Airidas Mažuolis

COMPUTER NETWORK MODERNIZATION PROJECT FOR A CREDIT REPORTING AGENCY

Bachelor’s thesis

Bachelor of Engineering

Information Technology

2023

XAMK
South-Eastern Finland
University of Applied Sciences

South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Airidas Mažuolis
Thesis title	Computer network modernization project for a credit reporting agency
Year	2023
Pages	60 pages
Supervisor(s)	Matti Juutilainen

ABSTRACT

After several successful business years, the company is expanding their business operations and increasing the number of employees. To accommodate additional personnel a bigger office will be required. Business expansion and new office building is a good chance to analyse company's current network equipment and upgrade any outdated network devices or other IT hardware.

The theory part of the thesis covers commonly used network topologies and networking protocols that will be used to design a new computer network. Additionally theoretical part covers surveillance systems analysis, operating systems analysis, and goes over the current company's IT equipment condition.

The project implementation part covers selection process of the new office network and IT equipment, and design choices for physical and logical topologies. Implementation part also includes the configuration and testing of a mock network using „Cisco Packet Tracer" software.

The end result of the project is a working computer network designed according the company needs.

Keywords: LAN, basic network configuration, computers, servers, routers, switches, IP cameras, network design

CONTENTS

Abbreviations

RAM – Random access memory

AP – Wireless access point

SSD – Solid state drive

HDD – Hard disk drive

IP – Internet protocol is a set of rules that describes how information sharing works over the internet. An IP address allows to identify a network or device on the Internet

POE – Power over Ethernet is a technology that allows to supply power to devices via Ethernet cable

HSRP – Hot standby router protocol allows to configure a fault tolerant default gateway for the network

NAT protocol – Network address translation protocol allows to map several local IP addresses to one public address

SNAT protocol – Stateful network address translation protocol allows to store and provides a way to share the information about all communication sessions between local clients and external networks

STP – Spanning tree protocol was created to prevent packet loops in networks

MAC address – Media access control address is an unique physical address assigned to each device

LAN – Local area network

VLAN – Virtual local area network technology allows to split local area networks into smaller isolated groups

UDP – User datagram protocol is a communication protocol that is used to establish low-latency and loss-tolerant connections

TCP – Transmission control protocol is a communication protocol that is used to establish and maintain a connection by which application can exchange data without any losses during transmission

OS – Computer operating system

1 INTRODUCTION

Today the modern world revolves around the Internet. The Internet itself consists of various separate devices or smaller local computer networks. A computer network is a group of devices that are interconnected together to form one larger network. Devices that are connected to the same network have a way to share and access various resources located on other network nodes. The first working computer network was created in the late 1960s and was called “ARPANET”. This computer network was used by government researchers to share information between labs as computers of that time were large and very difficult to move. From that time computer networks expanded and improved, now they can be found in every organization no matter its size. Organizations use computers networks to connect their employees and resources together for easier access and management. Disruptions in computer network caused by network equipment or other sources can cost hundreds of thousands if not millions to the company, so a properly configured computer network is a corner stone of today’s world.

The aim of this project is to modernize a computer network of an imaginary international company whose primary field of activity is credit reporting. This company is located in Kaunas, Lithuania. Currently the company employs 50 people. These past few years have been very successful for the business, hence the company’s director decided to expand business operations and personnel size. To support that goal a new office will be required. Moving to new office space will be used as a chance to upgrade outdated equipment.

Credit reporting involves processing large amounts of sensitive information. Therefore, the company’s employees have to perform tasks that are intensive in terms of random-access memory (RAM) usage. Currently employees who work with data analysis complain about long application load time. Data analysts are not the only ones who complain about slow equipment, some complaints were also received from programmers. Increased loading time reduces their efficiency.

Besides the expansion plans the company requests that the new office premises would be monitored by video cameras.

2 THEORY

This chapter covers most common network topology design choices in computer networks, network protocols that will be used during new computer network implementation and a general overview of the company’s current IT equipment.

2.1 Network topologies

In essence a network topology is the arrangement of physical devices in relation to each other. There are numerous ways a network could be planned and each of the designs have their own pros and cons. The most common network topology types include: star, tree, mesh, hybrid, bus and ring topologies. Bus and ring topologies are somewhat outdated and they no longer see frequent use, so the thesis will focus on the first four network topologies.

2.1.1 Star topology

The ease of use and durability of the star topology made it the most common network topology in local area networks. In this topology every device in the network is directly connected to a central network device that is most likely located in a server room.

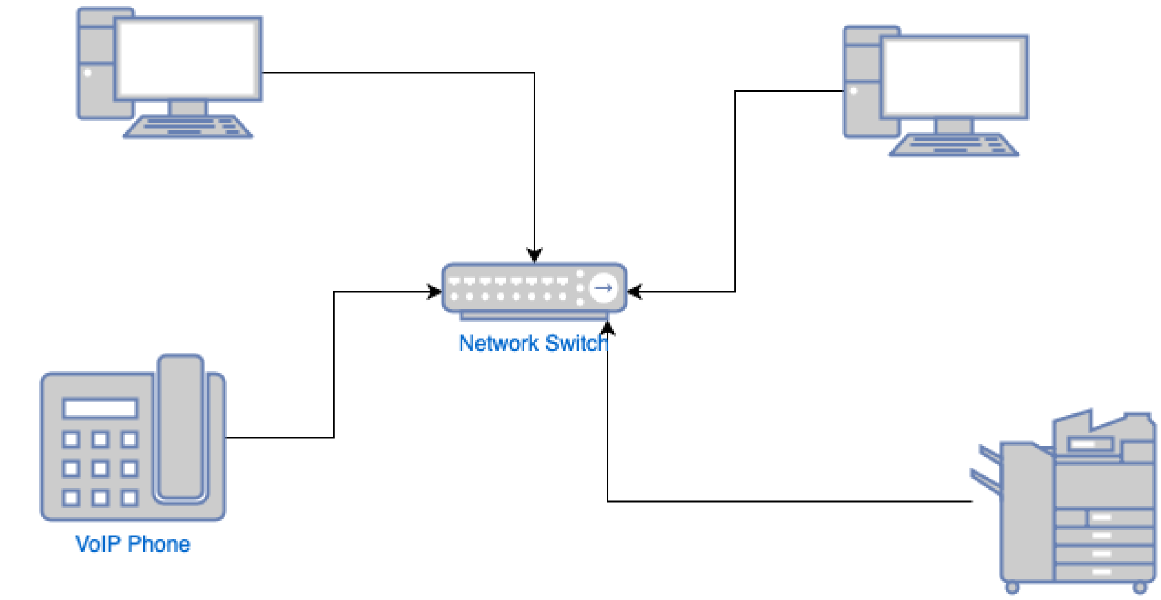


Figure 1. Star topology. Chapman, D. 2021.

The advantage of the star topology is that it is very easy to set it up, and because of its simplicity, it is very straightforward to manage. To isolate a problem that has occurred, the network engineer simply needs to know which server room or server's panel the specific end device is connected to. One of the biggest disadvantages is that while star topology is durable, if the central network device malfunctioned, then all devices that are connected to that network device would lose connection to the network. Which, depending on the company’s size and activities, could be catastrophic. Another disadvantage is the required amount of cabling, since each end device needs to have a separate cable running back to the network device, which could get messy when there is a large number of devices (DNSstuff 2019).

2.1.2 Tree topology

Tree topology is not commonly used, but this topology finds its use when a combination of scalability or hierarchical setup is required between two networks, in this topology there is central device that functions as the networks “trunk”, with other devices extending from it outwards like “branches”.

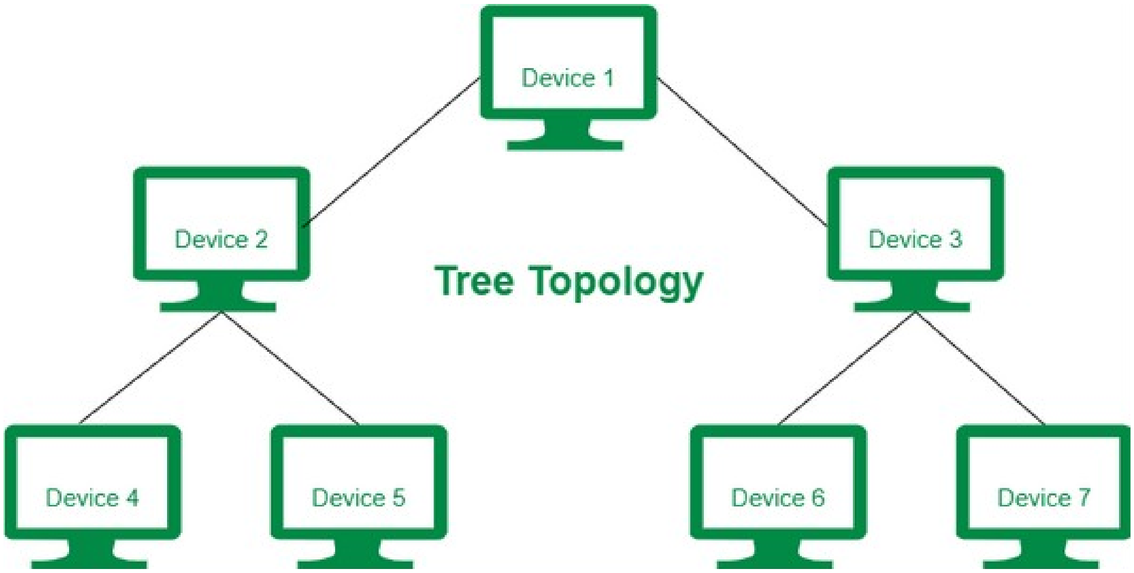


Figure 2. Tree topology. GeeksforGeeks. 2022.

Unlike star topology, where all nodes are connected to central device, tree topology has a parent-child hierarchy. In a sense tree topology is a combination of star and bus topologies and offers the advantages of both. Since this network topology is based on main backbone cable, if a cable or end device experiences failure, it will not bring down the whole network unless the malfunctioning device is the central device. In that case, instead of the whole network going down only the connectivity between the “branches” would be lost and the connectivity between devices within the “branches” would remain. Another advantage is the ease of expansion. Since this topology follows hierarchical pattern as long as there are available ports and cables, adding secondary devices to the network poses no issues. Tree topology is not perfect and has its own disadvantages. Because tree topology is a combination of star and bus topologies, its installation is a difficult process. And due to the large size of this topology, its maintenance takes up a lot of time which significantly increase the overall price of this topology (DNSstuff 2019).

2.1.3 Mesh topology

A mesh topology is an intricate structure of point-to-point connections where all the nodes are interconnected.

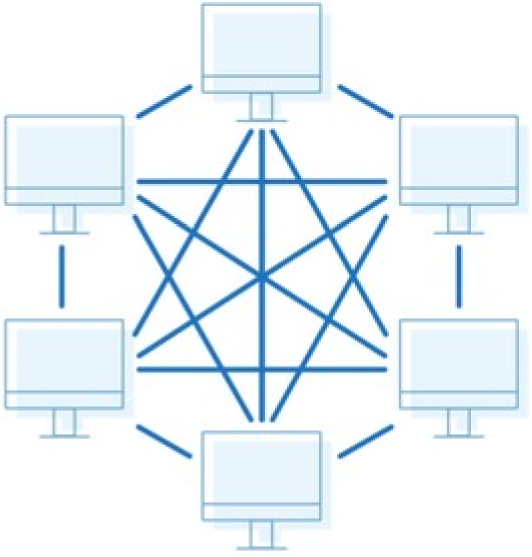


Figure 3. Mesh topology. DNSstuff. 2019.

Mesh networks can be either partial mesh or full mesh. Partial mesh topologies are mostly interconnected with few nodes having only two or three connections, while in a full mesh topology every computer in the network is interconnected to each other. The advantage of mesh topologies is that they are extremely reliable. Their complexity and inter-connectivity make the network resistant to failure as each device has several redundant paths for data transmission. The disadvantages are that mesh topologies are expensive and labor-intensive, each device requires several separate cables and configuration, which results in much higher setup costs (DNSstuff 2019).

2.1.4 Hybrid topology

As the name suggests, hybrid topologies are a combination of two or more different topologies.

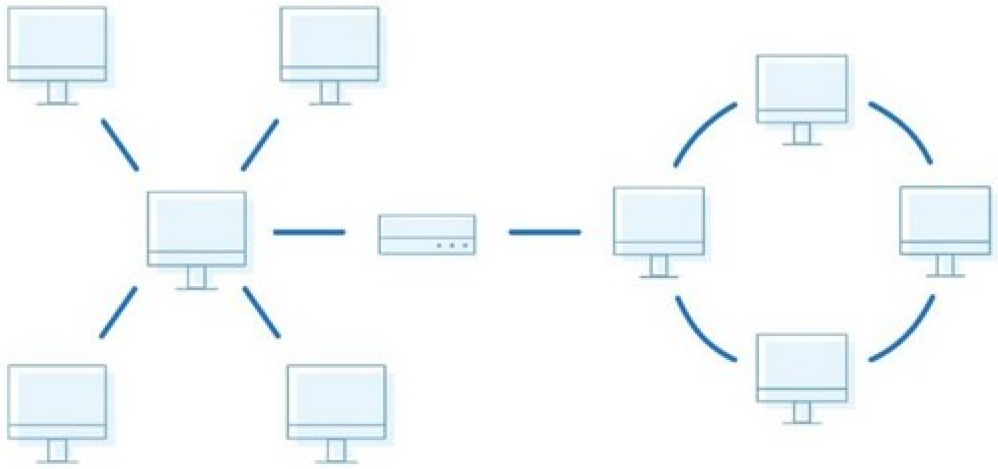


Figure 4. Hybrid topology. DNSstuff. 2019.

This type of topology is more commonly found in larger companies. Hybrid topology is very flexible as any of previously mentioned topologies can be combined depending on the needs of a business or the users. The number of computers, their locations and desired network performance also factors into the decision. Hybrid topology is not a concrete topology, it does not have its own advantages or disadvantages, but inherits them from the combined topologies (DNSstuff 2019).

2.2 Protocols and network technologies

This sub-chapter covers all protocols and network technologies that will be used during the project’s implementation.

2.2.1 Hot standby router protocol

Hot standby router protocol (HSRP) is a Cisco company’s proprietary protocol, which provides redundancy for a local subnet (Cisco 2022). HSRP works by using two or more physical routers to create an illusion of a single virtual router.

In HSRP group each member is assigned the same group ID. One of the group members gets elected as the active router while others are assigned a standby role. At any given time, there can only be one active router which is responsible for forwarding the traffic. The active router periodically sends out ”hello” messages to other standby routers. If the active device malfunctions, the messages stop. This triggers the ”hold-down timer”, after which the standby router will become the active router and will start forwarding the traffic of the local hosts. This is known as ”preempt”. If the original active router comes back online, the priority of the standby router gets decreased, and it returns the active router role to the original device.

All of the devices in a single HSRP group share one media access control (MAC) address and one internet protocol (IP) address, which also fulfills the role of the default gateway for the network.

2.2.2 Spanning tree protocol

The main purpose of the spanning tree protocol (STP) is to prevent the data packets from looping in the network which can affect the networks performance and even bring it to a near halt. Data packet looping usually occurs in local area networks that contain redundant paths. Mesh type network topologies are the most susceptible to these packet ”storms” as all devices in this type of topology are interconnected and have multiple redundant paths.

STP monitors all the network links, identifies redundant connections and disables the ports that can lead to looping. When spanning tree protocol is enabled, each network switch learns which devices belong to which network segment by sending out ”first-time” messages, which enables the network switch to learn about the network on its own without intervention from the network administrator.

To enable network switches to control the flow of traffic and prevent looping, it is crucial that the switches continuously update their information tables and keep track of changes in the network. To do this, they exchange bridge protocol data units (BPDUs). BPDUs are data messages that provide switches with network information that is used to carry out spanning tree protocol operations. On each STP-enabled device a specifically designed algorithm uses BPDUs to identify redudant links and to calculate the best path to forward the messages (Cisco Meraki 2021).

2.2.3 Dynamic host configuration protocol

Dynamic host configuration protocol (DHCP) is a client and server side protocol that automatically provides network devices with an IP address and other related configuration information. This protocol is very useful in larger networks with hundreds of end devices as it eliminates the need to manually assign each device an IP address. DHCP server maintains a pool of IP addresses and a list of already leased IP addresses. DHCP server assigns an address to any DHCP-enabled client when it appears on the network. Because the IP addresses are only “leased” when they are no longer in use they are returned to the pool for reallocation (Microsoft Learn 2021).

For a device to receive an IP address from DHCP server first it must send out a broadcast message called “DHCPDISCOVER”, this is because newly connected device is not aware of the current network topology and DHCP server’s location. The network itself directs that message to the appropriate DHCP server. Then the server determines the appropriate IP address and sends out an “OFFER” packet back to the client, which responds with a “REQUEST” packet for that IP address and finally the server sends out an “ACK” packet confirming that the client has been given an IP address (Weinberg 2022). Even though it sounds like there is a lot of back-and-forth communication, in reality this process is quick and automatic.

2.2.4 Network address translation protocol

Network devices are identified by their IP address. IPv4 protocol allows for up to 4 billion possible IP addresses, which seemed a lot when it was first launched. Over the years the internet’s popularity exploded, and while not all people on Earth use the internet most of those who do, have multiple devices that can connect to the internet. Therefore, the number of devices greatly surpasses the available addresses.

Network address translation (NAT) protocol is a way to map multiple local private addresses to a single public one which helps with IP address conservation and keeps more public IP addresses available for organizations or for devices that require it. This protocol is often used by home routers and by organizations that want multiple devices to employ a single IP address.

When an outbound packet reaches the router, the router first changes the outgoing IP address from private address to a public address and then sends it out. If the outgoing packet would keep the private address, the receiving server would not know where to send information back to. With NAT protocol, the information would make it back to the device using routers public address. The router keeps a network address translation table and uses the information in it to direct the returning packet to the correct end device.

2.2.5 Virtual local area network

A local area network (LAN) is a group of various network devices that share the same physical network, for example all devices in a school are part of a local area network. Virtual local area network (VLAN) is a way to divide LAN into separate groups and isolate the network traffic for each group. By using VLAN these things can be achieved:

- **Improved performance**

Virtual area networks improve the performance by blocking the traffic which was not meant for that VLAN. This reduces the amount of network traffic that endpoint devices have to process. Also, it is possible to set up traffic-handling rules, for example a rule to prioritize video traffic to guarantee meeting room’s equipment performance.

- **Improved network security**

By separating local area network into smaller groups, network administrators have a higher degree of control over which devices have access to specific networks or resources. For example, a separate guest network that would have no access to internal company's network.

- **Easier network administration**

Grouping network devices allows to simplify devices non-technical administration. For example, all data analytics computers would be assigned to one group and all software engineer's computers to another.

VLANs are identified by their VLAN ID. Each network switch port can have one or more VLAN IDs assigned to it. When a data frame is received from connected host, it has no VLAN ID tag. The network switch adds the tag and then forwards tagged frames to its destination MAC address. Once the frame reaches its destination switch port, the tag is removed and the frame is forwarded to the endpoint device (Slattery & Burke 2022).

2.2.6 Access control lists

Access control list contains rules that control network traffic by permitting or denying the inbound or outbound data frames. Similarly, to virtual local area networks, ACLs use those pre-defines rules to decide whatever received frame should be forwarded or not, which helps to improve the network security by decreasing network traffic and controlling user access. Originally ACLs were the only way to achieve firewall protection. Today there are many types of firewalls and alternatives to access control lists. But companies still continue to use ACLs in conjunction with other technologies. There are several different types of access control lists, the main ones being “standard” and “extended”. Standard ACLs can only evaluate packet source IP address, while extended access control lists allow for more configuration, in exchange standard ACLs use less computing power (ITGlobal, n.d).

2.3 Surveillance systems analysis

A video surveillance system is a network of cameras, monitors, and recorders. Cameras can be found inside or outside the building. Most common reason for business to set up a video surveillance system is to ensure their properties and employees safety.

Video surveillance systems consist of 4 components:

- Video cameras
- Storage
- Network video recorder (NVR)
- Other network elements such as switches and routers.

IP cameras capture video information, encode it, compress it, pack it into IP packets and send the recording data to a video recorder over wireless or wired connections. In wireless systems, cameras only need to be connected to a power source and the data itself is transmitted via the wireless network. These days wired systems often use the power over Ethernet (POE) technology. This technology allows the camera to receive power and transmit data over the same network cable. Some NVR devices often come with integrated data storage and others use cloud-based solutions. But they all fulfill the same function, which is to store the footage for later viewing.

NVR often comes with software that allows to set up cameras, perform on-boarding and provides video viewing capabilities. However, video viewing software provided by NVR manufacturers is usually very limited, for advanced viewing features like alerts and face detection, a video management system is required.

2.4 Operating system analysis

During 2021 Autumn, Microsoft released the latest Windows 11 OS, which was slated to replace Windows 10 released in 2015. However according to statistics (Kunert 2022) by November, 2022, only 15% percent of personal computers across the globe use Windows 11 daily. On January 2023 Microsoft announced that they are ending official Windows 10 sales by the end of the month (Noureen

2023). Since that day the only legal way to acquire a Windows 10 license is by buying the license from third-party retailers or by buying a device that comes with Windows 10 pre-activated.

From information provided in the Table 1 below, we can see that Window 11 OS requirements for personal computer components practically doubled comparing to Windows 10.

Table 1. Windows 10 and 11 requirements. Microsoft Windows. n.d.; Microsoft Support. n.d.

	Windows 11	**Windows 10**
CPU	>1 GHz, >2 Cores, 64-bit architecture	>1 GHz
RAM	>=4 GB	>=1 GB for 32-bit architectures, >=2 GB for 64-bit architectures
Software	UEFI, Secure boot	-
TPM	2.0	-
GPU	Must support DirectX12 and WDDM 2.0 drivers	Must support DirectX9 and WDDM 1.0 drivers

This means that computers with older hardware might not be capable of running Windows 11 operating system. But during the same announcement Microsoft has stated that they will provide support for Windows 10 OS until 2025. Meaning that keeping the old computers with Windows 10 operating system will not pose any security risks.

2.5 Storage technologies analysis

There are several different types of storage solutions for personal and office use computers. One common type is hard disk drives (HDDs), and another is solid state drives (SSDs). Usually, SSDs can be found with two different types of connectors, serial AT attachment (SATA) and peripheral component interconnect express (PCIe) connectors. Latter connector type is based on point-to-point architecture and is used in NVMe SSDs. PCIe allows to use multiple data lanes for data transfers, which in turn increases the possible bandwidth. While SATA

SSDs can only use one data transfer lane. Hard disk drives only use SATA type connectors.

Solid state storage is significantly faster than hard drives. The main reason for the speed differences is that hard disk drives use a spindle that has to move to data’s physical location on the disk. While solid state drives use floating gate transistors which use electrical charge to store data. Additionally, the lack of moving parts makes SSD a more reliable storage solution. Information about the storage solutions speeds is provided in the Table 2 below.

Table 2. Storage speed comparison. Router-switch. 2018.

	SATA SSD		**NVMe SSD**		**HDD**
	2.0	**3.0**	**2.0**	**3.0**	**-**
Connector speed	3 Gbps	6 Gbps	8 Gbps (x2) 16 Gbps (x4)	16 Gbps (x2) 32 Gbps (x4)	-
Maximum real speed	~275 Mbps	~560 Mbps	~780 Mbps ~1560 Mbps	~1560 Mbps ~3120 Mbps	~150 Mbps

Usually, Hard disk drive storage is about 3.5 times slower than any “SATA 3.0” type of storage. And “NVMe 3.0” type storage is 3-6 times faster than the “SATA 3.0” storage solutions.

2.6 Company’s situation analysis

This chapter will cover company’s current IT and network equipments situation and their state.

2.6.1 Current IT equipment in the company

Currently the company uses “HP EliteDesk 800 G1 SFF” desktop computers. Specification for the computers is provided in Table 3 below.

Table 3. Computers used in the company

HP EliteDesk 800 G1 SFF specification					
Operating system	**Processor**	**Memory**	**Storage**	**Graphics processor**	**Conclusion for further use PASS / FAIL**
Windows 10 Enterprise	Intel 4th Gen Core i5-4570 processor	8 GB 1600-MHz DDR3 SDRAM	256 GB SSD	Integrated Intel HD Graphics	PASS
Windows 8.1		16 GB 1600-MHz DDR3 SDRAM			

Some of these computers were partially customized according to employees needs, although the modifications are very limited. Even with new modifications, computers rarely have a noticeable improvement in performance and application runtimes often stay the same.

The most likely key causes for these issues are severely outdated core components and rapidly increasing resource requirements of the applications. One of the outdated components would be the motherboard. Motherboards themselves never directly influence the device performance as motherboards purpose is to bridge all of the components together. Older motherboard models usually lack proper connectors for newer components, which influences what parts can be used as a replacement. For example, the upgrades would be limited to older RAM modules with a lower frequency or older processors.

Currently the company has 50 computers. Almost all devices except 10 use Windows 10 Enterprise operating system. The 10 aforementioned devices use Windows 8.1 OS, which is no longer supported. The distribution of computers and their components is proved below in Table 4.

Table 4. Distribution of computers throughout the company

CPU	**CPU benchmark according to: https://www.cpu-monkey.com/en/**	**RAM**	**Storage**	**Graphics processor**	**OS**
Intel 4th Gen Core i5-4570 3.60 GHz (100%)	2841	8 GB 1600-MHz DDR3 SDRAM (~63%)	256 GB SSD (100%)	Integrated Intel HD Graphics (100%)	Windows 8.1 (~20%)
		16 GB 1600-MHz DDR3 SDRAM (~37%)			Windows 10 (~80%)

Since these computers still function properly, they can be repurposed. During the course of the project, new and more powerful computers will be selected for the new workstations, employees whose job specifications require more powerful computers will be moved to work with the new devices. While the old computers will be left for those employees whose job functions will not be hindered by slower devices.

The company’s servers use Windows Server 2008 R2 operating system, which is no longer supported and has stopped receiving general and security updates. The servers OS will need to be updated as well.

2.6.2 Current networking equipment in the company

“CISCO SG110-24HP” network switches were quite a common and popular option for networking solutions, but since autumn of 2021 the sale of these devices was discontinued and it’s no longer possible to buy this switch model. The device specification is provided in Table 5 below.

Table 5. Switches used in the company

Device	Device model	Number of ports	Switching capacity	Forwarding capacity	Conclusion for further use PASS / FAIL
Switch Nr.1	CISCO SG110-24HP	24	48 Gb/s	35.7 mpps	PASS
Switch Nr.2					
Switch Nr.3					

Manufacturers will support these devices and provide them with security updates until 2026 (Cisco, n.d.). Each switch has 24 Ethernet ports, 12 of which have power over Ethernet (POE) functionality which allows to provide power to various devices via an Ethernet cable. Currently the company has 3 switches of this model. The total amount of available ports adds up to 72. During the course of the project an office surveillance system will be installed and additional workstations will be added, thus the current number of available switch ports will not be sufficient in the future. It will be necessary to purchase an additional network switch.

The company uses a singular “Cisco 2951” model router in their network. General information about the device is provided in Table 6 below.

Table 6. Routers used in the company

Device	Device model	Ports	Security	RAM	Conclusion for further use PASS / FAIL
Router Nr.1	CISCO 2951	3 10/100/100 Gigabit Ethernet ports, 4 EHWIC slots, 3 DSP slots, 1 ISM slot	Faster VPN encryption, multiple VPN types, integrated threat management with Cisco IOS firewall, authentication using multiple authentication methods	512MB DRAM	FAIL

These devices were officially withdrawn from the market on December 2017. Under normal, circumstances “Cisco” devices receive security and general updates for five years after the end of the sales date. This means that this model devices are no longer supported by the manufacturer and needs to be replaced as soon as possible as the chances of these devices being compromised in a cyber-attack increases exponentially every day. Furthermore, the lack of general updates can cause problems in normal day to day operations of the network. In business environments such risks are unacceptable.

2.6.3 Current internet plan

Currently the internet for the company is provided by "Telia" telecommunication company that operates within the country. The internet plan from “Telia” offers speeds of up to 300 Mbps. But considering the future needs of the company, current internet speeds will no longer be enough, this decision came after referencing the information provided in Table 7 below.

Table 7. Internet speed criteria. Morrison. 2022.

Number of devices	**Internet speed**	**Use cases**
5-10	75 Mbps	Video streaming, frequent file transfer.
10-15	150 Mbps	Video conferences, frequent use of cloud services
15-20	250 Mbps	Conferences, management of the servers
20-30	500 Mbps	Constant usage of cloud services, management of multiple servers, frequent uploads of data backups to online storage
30+	1000 Mbps	Majority of office tasks with limited or no problems

From the gathered information the company will need an internet plan that offers internet speeds up to 1000 Mbps.

3 PROJECT IMPLEMENTATION

This chapter is divided into three parts: Design stages, network configuration, and network configuration testing. The first part covers equipment selection, surveillance system design, new network design, updating operating systems, and new internet plan selection. The second part covers network logical topology design and configuring mock network using packet tracer application. The third part will cover the testing of said network configuration.

3.1 Design stages

The implementation planning will start by selecting and preparing equipment for the new workstations. Next stage would be to design surveillance system, which will be done by identifying the areas that would need to be monitored and then identifying the suitable locations for their installation. Lastly we can select the cameras. The cameras should be able to provide desired video quality and fit specific parameters. Third stage would be the network equipment preparation. Said preparation includes their acquisition and configuration. And lastly a new internet plan must be chosen.

3.1.1 Computer hardware selection

The main criteria for the computer selection are: the processor, random access memory and storage. For office use computers, various sources recommend a CPU with test score of more than 4500 points. New computers must meet this requirement. For CPU comparison, the “Cinebench R23 Multicore” CPU test results will be used. Random access memory should be equal or larger than 8 GB. The storage must have a capacity larger or equal to 250 GB. The graphics processor unit won’t be taken into the consideration during the selection.

Table 8. Computer selection

Computer model	**CPU**	**CPU BENCHMARK (MULTICORE)**	**RAM**	**Storage**	**Price**
Requirements	**-**	**>4500**	**≥8 GB**	**≥250 GB SSD**	**-**
Asus Expertcenter D500SA	Intel Core I5-10400 2.9 GHz	8164	8 GB 2666 MHz DDR4 RAM	256 GB PCIe NVMe M.2 SSD	588.31 euro
HP XPS Desktop	Intel Core I5-12400 2.5 GHz	12454	16 GB 4400 MHz DDR5 RAM	256 GB PCIe NVMe M.2 SSD	769.33 euro
Lenovo ThinkStation P340 SFF Workstation	Intel Core I5-10400 2.9 GHz	8164	8 GB 2667 MHz DDR4 RAM	1 TB 7200 RPM HDD	1564.92 euro

“Asus Expertcenter D500SA” is the cheapest option and it satisfies all the requirements. This computer’s processor is almost 3 times more powerful than the processor in the old computers. The results are 8164 and 2841 points respectively. SSD capacity is the same in both computers, but “Asus Expertcenter D500SA” computer has NVMe type SSD, which is faster than SATA type SSD.

“Lenovo ThinkStation P340 SFF Workstation” is the most expensive option and also the least suitable when considering the company’s needs. In terms of the components, it is similar to the “Asus Expertcenter D500SA” with few key differences. Instead of an SSD this model has an HDD storage as well as a dedicated video graphics processor unit.

“HP XPS Desktop” computer is cheaper than “Lenovo ThinkStation P340 SFF Workstation” and a bit more expensive than “Asus Expertcenter D500SA”, but it also has components that outperform the first two computers.

After careful deliberation it was decided that “HP XPS Desktop” computer is the best choice for this project. Larger size random access memory and a more powerful processor will provide the necessary processing power required by the data analysts and programmers who will be using these computers.

Next step would be the selection of monitors. All of the information about monitors and their selection criteria is provided in Table 9.

Table 9. Monitor selection

Monitor model	**Screen diameter**	**Screen brightness**	**Resolution**	**Refresh rate**	**Response time**	**Price**
Requirements	**≥24”**	**≥250 cd/m^2**	**≥1920x1080**	**≥60 Hz**	**≥5 ms**	**-**
Acer KA270H	27”	300 cd/m^2	1920x1080	120 Hz	4 ms	199.72 euro
BenQ GW2480	24”	250 cd/m^2	1920x1080	60 Hz	5 ms	184.34 euro
Asus VZ249HE	24”	250 cd/m^2	1920x1080	60 Hz	5 ms	164.66 euro

“Acer KA270H” monitor is the superior choice compared to other options. But for simple office work simpler monitors will suffice. The other two monitors have the same specifications, the only difference is the prices. For this reason, “Asus VZ249HE” was chosen for this project.

During the course of the project 80 new workstations will be prepared for use. Currently the company has 50 functional computers that were deemed too slow. 15 of those computers will be modernized and reused. It will be necessary to buy

65 units of “HP XPS Desktop” computers and 80 units of “Asus VZ259HE” monitors as the new workstations will use 2-3 monitor setups.

3.1.2 Network hardware selection

All of network hardware will be installed in the server room. The new network switch will be used together with the old ones. Below Table 11 lists switches that were considered and the criteria they must meet. The new routers will completely replace the old one. The network hardware must be new and meet modern computer networking standards. Criteria for routers and the selection options are provided in Table 10 below.

Table 10. Router selection

Router model	**RAM**	**Flash memory**	**Bandwidth**	**Number of ports**	**Supported protocols**	**Does the manufacturer meet the Transatlantic values?**	**Price**
Requirements	**>512 MB**	**>256 MB**	**>75 Mbps**	**>3 10/100/1000 Ethernet ports**	**ACL, NAT, HSRP or VRRP**	**YES**	**-**
Cisco 4331	4 GB	4 GB	100 - 300 Mbps	3 10/100/1000 Ethernet ports, 2 SFP ports ir 1 ESMS	ACL, NAT, HSRP and VPN	YES	1605.39 euro
Juniper	32	-	20 Gbps	8	ACL,	YES	6126.

MX150	GB			10/100/1000 Ethernet ports, 2 SFP+ ports and 2 SFP ports	NAT and VRRP		28 euro
Mikrotik CCR1036-8G-2S+EM	8 GB	-	28 Gbps	8 10/100/1000 Ethernet ports	NAT, VLAN and VRRP	YES	1376.45 euro

“Juniper XM150” router is the most expensive option, but it is also the most powerful one with the highest number of available ports. This device does not support one of the required protocols. Therefore, this device is not suitable for this project.

Normally “Mikrotik CCR1036-8G-2S+EM” router would be a better choice than the “Cisco 4331” router, however the “Cisco” device has several advantages. One of those advantages is the Enhanced Service Module Slot (ESMS) port. This port allows to increase the number of existing ports to 24. Such expansion options while not necessary at the moment may come in handy in the future. Additionally, the “Mikrotik CCR1036-8G-2S+EM” router does not support all of the necessary protocols. Therefore the “Cisco 4331” router will be chosen to implement this project.

Table 11. Switch selection

Switch model	**MAC address table size**	**Switching capacity**	**Number of ports**	**POE capabilities**	**Does the manufacturer meet the Transatlantic values?**	**Price**
Requirements	**≥ 8K**	**≥ 48 Gbps**	**≥ 24**	**YES**	**YES**	**-**
Huawei S5735-S24P4X	-	128 Gbps	24	YES	NO	706.15 euro
Juniper EX2300-24P	16K	128 Gbps	24	YES	YES	1126.35 euro
HPE Aruba JL684A	16K	128 Gbps	24	YES	YES	725.46 euro

From the data in Table 11 we can see that all of the network switches are quite similar in their characteristics and their prices except for “Juniper EX2300-24P”. Another thing to take note of is that “Huawei” devices are considered unsafe in European Union. So, the choice is between “Juniper” and “HPE Aruba”. As mentioned before these switches are quite similar, so the cheaper option will be selected. That is “HPE Aruba JL684A” switch.

3.1.3 Operating systems installation process

Computers that still use Windows 8.1 operating system will be scrapped for parts, so updating their OS is not necessary. The computers that were selected earlier would come with Windows 11 Home operating system preinstalled. As discussed in theoretical part, due to Microsoft ending the sales of Windows 10 licenses, the only viable choice for new computers would be to acquire Windows 11 Enterprise licenses. Old licenses that are already being used are still valid, so reinstalling operating system for old office computers should pose no problem. Before installing the new operating system, the first step would be to backup all of the important files as OS installation process deletes all of the files on the computer.

The backup step can be skipped with the new computers, because these computers would not have any important files on them. The computers will also have to be connected to the company’s domain controller.

Servers operating systems will also need to be updated in exactly the same way. That is to back up important information so that it would not be deleted and restore it after OS installation. Servers will be updated to use the new Windows OS for servers, which would be Windows Server 2022. This updated operating system includes several important changes and improvements to its predecessor versions. Most important changes are that Windows Server 2022 was built to be more secure, more flexible and have a better support for hybrid operations. The support for hybrid operations makes it easier to use various services provided by Azure cloud services.

3.1.4 Surveillance system design

To design a video surveillance system first we must figure out how many cameras will be required, then the required storage space for the recordings and lastly we can go through NVR device selection process. The NVR device will be connected to a switch with an Ethernet cable. The cameras themselves will have to be connected to the ports that have POE functionality, these ports will either be available on NVR device itself or on the network switches. Additionally, the surveillance system will need a monitor, a mouse, a keyboard and a video management system for advanced viewing features. The peripherals will be taken from unused computers and VMS selection will be covered later.

Camera placement

The placement of the cameras must allow the cameras to film spaces that have been indicated in Figure 5 below.

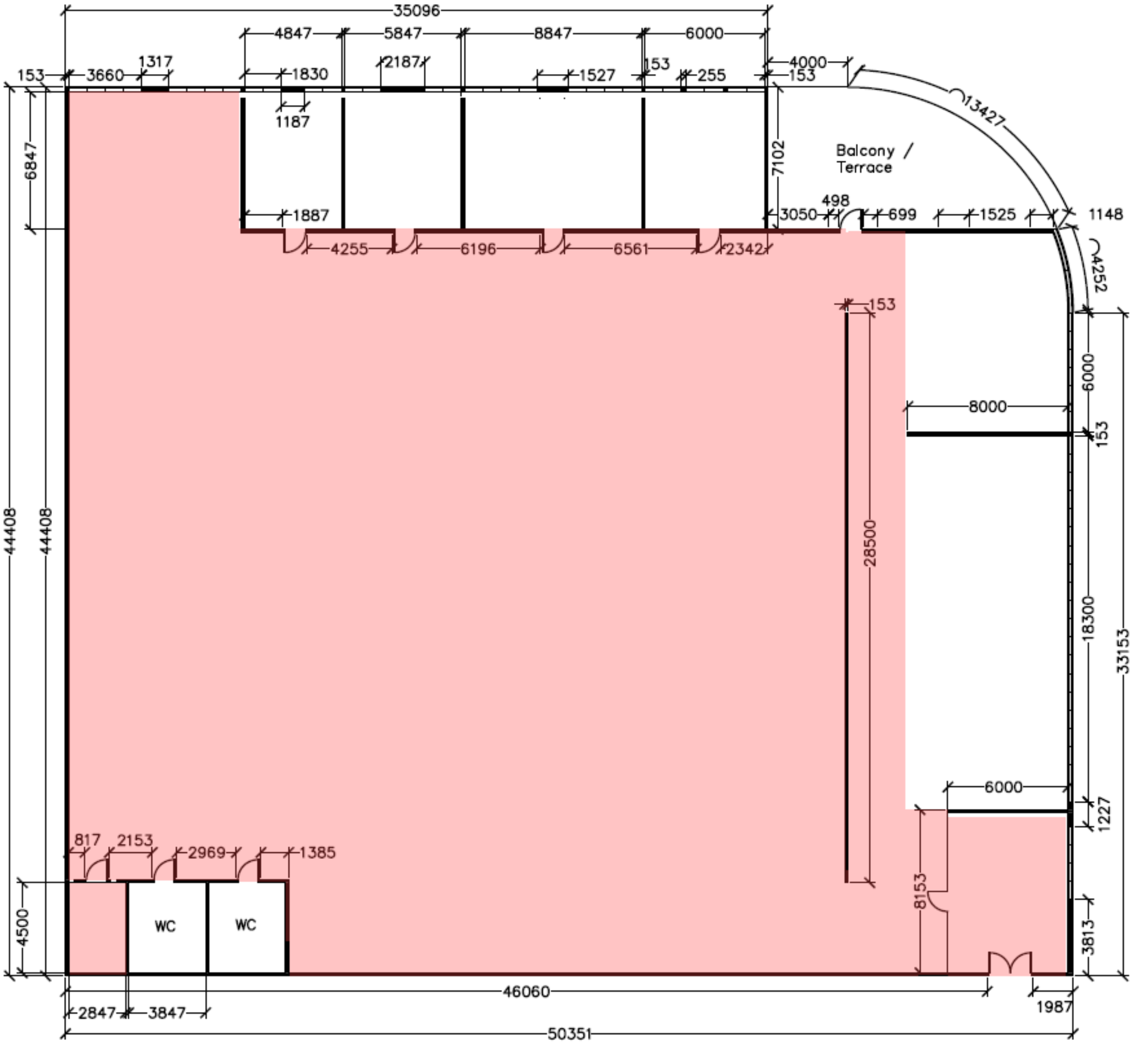


Figure 5. Locations that need to be monitored

To provide 100% coverage a large amount of cameras would be required, which is not cost effective. Therefore, a compromise solution was chosen, which is to place the cameras in the key locations, such as corridors, server room, entrances to the office and reception. The suggested camera locations are marked and shown in Figure 6 below.

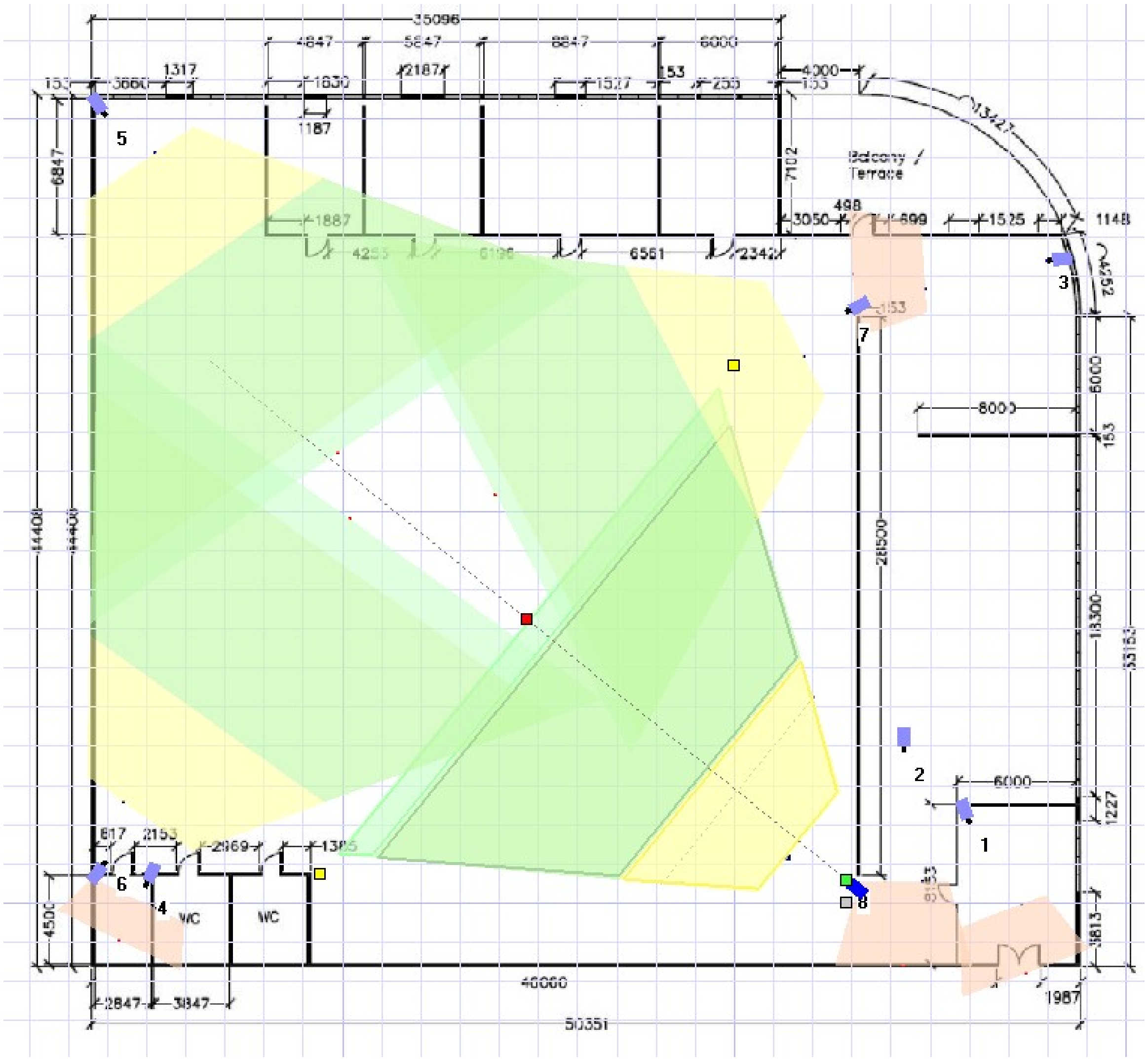


Figure 6. Suggested camera placement

To plan out the camera placement the “IP video system design tool” was used.

Required storage space for recordings

With the prepared camera placement set-up, we would only require 8 cameras in total. With this we can calculate the required storage space for video recordings. The storage capacity will be calculated using the “Seagate Video Storage Calculator” tool. The cameras will perform footage capture 24 hours a day and the footage will be stored for 30 days. The required storage space with these parameters is provided in Table 12.

Table 12. Required storage for recordings based on compression algorithms

Number of cameras	Frames per second	Filming duration per day	Video storage period	Recording resolution	Video quality	Compression algorithm	Required HDD capacity
8	15	24 hours	30 d.	1080p	Average	MPJEG	~80.26 TB
						H.264	~3.89 TB
						H.265	~2.23 TB

Judging from the provided data the cameras should use either H.264 or H.265 compression algorithms which reduce the required storage space under 5 TB.

Cameras and NVR selection

In order to reduce the project cost and to simplify required equipment’s purchase process, it has been decided to purchase a “NVR kit”. These kits come with NVR device itself and cameras. Information about NVR devices themselves and the cameras is written in Table 13 and Table 14 below.

Table 13. NVR kit selection

NVR kit name	Video compression algorithms	Supported number of cameras	Integrated HDD	Does the manufacturer meet the Transatlantic values?	Camera model and their number	Price
Requirements	**H.265**	**≥ 12**	**-**	**YES**	**-**	**-**
Reolink RLK16-820D8-A	H.265 and H.264	16	YES (3TB HDD)	NO	8 x RLC-820A POE	1169.09 euro
Amcrest NV4116E-HS-IP8M-2493EW8-4TB	H.265	16	YES (4TB HDD)	YES	8 x IP8M-2493EW-V2	1093.97 euro
Swann SONVK-1686812D	H.265 and H.264	16	YES (2TB HDD)	YES	12 x NHD-888MSD	1297.08 euro

Table 14. NVR kits cameras overview

Camera model	**Infrared laser distance**	**Resolution**	**Does the manufacturer meet the Transatlantic values?**	**Price**
Requirements	**≥ 15 m**	**1920 x 1080**	**YES**	**-**
RLC-820A POE	18m – 30m	3840 x 2160	NO	80.60 euro
IP8M-2493EW-V2	30m	3840 x 2160	YES	138.89 euro
NHD-888MSD	45m	3840 x 2160	YES	138.89 euro

After considering the provided information, it was concluded that the best NVR kit would be “Swann SONVK-1686812D”. This kit comes with 12 cameras in total, which means left over cameras could be used as a replacement. Additionally, the NVR device itself has 16 POE ports, which would allow to save ports on the network switch. The only downside is a relatively small storage, but that can be solved by purchasing additional HDD.

Video management system selection

As briefly mentioned before for various advanced surveillance features a VMS is required. A video management system can come preinstalled with NVR or bought separately.

Turing vision

According to the developers of the Turing vision (Turing, n.d.) this VMS software offers facial recognition, people detection, vehicle detection, license plate detection and intrusion detection functions. There is also a free demo, but to get access to it a complimentary consultation is required.

Advantages:

- Smart alerts in real-time
- Centralized monitoring
- Compatible with most cameras
- 3 - 10 years warranty

Disadvantages:

- Need to schedule consultation for a demo

Spot AI

Spot AI like Turing vision is an AI based video management system (Spot AI, n.d.). This solution offers similar or the same functionalities as “Turing vision”. Currently this solution price starts at around 1500 euros per year for one location and increases depending on the number of locations and subscription period. There is also a possibility for a custom package, which gives a tailored price depending on specific client’s situation. This VMS solution also has a free demo available, but just like Turing vision it is necessary to book a consultation for it.

Advantages:

- Intuitive and very easy to use software
- 24/7 local storage
- Unlimited users

Disadvantages:

- Rather expensive
- Need to schedule consultation for a demo

Bosch

Bosch video products come with AI based video management solution as built-in solution or bought separately. Bosch video management system software can offer functions such as people counting and vehicle classification (Bosch, n.d.).

Advantages:

- Easy to use and install
- Seamless integration with other systems
- Continuous firmware updates

Disadvantages:

- -

After comparing all 3 options, it has been decided that Turing vision and Spot AI solutions are the best choice for this company's situation. One of the deciding factors was that their solution price can be adjusted depending on the company's needs and both solutions offer free demos. Both solutions require a booked consultation to access the free demo, so the best course of action would be to book demos for both "Spot AI" and "Turing vision" solutions and test them both out, then compare them directly and decide which solution would work best for the company.

IP addresses of cameras and NVR devices will be assigned manually and will be of static type as shown in Table 15 below.

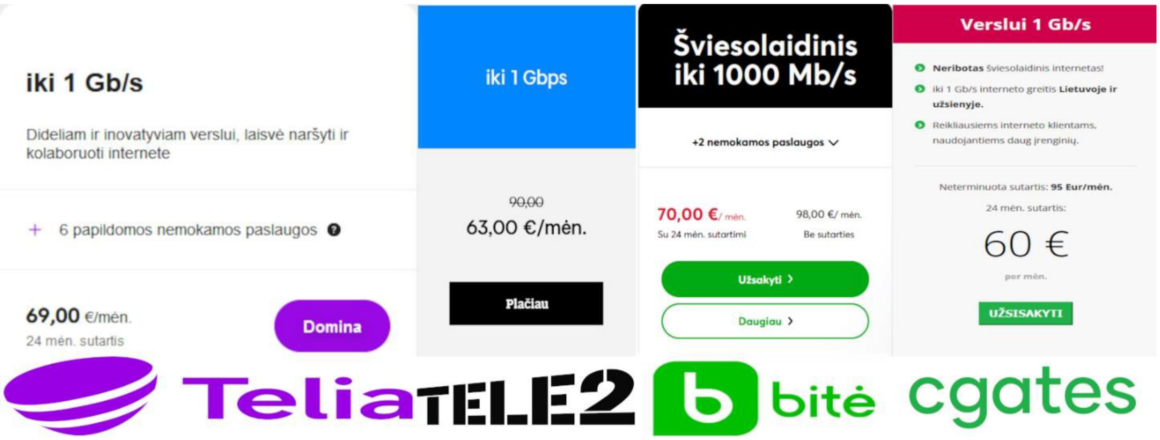
Table 15. Survailance system IP addressing table

Device	IP address type	IP address	Gateway	Subnet mask
IP cameras 1-8	Static	192.168.10.133-143	192.168.10.131	255.255.255.224
NVR	Static	192.168.10.132	192.168.10.131	255.255.255.224

The cameras will be installed inside the office. The NVR device itself will be installed inside reception. All of the cameras will be connected to the NVR unit using CAT6a category LAN cables. Cable length doesn't exceed 100 meters.

3.1.5 New internet plan selection

First the current internet contract must be reviewed to better coordinate the contract termination or change. The prices for the internet plans vary slightly. All contracts have a fixed period of 24 months. The price difference between all of the providers is minimal as seen in Figure 7 below.



iki 1 Gb/s

Dideliam ir inovatyviam verslui, laisvė naršyti ir kolaboruoti internete

+ 6 papildomos nemokamos paslaugos

69,00 €/mėn.
24 mėn. sutartis

iki 1 Gbps

~~90,00~~
63,00 €/mėn.

Šviesolaidinis iki 1000 Mb/s

+2 nemokamos paslaugos

70,00 €/ mėn.
Su 24 mėn. sutartimi

98,00 €/ mėn.
Be sutarties

Verslui 1 Gb/s

- **Neribotas** šviesolaidinis internetas!
- iki 1 Gb/s interneto greitis **Lietuvoje ir užsienyje.**
- Reikliausiems interneto klientams, naudojantiems daug įrenginių.

Neterminuota sutartis: **95 Eur/mėn.**

24 mėn. sutartis:

60 €

per mėn.

Figure 7. Internet plans prices

Some providers offer additional benefits together with the internet plan. The most interesting one comes from Telia, it is called “SLA Plius”. It states that if internet connectivity was less than 99% during given month, then Telia would refund half of the internet service fee for that month and if the connectivity was less than 97%, the full price would be refunded. Considering this benefit, the extra cost of the Telia plan might be worth it. For this project two internet plans will be required. One internet provider will serve as the main connection and the other one as a backup connection in case of connectivity loss due to some technical fault, this way the company will be able to continue their day-to-day operations with no problems. After some deliberation internet plans from Telia and Cgates were chosen. Telia internet will serve as the main connection and Cgates as a backup.

3.1.6 Network design

The cables will be guided via metal trays either attached at the bottom of the walls or hanged on the ceiling. Cables from the ceiling trays to workplaces will be lowered down and placed inside cable protectors. The cameras will be installed in suggested locations indicated in Figure 6 that was provided earlier. The LAN cables for the cameras will also be guided via the trays. All network devices will be placed in the server room. For floor planning “AutoCAD” software was used and for network topology “Cisco Packet Tracer” software. Office plan with wiring tray locations, suggested workstation and other equipment placement is shown in Figure 8 below.

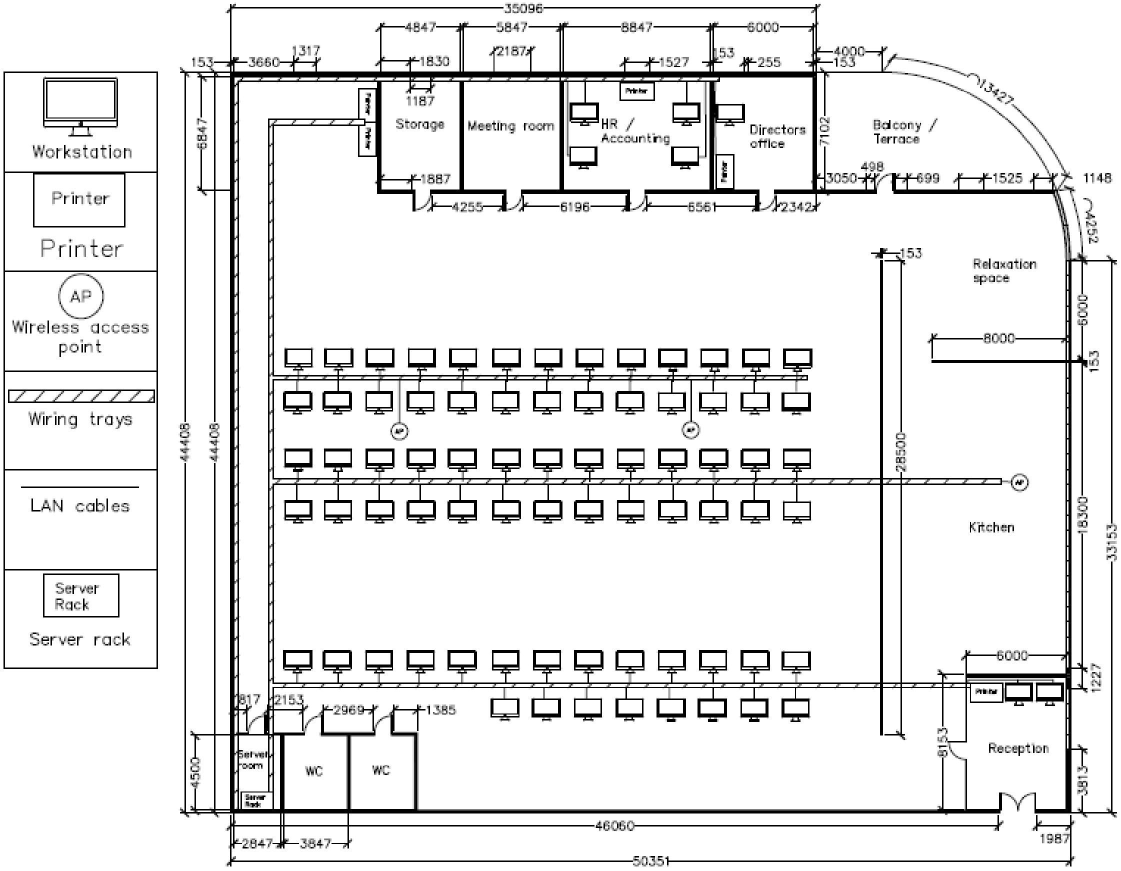


Figure 8. New office plan

After considering company’s situation, available equipment, and needs. It has been decided to proceed with hybrid network topology. The specifics of hybrid network topology was discussed in theoretical part. This hybrid topology will be a combination of mesh type topology and star type topology. Network switches will use mesh type topology to create redundant paths and all end devices will use the point-to-point connections to the switches. With the use of “Cisco packet tracer” application, it was possible to create a mock network topology of the planned network. The network topology is provided in Figure 9.

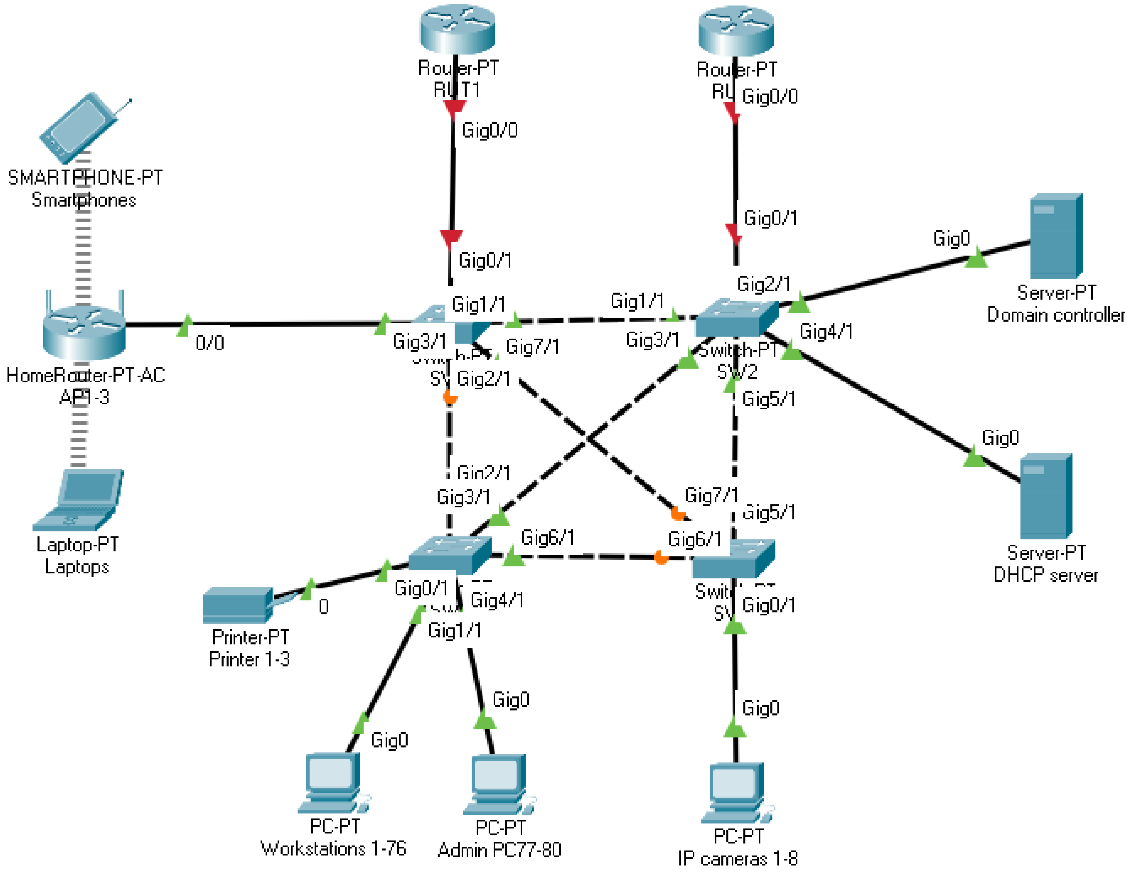


Figure 9. New network topology

In the new network topology two routers will be used instead of one. This was done so it would be possible to configure HSRP protocol that was discussed earlier. The internet cables will connected to both routers, one will be connected to the main ISP and the other one to the backup ISP. With network switches connected in a mesh type layout, it was possible to create several redundant paths in case one of the switches malfunctions. Point-to-point connection also simplifies the search for faulty link, as network administrators only need to know which switch the devices were connected to.

VLAN will be used to divide the local area network into smaller groups. There will be a seperate virtual local area networks for: workstations, surveillance system, network administrators and servers. What devices are assigned to what VLAN shown in Table 16 below.

Table 16. VLAN table

VLAN ID	Description
VLAN10	Workstations subnet
VLAN20	Surveillance system subnet
VLAN30	Network administrator’s subnet
VLAN40	Servers’ subnet

The IP addresses distribution for the new and old devices are listed in Table 17 below. All workstations will receive IP address from a DHCP server. Printers, wireless access points and other devices will have their IP address assigned manually.

Table 17. IP addressing table

Device	VLAN ID	IP address type	IP address	Default gateway	Subnet
PC1-76	10	DHCP	192.168.10.20-126	192.168.10.3	255.255.255.128
Admin PC1-4	30	Static	192.168.10.164-167	192.168.10.163	255.255.255.240
IP cameras 1-8	20	Static	192.168.10.133-140	192.168.10.131	255.255.255.224
NVR	20	Static	192.168.10.132	192.168.10.131	255.255.255.224
Printers1-3	10	Static	192.168.10.7-11	192.168.10.3	255.255.255.128
AP1-3	10	Static	192.168.10.4-6	192.168.10.3	255.255.255.128
DHCP server	40	Static	192.168.10.180	192.168.10.179	255.255.255.248
Domain controller	40	Static	192.168.10.181	192.168.10.179	255.255.255.248

With the mock network plan, IP addressing, and VLAN tables ready, it is possible to start configuring and testing the network.

3.2 Network configuration

This chapter will cover the configuration of the new network. Some protocols as a prerequisite must be configured first. For that reason, configuration will follow a specific order. Additionally, some of the protocols can be configured at the same time.

3.2.1 HSRP and VLAN configuration in routers

The hot standby router protocol and virtual local area network will be configured first. One of the reasons being that these technologies can be configured at the same time. The other reason is that HSRP provides a virtual IP address that will act as the default gateway for the network and which will be required for subsequent configuration. The VLAN ID's and designations were discussed earlier and can be found in a Table 16. Commands to configure HSRP and VLAN for RUT1:

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.128
standby 10 ip 192.168.10.3
standby 10 priority 110
standby 10 preempt
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.10.129 255.255.255.224
standby 20 ip 192.168.10.131
standby 20 priority 110
standby 20 preempt
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.10.161 255.255.255.240
standby 30 ip 192.168.10.163
standby 30 priority 110
standby 30 preempt
```

```
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.10.177 255.255.255.248
standby 40 ip 192.168.10.179
standby 40 priority 110
standby 40 preempt
```

RUT1 will have the active role and RUT2 will be the standby router. Commands to configure HSRP and VLAN for RUT2:

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.2 255.255.255.128
standby 10 ip 192.168.10.3
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.10.130 255.255.255.224
standby 20 ip 192.168.10.131
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.10.162 255.255.255.240
standby 30 ip 192.168.10.163
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.10.178 255.255.255.248
standby 40 ip 192.168.10.179
```

3.2.2 VLAN configuration in network switches

The network will be divided into 4 groups. All the necessary information about VLANs has been provided in Table 16 and Table 17 earlier. “Cisco Packet Tracer” does not have any objects that could be used for cameras. That is why for demonstration purposes computer objects will be used instead of cameras. Commands to create specified VLANS are the same for all 4 network switches:

```
vlan 10
name 10
vlan 20
name 20
vlan 30
name 30
vlan 40
name 40
```

Additionally, we need to run these commands for SW1:

```
int range g0/1, g7/1, g2/1, g1/1
switchport mode trunk
int g3/1
switchport access vlan 10
```

To configure SW2 we must run these commands:

```
int range g0/1, g1/1, g3/1, g5/1
switchport mode trunk
int range g2/1, g4/1
switchport access vlan 40
```

To configure SW3 we need to run these commands:

```
int range g2/1, g3/1, g6/1
switchport mode trunk
int range g0/1, g1/1
switchport access vlan 10
int g4/1
switchport access vlan 30
```

To configure SW4 we need to run these commands:

```
int range g6/1, g7/1, g5/1
switchport mode trunk
int g0/1
switchport access vlan 20
```

3.2.3 NAT configuration

As it was discussed earlier, the HSRP allows one active router to handle all incoming requests. The standby router waits for a signal to take over as the primary router. However, normally, the NAT table exists only on the active router, and in case of a device failure this table is not transferred to the standby router. To enable such transfers a stateful network address translation (SNAT) protocol is required. SNAT protocol supports asymmetric routing, which allows NAT tables to be shared across multiple routers. Stateful network translation uses UDP messages to pass network translation table updates between the primary and standby NAT router. Usually, SNAT protocol is embedded into HSRP protocol. The selection of the primary and backup network translation router is done automatically using the hot standby router protocol standby state or it can be done manually. Due to limitations of the “Cisco Packet Tracer” program itself, the stateful network translation protocol cannot be configured. However, NAT and

SNAT operation and configuration is very similar. That is why for demonstration purposes a network address translation protocol will be configured. In real life situations SNAT protocol would be preferred. Required commands to configure NAT for RUT1:

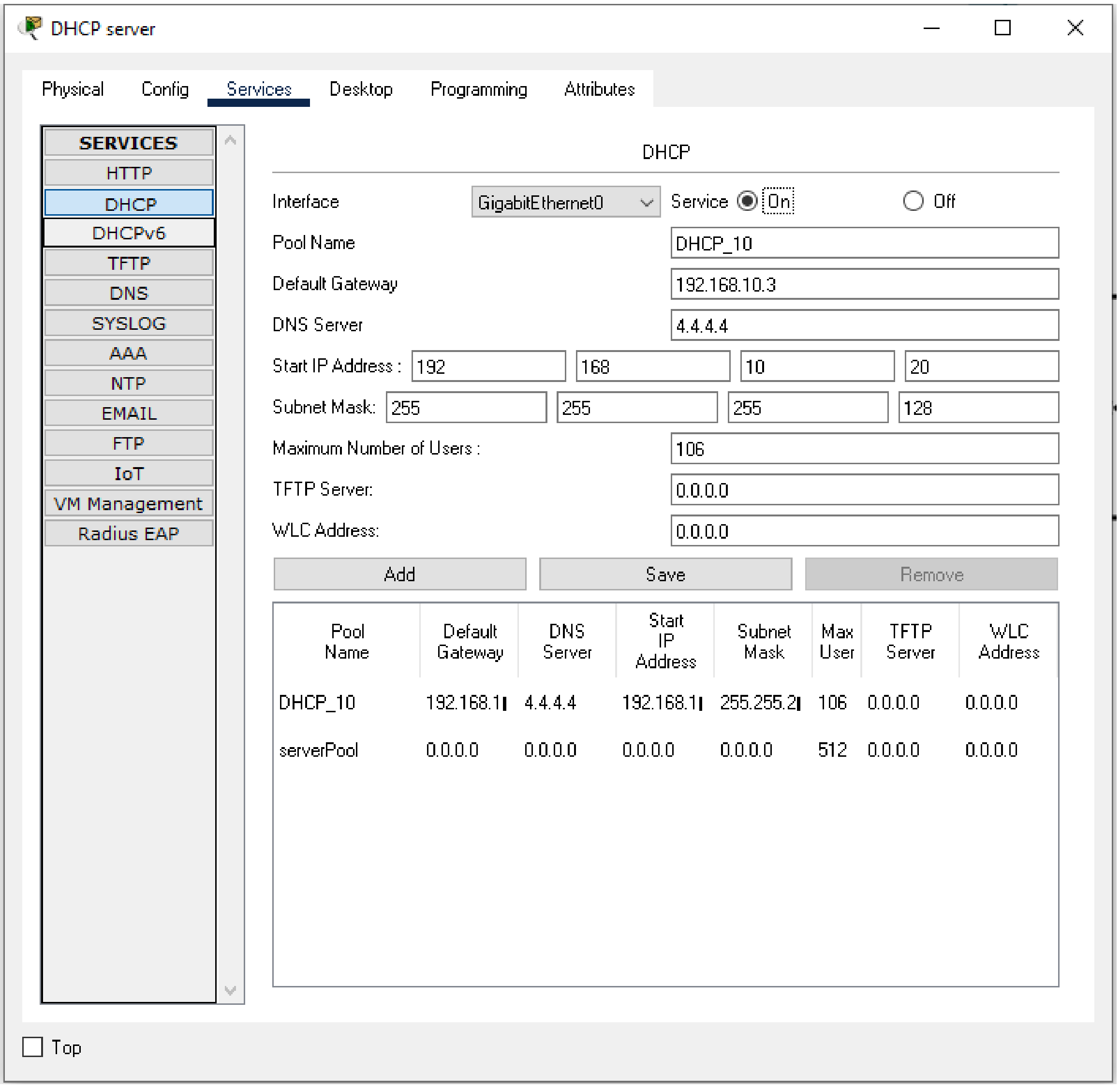
```
access-list 10 permit 192.168.10.0 0.0.0.127
access-list 20 permit 192.168.10.128 0.0.0.31
access-list 30 permit 192.168.10.160 0.0.0.15
access-list 40 permit 192.168.10.176 0.0.0.7
ip nat pool NAT_POOL 1.1.1.1 1.1.1.1 netmask 255.255.255.252
ip nat inside source list 10 pool NAT_POOL overload
ip nat inside source list 20 pool NAT_POOL overload
ip nat inside source list 30 pool NAT_POOL overload
ip nat inside source list 40 pool NAT_POOL overload
interface GigabitEthernet0/0.10
ip nat inside
interface GigabitEthernet0/0.20
ip nat inside
interface GigabitEthernet0/0.30
ip nat inside
interface GigabitEthernet0/0.40
ip nat inside
interface GigabitEthernet1/0
ip address 1.1.1.1 255.255.255.252
ip nat outside
```

To configure NAT for RUT2 we must run these commands:

```
access-list 10 permit 192.168.10.0 0.0.0.127
access-list 20 permit 192.168.10.128 0.0.0.31
access-list 30 permit 192.168.10.160 0.0.0.15
access-list 40 permit 192.168.10.176 0.0.0.7
ip nat pool NAT_POOL 1.1.1.5 1.1.1.5 netmask 255.255.255.252
ip nat inside source list 10 pool NAT_POOL overload
ip nat inside source list 20 pool NAT_POOL overload
ip nat inside source list 30 pool NAT_POOL overload
ip nat inside source list 40 pool NAT_POOL overload
interface GigabitEthernet0/0.10
ip nat inside
interface GigabitEthernet0/0.20
ip nat inside
interface GigabitEthernet0/0.30
ip nat inside
interface GigabitEthernet0/0.40
ip nat inside
interface GigabitEthernet1/0
ip address 1.1.1.5 255.255.255.252
ip nat outside
```

3.2.4 DHCP server configuration

DHCP can be configured inside the routers or as a service in a server. In this situation the company has a dedicated server for dynamic host configuration protocol. During the DHCP server configuration. Few things must be provided: DHCP pools name, the default gateway, DNS server address and the IP addresses array to be used in the pool. DHCP server configuration interface is shown in Figure 10 below.



DHCP

Interface GigabitEthernet0 Service ● On ○ Off

Pool Name: DHCP_10

Default Gateway: 192.168.10.3

DNS Server: 4.4.4.4

Start IP Address : 192 168 10 20

Subnet Mask: 255 255 255 128

Maximum Number of Users : 106

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
DHCP_10	192.168.1	4.4.4.4	192.168.1	255.255.2	106	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

Figure 10. DHCP server configuration

To make sure that DHCP works properly we must configure helper adresses inside the routers, this command is the same for both routers:

```
ip helper-address 192.168.10.180
```

3.2.5 ACL configuration

According to the planned ACL rules devices that belong to VLAN10 will only be able to reach other devices that are in the same VLAN. ACL rules should not prevent VLAN10 devices from sending and receiving packets related to DHCP. Devices that belong to VLAN20 are part of video surveillance system, they should not be able to reach or be reached by other devices. VLAN30 devices should be able to reach all devices. All TCP traffic from outside should be blocked, unless the session was started from inside the network. Same applies to ICMP packets. Both routers will share the same configuration. ACL's will be placed facing the outside of the router. ACL configuration commands for RUT1:

```
access-list 10 permit 192.168.10.0 0.0.0.127
access-list 20 permit 192.168.10.128 0.0.0.31
access-list 30 permit 192.168.10.160 0.0.0.15
access-list 40 permit 192.168.10.176 0.0.0.7
access-list 171 permit ip 192.168.10.0 0.0.0.127
192.168.10.0 0.0.0.127
access-list 171 permit ip 192.168.10.160 0.0.0.15
192.168.10.0 0.0.0.127
access-list 171 permit ip 192.168.10.0 0.0.0.127 1.1.1.0
0.0.0.3
access-list 171 permit icmp any 192.168.10.0 0.0.0.127 echo-
reply
access-list 171 permit tcp any any gt 1023 established
access-list 171 permit udp any eq bootpc any eq bootps
access-list 172 permit ip 192.168.10.160 0.0.0.15 any
access-list 173 permit ip 192.168.10.160 0.0.0.15 any
access-list 173 permit icmp any any echo-reply
access-list 173 permit tcp any any gt 1023 established
access-list 174 permit ip 192.168.10.160 0.0.0.15 any
access-list 174 permit ip 192.168.10.176 0.0.0.7 any
access-list 174 permit udp any eq bootpc any eq bootps
access-list 180 permit icmp any any echo-reply
access-list 180 permit tcp any any gt 1023 established
interface GigabitEthernet0/0.10
ip access-group 171 out
interface GigabitEthernet0/0.20
ip access-group 172 out
interface GigabitEthernet0/0.30
```

```
ip access-group 173 out
interface GigabitEthernet0/0.40
ip access-group 174 out
interface GigabitEthernet1/0
ip access-group 180 in
```

To configure ACLs for RUT2 we can run the same commands as we did for RUT1.

3.3 Network configuration testing

After configuring the network, it is necessary to test out the configuration to make sure that everything works as intended and that the network performs as expected. For testing purposes additional routers for internet service providers were added to the packet tracer application to simulate “outside” network.

3.3.1 HSRP testing

To test host standby router protocol, a failure must occur. In the case of a failure the stand-by router should take over the role of the active router. To simulate a failure an ethernet cable between the active router and switch was disconnected as shown in Figure 11 below.

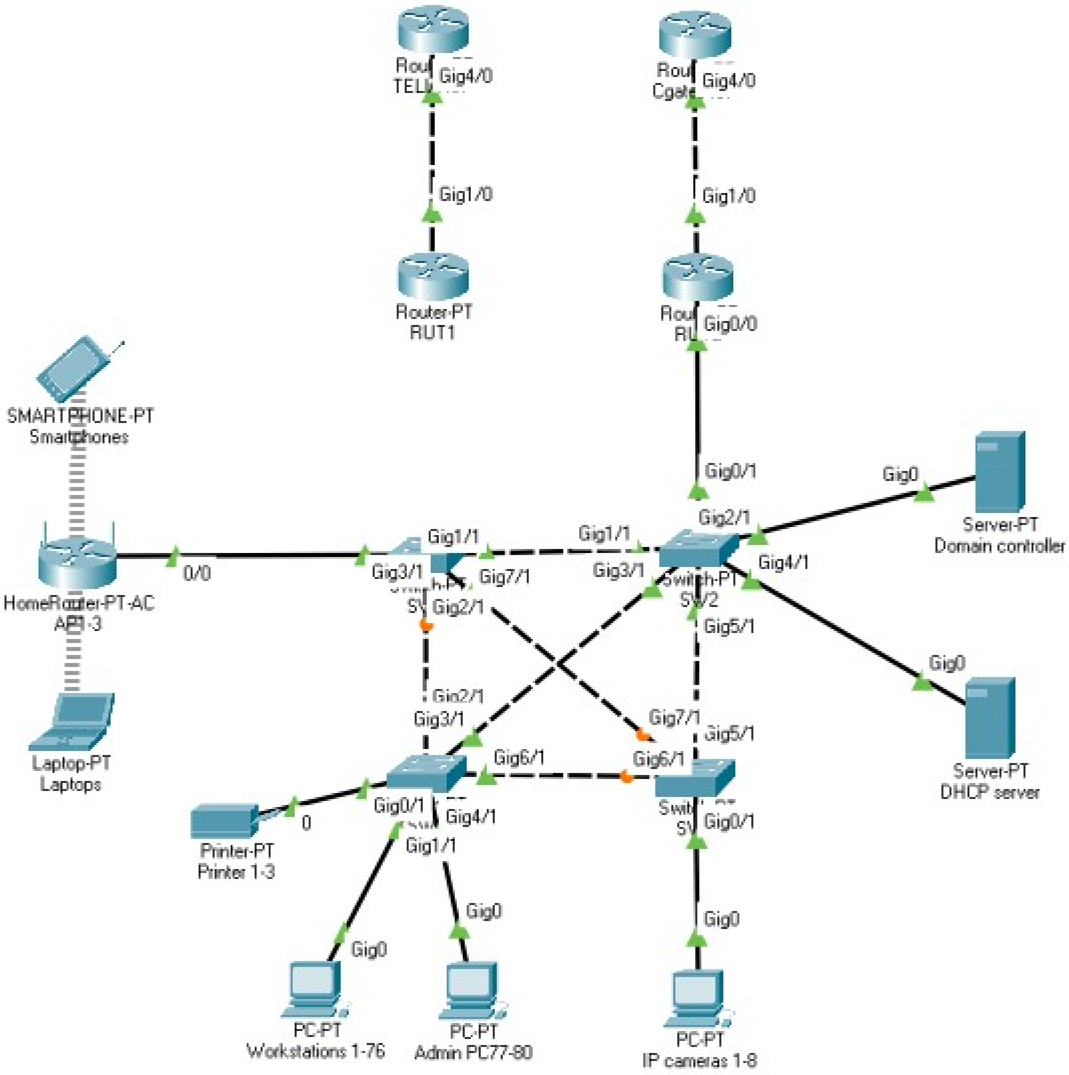
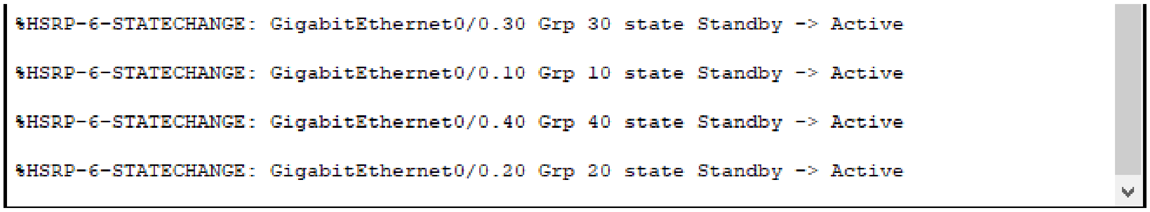


Figure 11. Testing HSRP protocol 1

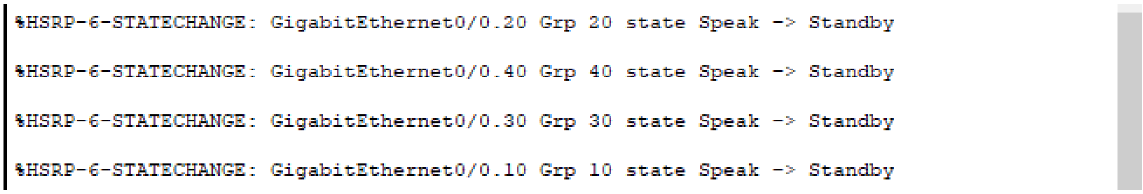
After the cable was disconnected, few moments later RUT2 took over the role of active router as it can be seen from CLI output in Figure 12 below.



```
%HSRP-6-STATECHANGE: GigabitEthernet0/0.30 Grp 30 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0.40 Grp 40 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0.20 Grp 20 state Standby -> Active
```

Figure 12. Testing HSRP protocol 2

After the RUT1 was reconnected, RUT2 returned to standby mode as seen from Figure 13 below.



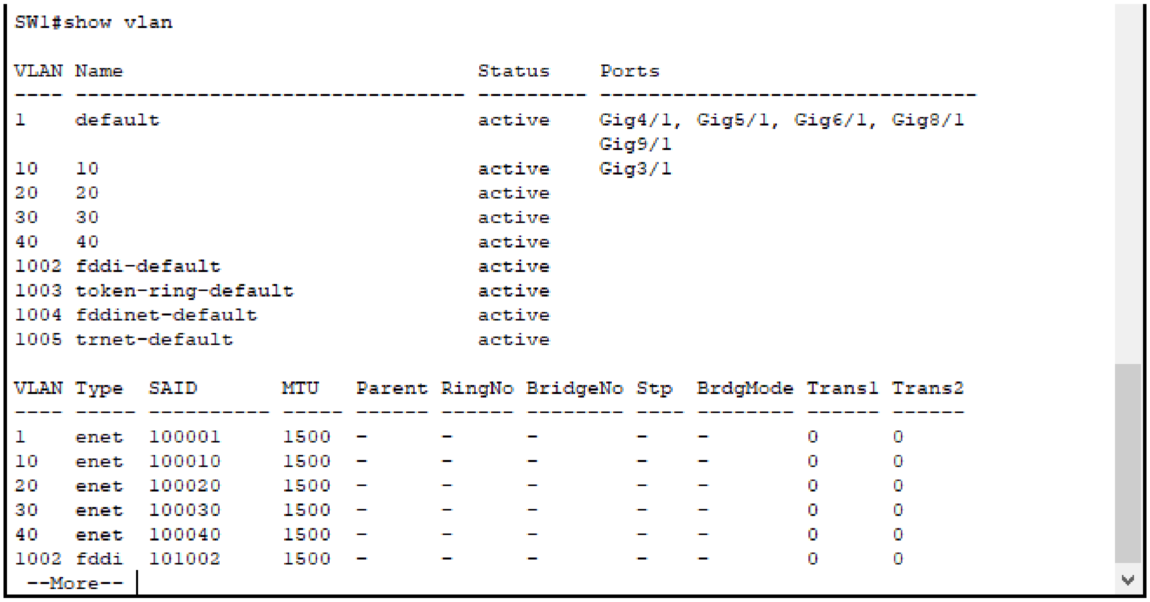
```
%HSRP-6-STATECHANGE: GigabitEthernet0/0.20 Grp 20 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0.40 Grp 40 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0.30 Grp 30 state Speak -> Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Speak -> Standby
```

Figure 13. Testing HSRP protocol 3

Therefore it can be concluded that the HSRP protocol is working properly.

3.3.2 VLAN testing

To test if the virtual local area network configuration was successful, we must check if all specified VLANS were created and if all network switch ports have been configured with correct VLANs. From Figure 14 provided below we can see that VLAN10, VLAN 20, VLAN30 and VLAN40 were successfully created on switch SW1. Additionally, the required ports have been assigned to the correct VLANs.



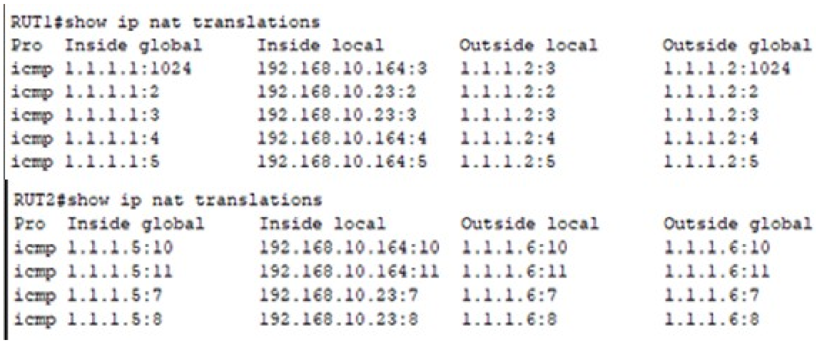
```
SW1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig4/1, Gig5/1, Gig6/1, Gig8/1
                                                Gig9/1
10   10                               active    Gig3/1
20   20                               active
30   30                               active
40   40                               active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

Figure 14. VLAN port assignment SW1

In all 4 network switches all VLANs were successfully created and all ports have assigned to the correct VLANs. Thus, it is safe to conclude that virtual local area network was configured correctly.

3.3.3 NAT protocol testing

To test if network address translation protocol was configured correctly, we must view NAT table. The translation table provides information about all internal IP addresses that were translated to public address as shown in the Figure 15 below.



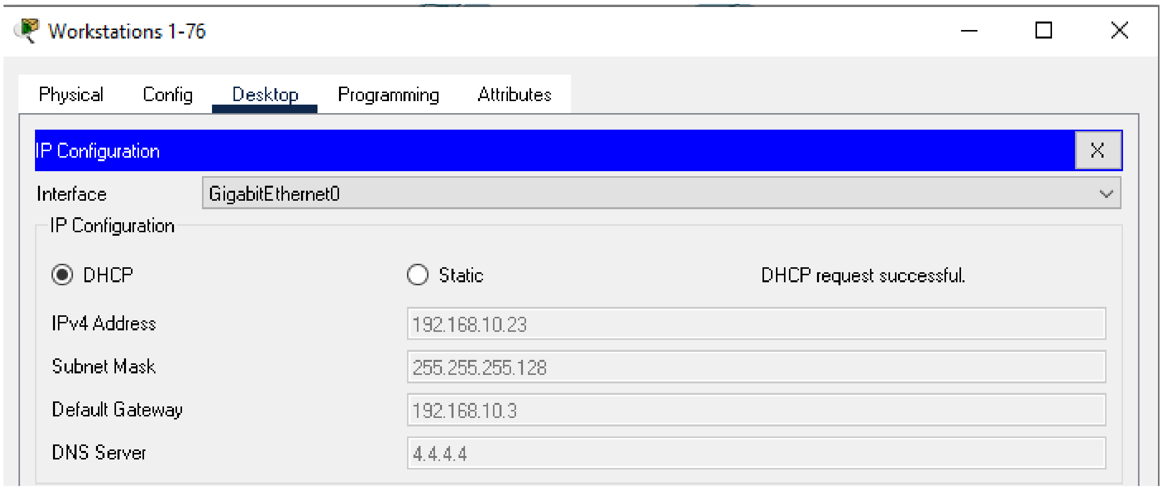
```
RUT1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.1.1.1:1024      192.168.10.164:3   1.1.1.2:3          1.1.1.2:1024
icmp 1.1.1.1:2         192.168.10.23:2    1.1.1.2:2          1.1.1.2:2
icmp 1.1.1.1:3         192.168.10.23:3    1.1.1.2:3          1.1.1.2:3
icmp 1.1.1.1:4         192.168.10.164:4   1.1.1.2:4          1.1.1.2:4
icmp 1.1.1.1:5         192.168.10.164:5   1.1.1.2:5          1.1.1.2:5
RUT2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.1.1.5:10        192.168.10.164:10  1.1.1.6:10         1.1.1.6:10
icmp 1.1.1.5:11        192.168.10.164:11  1.1.1.6:11         1.1.1.6:11
icmp 1.1.1.5:7         192.168.10.23:7    1.1.1.6:7          1.1.1.6:7
icmp 1.1.1.5:8         192.168.10.23:8    1.1.1.6:8          1.1.1.6:8
```

Figure 15. NAT protocol testing

We can see that the NAT protocol successfully changes internal addresses to external addresses and vice versa. Therefore, it can be concluded that the NAT protocol is working properly.

3.3.4 DHCP testing

To test if the DHCP server is configured properly and that the devices are receiving IP addresses from this server we must change the end device network connectivity settings to use DHCP instead of Static addressing. From the Figure 16 below we can see that the “Workstations1-76” are able to receive its IP addresses from the DHCP server.



Interface GigabitEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.10.23

Subnet Mask 255.255.255.128

Default Gateway 192.168.10.3

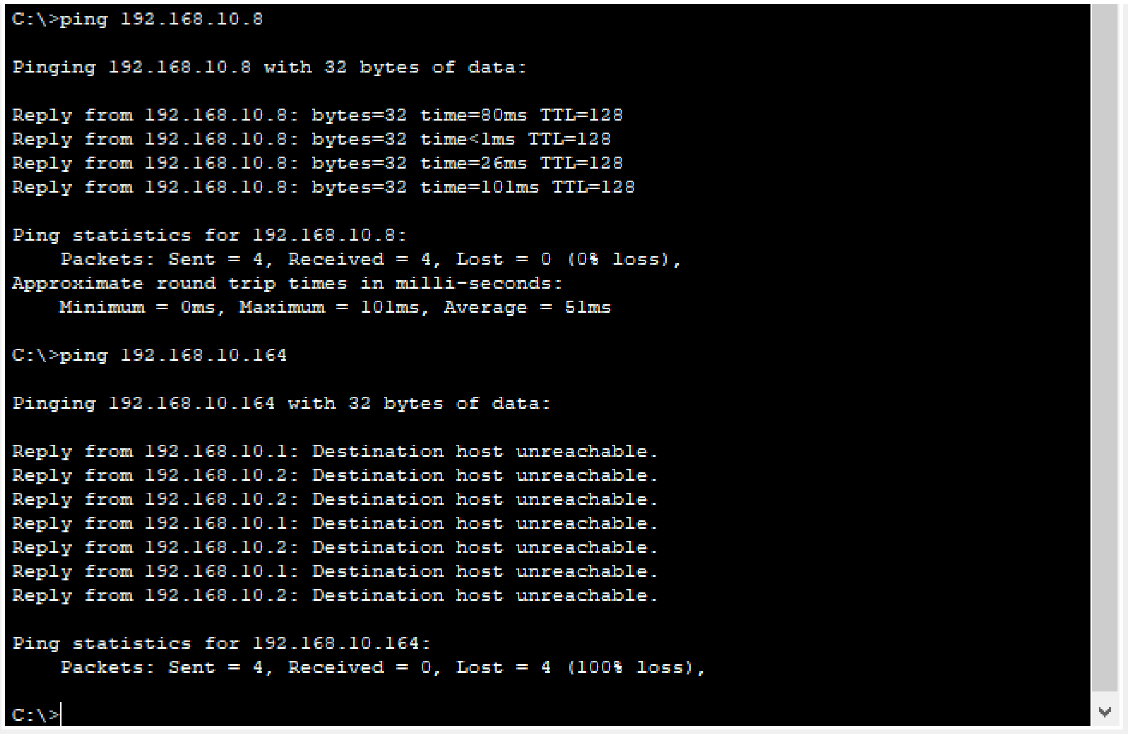
DNS Server 4.4.4.4

Figure 16. DHCP testing

The assigned IP address is part of the defined IP address array “DHCP_10”. Therefore, it can be concluded that the DHCP server configuration is working properly.

3.3.5 ACL testing

Testing access control list configuration involves multiple steps. One for each defined rule. The testing will proceed from first defined ACL down to the last one. Devices belonging to VLAN10 should only be able to reach other devices that belong to VLAN10, this was tested by trying to ping devices that belong to VLAN10 and VLAN30. The results are shown in Figure 17 below. Additionally, VLAN10 devices should also be able to send DHCP requests and receive responses to these requests which was already tested during the “DHCP testing” step.

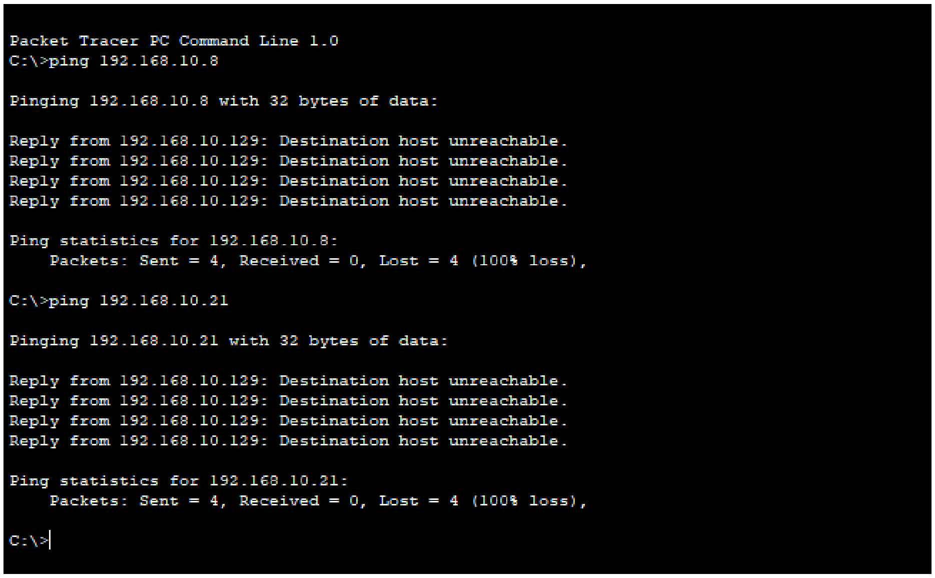


```
C:\>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.8: bytes=32 time=80ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time=26ms TTL=128
Reply from 192.168.10.8: bytes=32 time=101ms TTL=128

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 101ms, Average = 51ms

C:\>ping 192.168.10.164

Pinging 192.168.10.164 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.2: Destination host unreachable.
Reply from 192.168.10.2: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.2: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.2: Destination host unreachable.

Ping statistics for 192.168.10.164:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 17. ACL testing 1

We can see that the device that belongs to the VLAN10 is able to ping other devices that belong to the same VLAN and that it is unable to reach devices that belong to VLAN30.

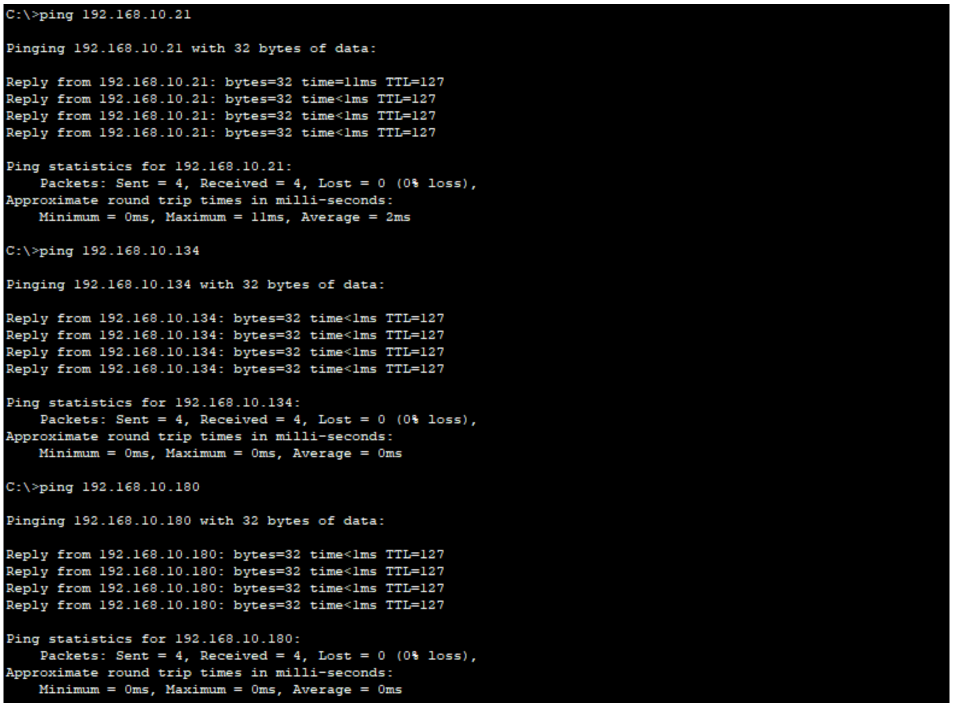
The devices that belong to VLAN20 should not be able to reach other devices or be reachable by others. A test for this ACL rule is shown in Figure 18 below.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.21

Pinging 192.168.10.21 with 32 bytes of data:

Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.
Reply from 192.168.10.129: Destination host unreachable.

Ping statistics for 192.168.10.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 18. ACL testing 2

The end result is that VLAN20 was unable to reach any of devices from VLAN10. The network administrators, i.e., VLAN30 devices should be able to access all network devices without restriction. The ping tests for that are shown in Figure 19 below.

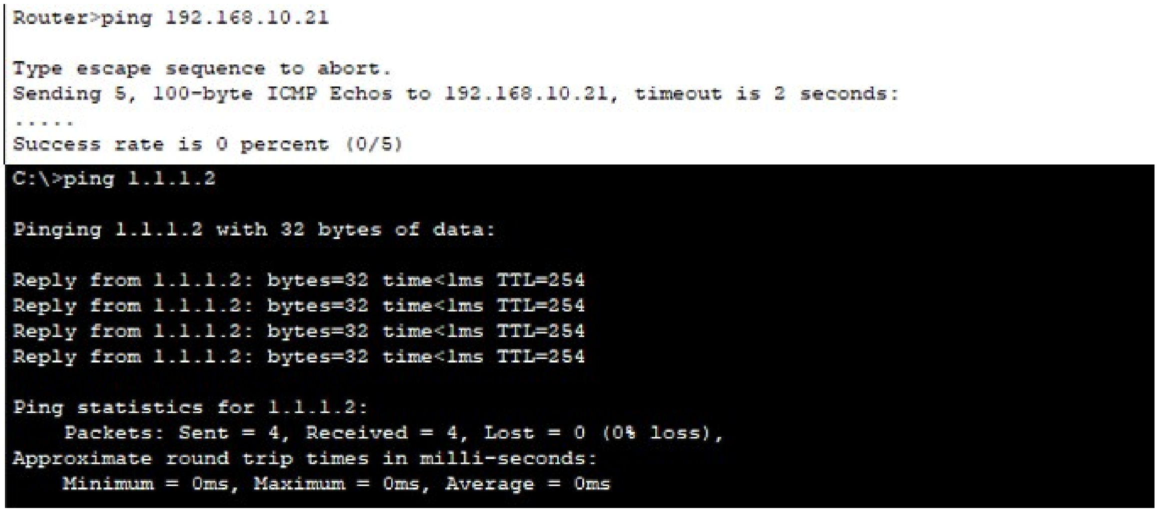


```
C:\>ping 192.168.10.21

Pinging 192.168.10.21 with 32 bytes of data:

Reply from 192.168.10.21: bytes=32 time=11ms TTL=127
Reply from 192.168.10.21: bytes=32 time<1ms TTL=127
Reply from 192.168.10.21: bytes=32 time<1ms TTL=127
Reply from 192.168.10.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>ping 192.168.10.134

Pinging 192.168.10.134 with 32 bytes of data:

Reply from 192.168.10.134: bytes=32 time<1ms TTL=127
Reply from 192.168.10.134: bytes=32 time<1ms TTL=127
Reply from 192.168.10.134: bytes=32 time<1ms TTL=127
Reply from 192.168.10.134: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.180

Pinging 192.168.10.180 with 32 bytes of data:

Reply from 192.168.10.180: bytes=32 time<1ms TTL=127
Reply from 192.168.10.180: bytes=32 time<1ms TTL=127
Reply from 192.168.10.180: bytes=32 time<1ms TTL=127
Reply from 192.168.10.180: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 19. ACL testing 3

We can see that VLAN30 can succesfully reach devices from VLAN10, VLAN20 and VLAN40.

No outside connections should be able to reach the internal network unless the session has been started internally. This ACL rule was tested by trying to ping a device that belongs to VLAN10 from router labeled “TELIA ISP” and by trying to ping the same router from the device. The results of the test are shown in Figure 20 below.



```
Router>ping 192.168.10.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
C:\>ping 1.1.1.2

Pinging 1.1.1.2 with 32 bytes of data:

Reply from 1.1.1.2: bytes=32 time<1ms TTL=254
Reply from 1.1.1.2: bytes=32 time<1ms TTL=254
Reply from 1.1.1.2: bytes=32 time<1ms TTL=254
Reply from 1.1.1.2: bytes=32 time<1ms TTL=254

Ping statistics for 1.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 20. ACL testing 4

We can see that the outside network router was unable to ping the local network device, while the same device was able to ping the router and receive the response.

All performed ACL tests were successful, so it is safe to assume that ACL rules are working as intended.

4 CONCLUSIONS

After company’s current computer network and its technologies were examined, it was concluded that some of the network equipment is still usable and there is no need to replace it right away. Office computers are also still fit for use after a minimal modernization. Computers that won’t be reused will be stored and scraped for spare parts. Servers operating systems had been updated to a newer OS.

The business requested that a video surveillance system would be designed and implemented inside the office. The cameras were placed in locations with most foot traffic.

To accommodate new network devices and workstations, a new computer network has been designed. The new network required an additional network switch and it was necessary to replace the old router.

For the planned number of employees, a total of 80 new workstations were required. This number was fulfilled by buying 65 new computers that were chosen during the implementation phase and by reusing few old office computers.

Finally, a mock simulation of the new computer network has been configured and tested. After testing the implemented network, it was found that it is working properly.

The final result is a working computer network designed according to the company needs. It is more efficient and provides more reliability compared to the old network and equipment, however the network was tested and implemented in simulated environment which proved lacking in some aspects. Additionally, there are few things that could be expanded upon, for example: the network topology itself could be expanded upon to provide even more reliability. Same goes for network security, as this project only covered the usage of VLANs and ACLs. To increase the security, it is necessary to use firewalls and possibly a VPN.

5 REFERENCES

Bosch. n.d. Video systems. Web page. Available at: https://www.boschsecurity.com/us/en/solutions/video-systems/ [Accessed 04 January 2023].

Cisco Meraki. 2021. Spanning tree protocol (STP) overview. Web page. Available at: https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview [Accessed 26 December 2022].

Cisco. 2022. Understand the hot standby router protocol features and functionality. Web page. Available at: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html [Accessed 26 December 2022].

Cisco. n.d. Cisco small business 110 series unmanaged switches. Web page. Available at: https://www.cisco.com/c/en/us/support/switches/110-series-unmanaged-switches/series.html [Accessed 26 December 2022].

DNSstuff. 2019. What is network topology? Best guide to types and diagrams. Web page. Available at: https://www.dnsstuff.com/what-is-network-topology [Accessed 19 January 2023].

ItGlobal. n.d. Access Control List. Web page. Available at: https://itglobal.com/company/glossary/access-control-list/ [Accessed 23 January 2023].

Kunert, P. 2022. Windows 11 runs on fewer than 1 in 6 PCs. Web page. Available at: https://www.theregister.com/2022/11/02/windows_11_statcounter/ [Accessed 30 December 2022].

Microsoft Learn. 2021. Dynamic Host Configuration Protocol. Web page. Available at: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top [Accessed 19 January 2023].

Microsoft Support. n.d. Windows 10 system requirements. Web page. Available at: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715 [Accessed 30 December 2022].

Microsoft Windows. n.d. Find Windows 11 specs, features, and computer requirements. Web page. Available at: https://www.microsoft.com/en-us/windows/windows-11-specifications [Accessed 30 December 2022].

Morrison, S. 2022. What is the best internet speed for your business. Web page. Available at: https://www.business.com/internet/bandwidth/ [Accessed 26 December 2022].

Noureen, R. 2023 Jan 19. Microsoft to end sale of Windows 1- Home and pro licenses this month. Web page. Available at: https://petri.com/microsoft-block-sale-windows-10-licenses/ [Accessed 23 January 2023].

PCMag. n.d. Windows 10 versions. Web page. Available at: https://www.pcmag.com/encyclopedia/term/windows-10-versions [Accessed 30 December 2022].

Router-switch. 2018. PCIe vs SATA: Which SSD interface should you go for. Web page. Available at: https://www.router-switch.com/faq/pcie-vs-sata-ssd-interface-difference.html [Accessed 26 December 2022].

Slattery, T & Burke, J. 2022. VLAN (virtual LAN). Web page. Available at: https://www.techtarget.com/searchnetworking/definition/virtual-LAN [Accessed 23 January 2023].

Spot AI. n.d. Video intelligence. Web page. Available at: https://www.spot.ai/video-intelligence [Accessed 04 January 2023].

Turing. n.d. Turing vision. Web page. Available at: https://turing.ai/products/turing-vision [Accessed 04 January 2023].

Weinberg, N. 2022. DHCP defined and how it works. Web page. Available at: https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html [Accessed 19 January 2023].

LIST OF FIGURES

LIST OF TABLES