ 45	1 RJ 45
HDMI	1 connector	1 connector	1 connector	1 connector	1 connector
Processor	4 cores	4 cores	4 cores	4 cores	4 cores
VGA		1 connector	1 connector	1 connector	1 connector
3G-4G-WiFi support		+	+	+	+
Price		266,62 €	278,81 €	273,46 €	287,98 €

4.4.3 Analysis of IP video camera viewer applications

After reviewing these 3 CCTV viewer programs, the decision was made to use Dahua's Smart PSS program because the selected recorders and cameras were most compatible with their program.

Table 14 Choosing a viewer for IP video cameras

Name	SmartPSS	iVMS-4200	NetCam Studio
Free/Paid	Free	Free	Free 2 cameras
Maximal channel count	128	256	64
Watermarks	-	-	+ for free version
4k support	+	+	-
Surveilance	+	+	-

4.5 Computer network equipment design

Based on the recommendations of the NKSC, the decision was made to get rid of the insecure computer network equipment and to purchase more secure and reliable equipment.

4.5.1 Selecting a switch

The selection of the switch is on the basis of the number of PoE ports, the switching bandwidth, the number of ports and the price. From these options it is clear that all the switches have 48 PoE ports, the switching bandwidth of the Zyxel and Cisco devices is the same, while the HP device is slightly less, but it is suitable for the needs. Regarding the price, the HP is the cheapest and it meets all the requirements, but two switches are needed to upgrade, so the price aspect is quite important, which is why these two will be purchased.

Table 15 Comparing / choosing switches

Manufacturer	Minimal functional requirements	Cisco	Zyxel	HP
Model		Cisco Catalyst 2960L-SM-48PS	Zyxel XGS2210-52HP	Aruba 6000 48G 4SFP Switch
Number of ports	48 ports	48 ports	48 ports	48 ports
„RACK“ type?	+	+	+	+
SFP+	4 ports	4 Gigabit Ethernet ports	4 ports	4 Gigabit Ethernet ports
PoE maximal power	PoE	PoE + 370 W	PoE + 370 W	PoE+ 370 W
Transfer bandwidth	70 Gbps	88 Gbps	88 Gbps	77,3 Gbps
Switching bandwidth	100 Gbps	176 Gbps	176 Gbps	104 Gbps
Routing Protocol	IGMP	RIP, IGMP, MLDv2, MLD	IGMP, IGMPv2, IGMPv3 MLD	IGMPv2, IGMP, IGMPv3
Price		2252,76 €	2299,99 €	1519,00 €

4.5.2 Selecting a router

Installation type, rack-mountable, routing capacity and price were the criteria for choosing a router. The Zyxel router is too expensive and has only 4 RJ-45 ports. This is not an important criterion, but it is a minus in terms of price. The Cisco unit is not a good choice because it is not suitable for rack mounting. We can clearly see that the HP MSR1003-8 ticks all the boxes and so the decision was made to go with this.

Table 16 Comparing / choosing router

Manufacturer	Minimal functional requirements	Cisco	Zyxel	HP
Model		C891F	OLT2406	MSR1003-8
Total router bandwidth	1 Gbps	1 Gbps	1 Gbps	1 Gbps
„Switch“ integration	8 ports	8 ports	4 ports	8 ports
NAT support		+	+	+
Qos support	+	+	+	+
DHCP server	+	+	+	+
ACL support	+	+	+	+
„Rack“ type?	+	-	+	+
Price		1491,96 €	1836,86 €	1569,89 €

4.5.3 Selecting a wireless access-point

The HP Aruba Instant On AP was chosen as the wireless access point of choice. It outperformed the competition on most parameters and was the most attractive in terms of price.

Table 17 Comparing/selecting wireless access-points

Manufacturer	Minimal functional requirements	Zyxel	Cisco	Aruba
Model	▨	NWA210AX	Aironet1815I	Instant On Ap
Wi-Fi version	Wi-Fi 6	Wi-Fi 6	Wi-Fi 5	Wi-Fi 6
Antenna gain	▨	>= 3 dBi	>= 4 dBi	>= 5,6 dBi
Ethernet ports	▨	1 x GbE	1 x GbE	1 x GbE
2,4 Ghz	500 Mbps	575 Mb/s	368 Mbps	574 Mbps
5 Ghz	1 Gbps	2,4 Gbps	867 Mbps	1,2 Gbps
Wi-Fi standart 2,4 Ghz	802.11ax	802.11ax	802.11ac	802.11ax
Wi-Fi standart 5 Ghz	802.11ax	802.11ax	802.11ac	802.11ax
USB	▨	USB 2.0	USB 2.0	USB 2.0
Price	▨	337,78 €	368,24 €	284,22 €

After reviewing the computer networking equipment, which included three manufacturers, Zyxel, Cisco and HP, it was decided not to go with Zyxel because it lacked longevity and reliability. The remaining two manufacturers are very similar in terms of performance and reliability, but the overall cost of HP's networking equipment is lower. This led to the decision to purchase HP's networking equipment (two switches, a router and two wireless access points).

4.5.4 Selecting a firewall

The Cisco Firewall was found to be too expensive to buy and immediately rejected. The only differences between the next two firewalls were bandwidth speed and latency, which were quite similar. Taking these parameters into account, the Sophos XGS 2100 firewall was chosen. It has a higher bandwidth than the Fortinet firewall. The Sophos Firewall is also rack-mountable, enabling proper installation in a switch cabinet.

Table 18 Comparing / choosing firewalls

Manufacturer	Minimal functional requirements	Fortinet	Sophos	Cisco
Model		FortiGate 60 D	XGS 2100	FPR-1140
Remote control protocol		HTTP	HTTP	HTTP
VPN support?	+	+	+	+
Firewall bandwidth	1,5 Gbps	1,5 Gbps	3 Gbps	4 Gbps
IPSEC VPN	1,4 Gbps	1,5 Gbps	1,6 Gbps	1,4 Gbps
Protection against threats	1,3 Gbps	1,5Gbps	1,3 Gbps	1,4 Gbps
Firewall delay		4 µs	6 µs	4 µs
NGFW		-	5200 Mbps	-
„RACK“ type?	+	-	+	+
Price		2444,22€	2689,99 €	7874,97 €

4.6 Designing the CCTV network

The purpose of the IP CCTV system will be perimeter surveillance as well as surveillance of the main ground floor areas inside the company. All of the IP cameras will be connected to the company's server room using LAN type CAT 5e cabling, where a recorder will be installed and connected to a switching panel.

Table 19 IP Video Surveillance System IP Address Table

Device	IP address	Default gateway	Subnet mask
NVR	192.168.20.2	192.168.20.1	255.255.255.240
IP camera 1	192.168.20.3	192.168.20.1	255.255.255.240
IP camera 2	192.168.20.4	192.168.20.1	255.255.255.240
IP camera 3	192.168.20.5	192.168.20.1	255.255.255.240
IP camera 4	192.168.20.6	192.168.20.1	255.255.255.240
IP camera 5	192.168.20.7	192.168.20.1	255.255.255.240
IP camera 6	192.168.20.8	192.168.20.1	255.255.255.240
IP camera 7	192.168.20.9	192.168.20.1	255.255.255.240
IP camera 8	192.168.20.10	192.168.20.1	255.255.255.240

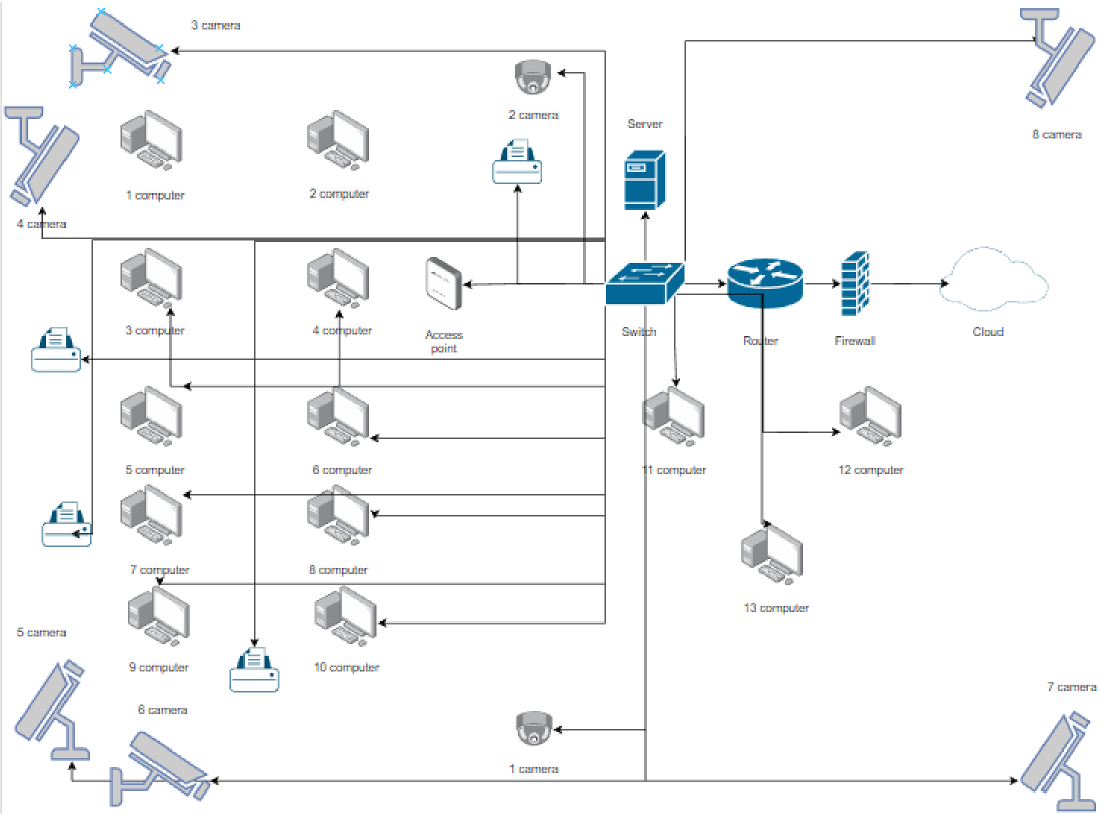


Figure 8 Diagram of how IP cameras were connected to the upgraded network

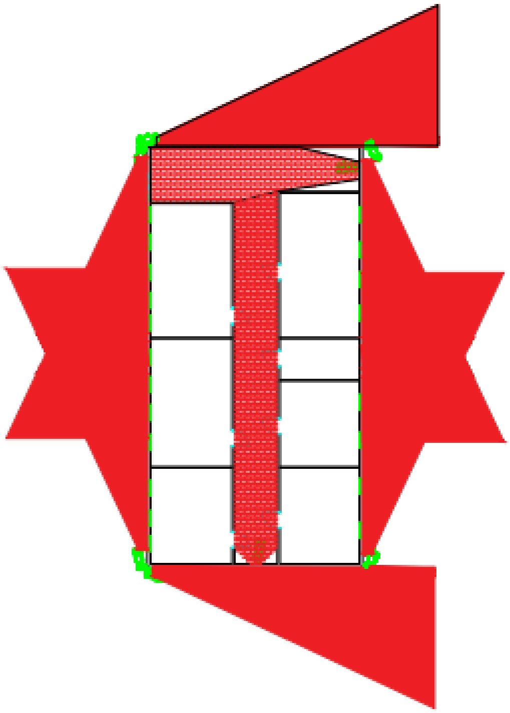


Figure 9 Camera layout plan

The area marked in red is the area clearly visible by cameras.

4.7 Choosing an internet speed

At this stage, enquiries were made to Internet service providers, and the plan that had the most stability, speed and lowest cost was taken into consideration. The company has a fibre optic cable connection, which means it can choose from a number of different offers.

Table 20 Comparison of plans offered by internet providers

Provider	Minimal functional requirements	Telia	FASTLINK	CGates	Splius	csctelecom
Speed	500 Mb/s	>= 300 Mb/s	> 1 Gb/s	> 400 MB/s	> 600 Mb/s	300 Mb/s
Term of contract		24 mos.	24 mos.	24 mos.	24 mos.	12 mos.
Price mos.		46,00 €	44,90 €	40,00 €	34,90 €	46,00 €

Three of the offers submitted do not meet the speed requirements and are not the cheapest in terms of price. This makes the even higher speeds offered by these suppliers even more expensive. The plan offered by Splius offers Internet speeds of up to 600 Mbps, which meets the requirements. However, FASTLINK offers speeds of 1 Gbps and the price difference is not very great. It was for these reasons that the decision was taken to opt for the FASTLINK Internet plan, which offers a speed of 1 Gbps.

4.8 Configuring a computer network using Cisco Packet Tracer

Static IP address range 192.168.33.101 - 192.168.33.254, Dynamic IP address range 192.168.33.1 - 192.168.33.100

```
ip dhcp excluded-address 192.168.33.101 192.168.33.254
ip dhcp pool LAN
 network 192.168.33.0 255.255.255.0
 default-router 192.168.33.254
 dns-server 8.8.8.8              // Google DNS is being used.
 domain-name google.com
ip dhcp pool Guest
 network 192.168.200.0 255.255.255.0    // 1-254 DHCP address „pool“ for guests
 default-router 192.168.200.254
 dns-server 8.8.8.8
```

Translates internal IP addresses into external ones

```
 interface GigabitEthernet0/0
 description WAN
 ip address 88.169.50.10 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
```

Translates the source IP address of packets travelling from the outside to the inside network

```
 interface GigabitEthernet0/1.33
 encapsulation dot1Q 33
 ip address 192.168.33.254 255.255.255.0                SUB interface
 ip access-group 110 in
 ip nat inside
interface GigabitEthernet0/1.200
 encapsulation dot1Q 200
 ip address 192.168.200.254 255.255.255.0
 ip access-group 120 in
  ip nat inside
 interface GigabitEthernet0/1.800
 encapsulation dot1Q 800
 ip address 10.10.10.1 255.255.255.240
 ip nat inside
```

ACL 80 - Allows access to network equipment management via SSH or Telnet protocols. Everything else is blocked.

```
access-list 80 permit 10.10.10.0 0.0.0.15
access-list 80 deny any
```

ACL 120 - Guest is denied access to LAN and Management subnets, is allowed to go outside, there are no prohibitions on its own subnet (192.168.200.0).

Bootpc and bootps are needed for this subnet to get IP addresses from the DHCP server. It works over the UDP protocol.

```
access-list 120 deny ip 192.168.200.0 0.0.0.255 192.168.33.0 0.0.0.255
access-list 120 deny ip 192.168.200.0 0.0.0.255 10.10.10.0 0.0.0.15
access-list 120 permit ip 192.168.200.0 0.0.0.255 any
access-list 120 permit udp any any eq bootpc
access-list 120 permit udp any any eq bootps
```

ACL 110 - LAN is denied access to Guest and Management subnets, is allowed to go outside, there are no restrictions on its own subnet (192.168.33.0).

Bootpc and bootps are needed for this subnet to get IP addresses from the DHCP server.

```
access-list 110 deny ip 192.168.33.0 0.0.0.255 10.10.10.0 0.0.0.15
access-list 110 deny ip 192.168.33.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.33.0 0.0.0.255 any
access-list 110 permit udp any any eq bootpc
access-list 110 permit udp any any eq bootps
```

NAT Creating a WAN "interface" and adapting its rules.

```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source list 2 interface GigabitEthernet0/0 overload
ip nat inside source list 3 interface GigabitEthernet0/0 overload
```

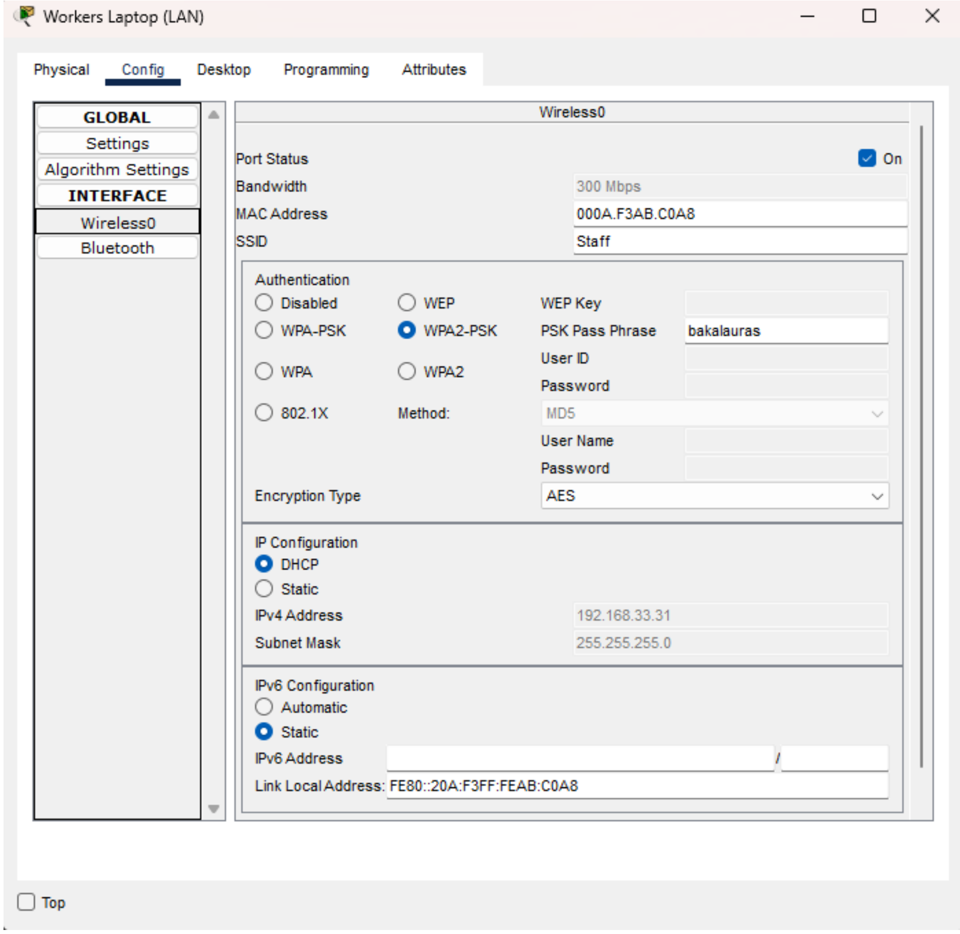
Creating an "Access list" for each subnetwork and applying NAT rules.

```
access-list 1 permit 192.168.33.0 0.0.0.255
access-list 2 permit 192.168.200.0 0.0.0.255
access-list 3 permit 10.10.10.0 0.0.0.15
```

4.9 Project testing

During the testing phase of the project, the upgraded computer network is tested. Cisco Packet Tracer was used to provide a visual/virtual representation of everything. Its functionality allows to replicate the real situation quite accurately. Computer network topology could be seen in Figure 5.

The topology of the computer network created by this software must be more or less the same as the real-life network. Instead of the 2 switches on the ground-floor shown in Figure 5, a single 48-port device will be used in the real site. The ground-floor switch will be connected to the first-floor switch, thus ensuring seamless access for all employees to the server located on the ground floor.



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 000A.F3AB.C0A8

SSID Staff

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase bakalauras

User ID

○ WPA ○ WPA2 Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.33.31

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

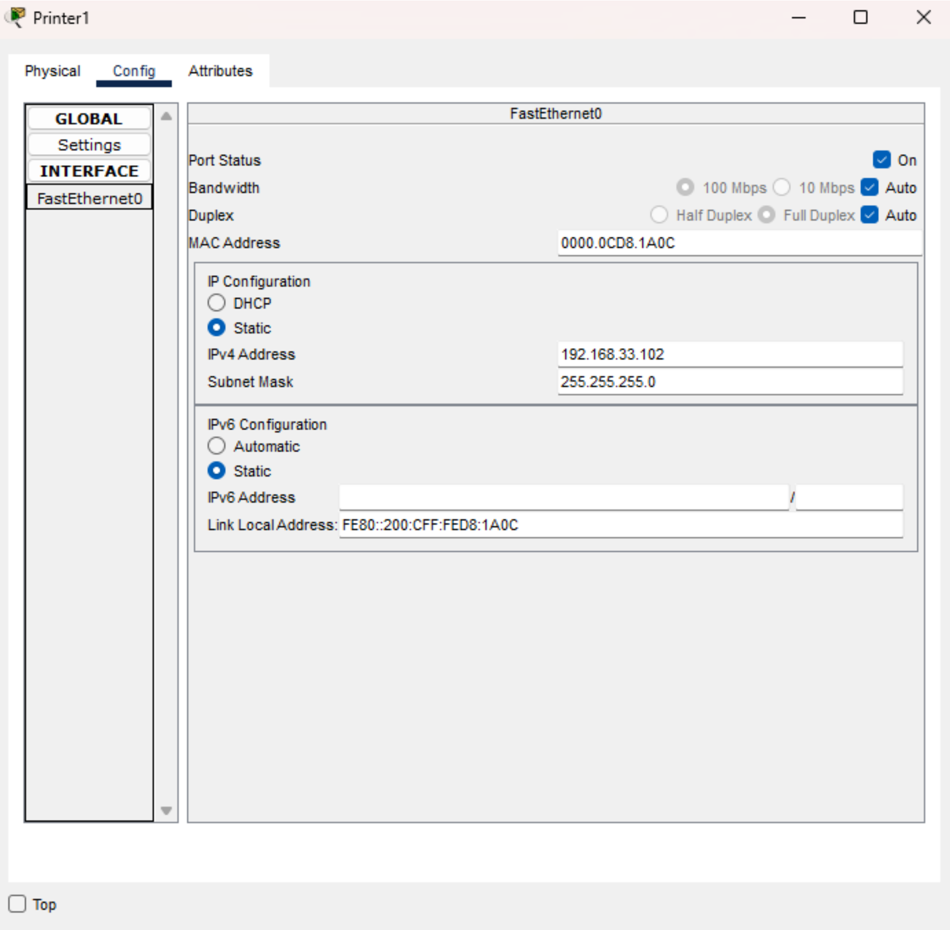
● Static

IPv6 Address /

Link Local Address: FE80::20A:F3FF:FEAB:C0A8

Figure 10 IP addresses assigned to an employee connected to a Wi-Fi network for employees

Employees connected to the Wi-Fi network, as well as to the local LAN network, receive IP addresses via a DHCP server. Addresses are assigned automatically to each device.



FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0000.0CD8.1A0C

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.33.102

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

● Static

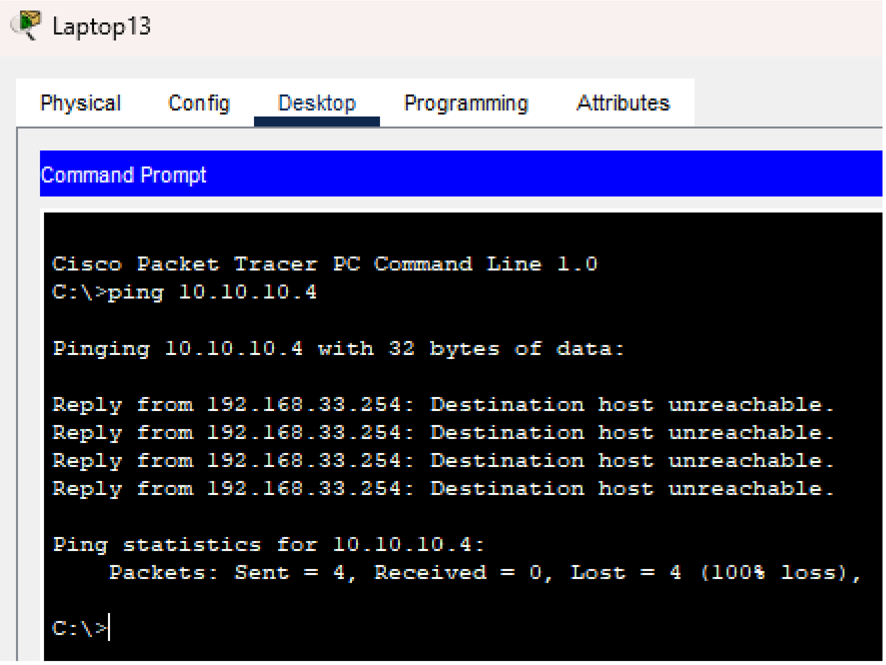
IPv6 Address /

Link Local Address: FE80::200:CFF:FED8:1A0C

□ Top

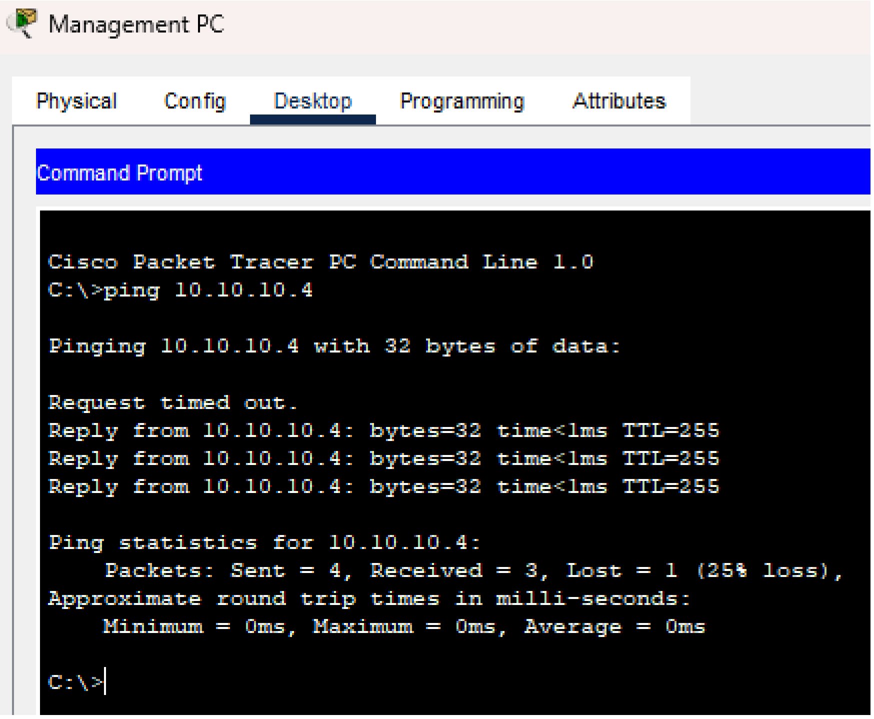
Figure 11 Allocation of IP addresses for printers

The printers are assigned static IP addresses : 192.168.33.101 – 192.168.33.104. Each printer on the network is accessible to staff.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:

Reply from 192.168.33.254: Destination host unreachable.
Reply from 192.168.33.254: Destination host unreachable.
Reply from 192.168.33.254: Destination host unreachable.
Reply from 192.168.33.254: Destination host unreachable.

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

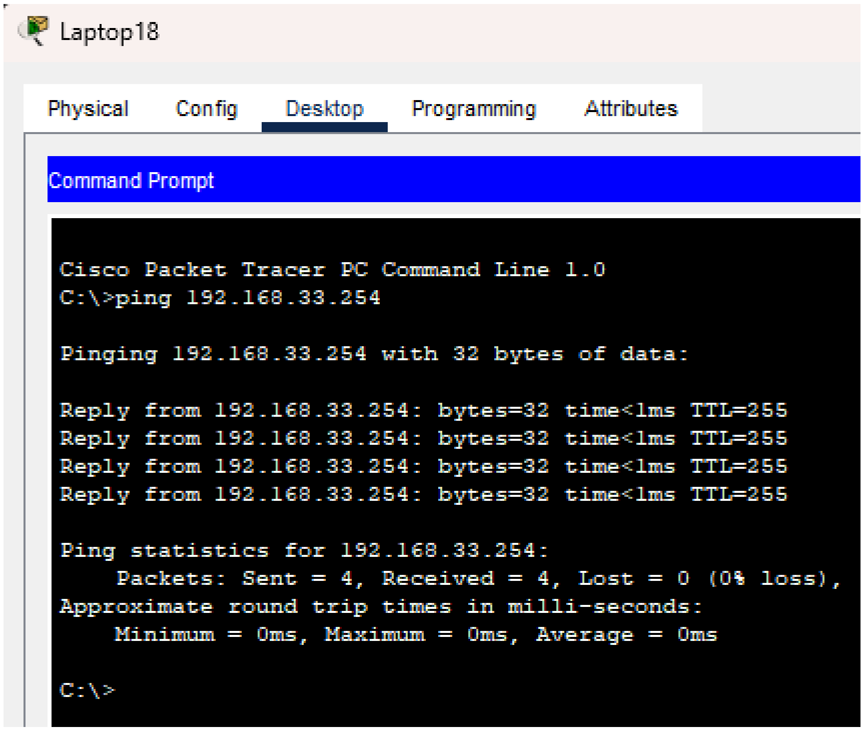
Figure 12 Checking the accessibility of a staff computer to a switch



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.4

Pinging 10.10.10.4 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.4: bytes=32 time<1ms TTL=255
Reply from 10.10.10.4: bytes=32 time<1ms TTL=255
Reply from 10.10.10.4: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 13 Checking the accessibility of a management computer to a switch

We can access switches and other devices on the computer network from a computer dedicated to managing the computer network, or configured to view the computer network and change settings.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.33.254

Pinging 192.168.33.254 with 32 bytes of data:

Reply from 192.168.33.254: bytes=32 time<1ms TTL=255
Reply from 192.168.33.254: bytes=32 time<1ms TTL=255
Reply from 192.168.33.254: bytes=32 time<1ms TTL=255
Reply from 192.168.33.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.33.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 14 Checking the accessibility of a workers computer to a server

5 CONCLUSION

The current situation in the company was analysed for the thesis. It was found out that the computer equipment was outdated it could no longer cope with the demands placed on it.

The current computer network used D-Link equipment and this is not secure according to NKSC recommendations. A new more secure computer network was implemented. For employees and general security purposes video surveillance system was installed.

For security measures the computer network was separated in three different segments (management, employees and guests). Access-lists were configured also which permitted guests to access company’s data. Also, employees could not access network equipment if there was an inside threat.

The computer network configuration was tested out using “Cisco Packet Tracer” virtual environment. The tests results showed that the configured computer network was working properly, unfortunately the firewall in this environment could not be configured and tested. Firewall configuration and testing should be carried out in a real-life environment.

REFERENCES

Analysis of D-Link products. n.d. NKSC report. Available at: https://www.nksc.lt/doc/biuleteniai/Yandex-DNS-tyrimas.pdf [Accessed 06 February 2023]

CityBee database hacker: companies never learn. 2021. Verslo žinios. Web page. Available at: https://www.vz.lt/technologijos-mokslas/2021/02/17/citybee-duomenu-baze-paviesines-isilauzelis-kompanijos-niekaip-nepasimoko [Accessed 06 February 2023]

Dynamic Host Configuration Protocol. 2021. Microsoft. Article. Available at: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top [Accessed 29 January 2023]

Everything about processors. n.d. Microsoft. Web page. Available at: https://support.microsoft.com/lt-lt/windows/viskas-apie-procesori%C5%B3-cpu-06dc72ec-3de2-4eb8-8cc2-7e5f2417b90b [Accessed 25 January 2023]

Fines and other sanctions following the General Data Protection Regulation (GDPR). 2018. National data protection inspectorate. Web page. Available at: https://vdai.lrv.lt/lt/naujienos/baudos-ir-kitos-sankcijos-pradejus-taikyti-bendraji-duomenu-apsaugos-reglamenta-bdar [Accessed 07 February 2023]

Francom, S. 2022. How Fast Should My Business Internet Be? Business.org. Feature. Available at: https://www.business.org/services/internet/business-internet-speed/ [Accessed 14 February 2023]

Network Address Translation. n.d. Avi Networks. Web page. Available at: https://avinetworks.com/glossary/network-address-translation/ [Accessed 25 January 2023].

PassMark Software. n.d. PassMark. Webpage. Available at: https://www.passmark.com/ [Accessed 29 January 2023]

Power over Ethernet. n.d. INTELLINET NETWORK SOLUTIONS. Web page. Available at: https://intellinetnetwork.eu/pages/power-over-ethernet [Accessed 01 February 2023].

Russian-origin software components pose security threat. 2022. NKSC article. Available at: https://www.nksc.lt/naujienos/rusiskos_kilmes_programines_irangos_komponentai_ke.html [Accessed 10 February 2023]

What is VLAN? n.d. Study CCNA. Web page. Available at: https://study-ccna.com/what-is-a-vlan/ [Accessed 29 December 2022]

What is a Hardware Firewall? Hardware vs. Software firewalls. n.d. Fortinet. Webpage. Available at: https://www.fortinet.com/resources/cyberglossary/hardware-firewalls-better-than-software [Accessed 01 March 2023]

What is a Network Access Control List? n.d. Fortinet. Web page. Available at: https://www.fortinet.com/resources/cyberglossary/network-access-control-list [Accessed 05 February 2023]

What is a VPN, and why do business use them?. n.d. CloudFlare. Article. Available at: https://www.cloudflare.com/learning/access-management/what-is-a-business-vpn/ [Accessed 06 February 2023]

What is a VPN, and why do business use them?. n.d. CloudFlare. Article. Available at: https://www.cloudflare.com/learning/access-management/what-is-a-business-vpn/ [Accessed 19 January 2023]

What is computer networking? n.d. Amazon. Web page. Available at: https://aws.amazon.com/what-is/computer-networking [Accessed 19 January 2023]

What is networking? n.d. IBM. Web page. Available at: https://www.ibm.com/topics/networking [Accessed 19 January 2023]

Windows 10 versions. n.d. PCMag. Webpage. Available at: https://www.pcmag.com/encyclopedia/term/windows-10-versions [Accessed 15 January 2023]

Windows 8.1 end of support and Microsoft 365 apps. 2023. Microsoft. Article. Available at: https://learn.microsoft.com/lt-lt/deployoffice/endofsupport/windows-81-support [Accessed 15 January 2023]

List of Figures

List of Tables

Appendices

Appendice 1/1

Device	IP address	Gateway	Subnet mask
Computers	DHCP 192.168.33.1-100	192.168.33.254	255.255.255.0
Router	10.10.10.1	10.10.10.1	255.255.255.240
1 Switch	10.10.10.3	10.10.10.1	255.255.255.240
2 Switch	10.10.10.4	10.10.10.1	255.255.255.240
Firewall	10.10.10.2	10.10.10.1	255.255.255.240
1 Wireless access point	192.168.33.240	192.168.33.254	255.255.255.0
2 Wireless access point	192.168.33.241	192.168.33.254	255.255.255.0
Server	10.10.10.5 (Management) 192.168.33.253 (LAN)	10.10.10.1 (Management) 192.168.33.254 (LAN)	255.255.255.240 (Management) 255.255.255.0 (LAN)
1 Printer	192.168.33.101	192.168.33.254	255.255.255.0
2 Printer	192.168.33.102	192.168.33.254	255.255.255.0
3 Printer	192.168.33.103	192.168.33.254	255.255.255.0
4 Printer	192.168.33.104	192.168.33.254	255.255.255.0
NVR	192.168.20.2	192.168.20.1	255.255.255.240
1 IP camera	192.168.20.3	192.168.20.1	255.255.255.240
2 IP camera	192.168.20.4	192.168.20.1	255.255.255.240
3 IP camera	192.168.20.5	192.168.20.1	255.255.255.240
4 IP camera	192.168.20.6	192.168.20.1	255.255.255.240
5 IP camera	192.168.20.7	192.168.20.1	255.255.255.240
6 IP camera	192.168.20.8	192.168.20.1	255.255.255.240
7 IP camera	192.168.20.9	192.168.20.1	255.255.255.240
8 IP camera	192.168.20.10	192.168.20.1	255.255.255.240