KAUNO KOLEGIJA

TECHNOLOGIJŲ FAKULTETAS

INFORMATIKOS IR MEDIJŲ TECHNOLOGIJŲ KATEDRA

Algimantas Januška

KOMPIUTERINIO TINKLO MODERNIZAVIMO PROJEKTAS

Baigiamasis darbas

Kibernetinių sistemų ir saugos studijų programos
valstybinis kodas 6531BX024
Informatikos inžinerijos studijų krypties

Vadovas Matti Juutilainen

Konsultantai dr. Jovita Danielytė
Gintarė Jurkševičiūtė

Kaunas, 2024

SANTRAUKA

Autorius Algimantas Januška. ***Kompiuterinio tinklo modernizavimo projektas.*** **Baigiamasis darbas. Vadovas Matti Juutilainen. Kauno kolegija, Technologijų fakultetas, Informatikos ir medijų technologijų katedra, Kaunas, 2024, 73 psl.**

Reikšminiai žodžiai: kompiuterio tinklas, Cisco Packet Tracer ir Ekahau, bevielis ryšys.

Baigiamajame darbe siekiama išsamiai modernizuoti organizacijos tinklo infrastruktūrą, integruojant teorinius tyrimus ir praktinį pritaikymą. Pradžioje pateikiamas detali teorinė pagrindų apžvalga, kuri paaiškina būtinas šiuolaikinio tinklo sudedamąsias dalis, pradedant nuo pagrindinių elementų ir baigiant visa infrastruktūra. Panaudojant šią teorinę informaciją, atliekama esamos tinklo infrastruktūros analizė, identifikuojant pagrindines problemas, tokias kaip tinklo perkrova ir ribotas bevielis ryšys. Po to, remiantis teorine baze, pateikiamos problemų sprendimo būdai, siekiant pagerinti tinklo našumą ir saugumą. Naudojamos priemonės, tokios kaip Cisco Packet Tracer ir Ekahau, padeda modeliuoti naują tinkle išdėstymą ir vizualizuoti bevielio ryšio patobulinimus. Pateikiama išsami naujo tinklo konfigūracija, sąnaudų analizė ir apibendrinama visa modernizavimo proceso eiga. Baigiamajame darbe pabrėžiama, kaip šis projektas padės pagerinti tinklo efektyvumą ir pasiruošti ateities technologiniams iššūkiams.

Projektą sudaro šios dalys: įvadas, teorinė dalis, esamo tinklo analizė, naujo tinkle projektavimo dalis, darbo rezultatai ir išvados, naudotos literatūros sąrašas (26 šaltiniai). Darbo apimtis 73 psl. Teorinės dalies 21 lapas, esamos situacijos analizė 16 lapų, naujos infrastrukturos analizė, ir implementacija 15 lapų, rezultatai ir išvados 4 lapai . Visame darbe yra 7 figuros ir 29 lentelės.

Algimantas Januška

Computer Network Modernization

Bachelor’s thesis

Bachelor of Engineering

Information Technology

2024

South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor or Engineering
Author(s)	Algimantas Januška
Thesis title	Computer network modernization
Commissioned by	Matti Juutilainen
Year	2024
Pages	71 pages
Supervisor(s)	Matti Juutilainen

Abstract

This thesis presents a comprehensive modernization of a network infrastructure, merging extensive theoretical exploration with practical application. It begins by establishing a detailed theoretical framework that elucidates the essential components required for a modern network, ranging from basic elements to complete infrastructure systems.

Utilizing theoretical framework, the current network infrastructure is assessed, identifying prevailing issues and discussing potential improvements. Subsequently, the theoretical insights are applied to guide the modernization of the network, aiming to address identified problems effectively.

The thesis then provides a meticulous presentation of the updated network, covering aspects from configurations and implementation to the financial implications of the upgrades.

Finally, it concludes with a summary of the interventions undertaken and their impacts, offering a critical evaluation of the modernization process. This work emphasizes the importance of a well-grounded theoretical approach in driving practical network enhancements that are both effective and economically viable.

Abbreviations:

QoS (Quality of Service) - QoS refers to the set of techniques to manage network resources by setting priorities for specific types of data on the network, ensuring optimal performance of critical applications and services.

Wi-Fi - A wireless networking technology that allows devices to connect to the internet and communicate with each other without physical cables.

OSPF (Open Shortest Path First) - OSPF is an adaptive routing protocol for Internet Protocol (IP) networks which uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

Dijkstra's Algorithm - A graph search algorithm that solves the shortest path problem for a given source node in a graph with non-negative path costs, providing the shortest path from one node to another.

ACL (Access Control List) - A list of permissions attached to an object in a computer system, specifying which users or system processes can access that object and what operations they can perform.

Firewall - Security system that monitor and control incoming and outgoing network traffic based on predetermined security rules to protect networks from unauthorized access.

MFA (Multi-Factor Authentication): MFA enhances security by requiring two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

VPN (Virtual Private Network) - A service that encrypts a user’s internet connection and routes it through an intermediary server in another location, masking the user's IP address and providing privacy and security.

IPSec (Internet Protocol Security) - IPSec is a suite of protocols for securing internet protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

SSH (Secure Shell) - SSH is a protocol that provides a secure, encrypted connection between two devices to enable confidential communication over an insecure network.

TLS (Transport Layer Security) - TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the internet.

S/MIME (Secure/Multipurpose Internet Mail Extensions) - A standard for public key encryption and signing of MIME data, used to secure email by authenticating sender and encrypting email content.

PGP (Pretty Good Privacy) - A data encryption and decryption program that provides cryptographic privacy and authentication for data communication, commonly used for securing emails.

WPA2 (Wi-Fi Protected Access 2) - A security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.

WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) - A method of securing Wi-Fi networks where all users share a single password or passphrase for network access.

SNMP (Simple Network Management Protocol) - A protocol used for network management and monitoring of network devices for conditions that warrant administrative attention.

Syslog - A standard for message logging, allowing software to generate and store logs with a uniform format across different systems for review and analysis.

SMTP (Simple Mail Transfer Protocol) - The main protocol used to send electronic mail from server to server on the Internet

POP3 (Post Office Protocol version 3) - An older, yet still used, email retrieval protocol that allows users to download messages from their email server to their local computer and read them offline.

IMAP (Internet Message Access Protocol) - An email retrieval protocol designed to enable users to access their email from multiple devices without having to download the messages to each individual device.

AES-256 (Advanced Encryption Standard 256-bit) - AES-256 is an encryption standard used by the U.S. government and other entities to encrypt sensitive information, utilizing a 256-bit key for a high level of security.

RPO (Recovery Point Objective) - This metric determines the maximum tolerable period in which data might be lost due to a major incident before it affects business continuity.

RTO (Recovery Time Objective) - This metric defines the target time you have to restore your business functions after a disaster has struck, minimizing the impact on operations.

BIA (Business Impact Analysis) - This process systematically identifies and evaluates the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.

1 Introduction

1.1 Background and motivation

The relentless pace of technological innovation demands an equally dynamic approach to the modernization of computer networks. In an era where digital connectivity is the lifeline of organizations, the need to keep the networks up to date has become a pressing priority. This thesis explores the journey of network modernization through the case study of an undisclosed company, aiming to shed light on the critical aspects of scalability, security, and productivity that define the success of this project. It is a journey into the heart of network infrastructure, seeking solutions that can meet the ever-evolving demands of the digital age.

1.2 Objectives:

Understand components of network infrastructure

Conducting a detailed analysis of the essential components of the network, examining their functionality and interrelations. This stage involves mapping out crucial details that will form the theoretical framework, including key points and references that are foundational for understanding the network's structure and operations.

Understand current network

Utilizing theoretical insights to assess the current network infrastructure, identifying performance capabilities, operational difficulties, and security structures. Focusing on key areas within the network architecture, the evaluation aims to pinpoint factors that may be slowing down the network or causing other functional issues.

Develop a modernized network infrastructure

Following a comprehensive analysis of the existing network infrastructure and the identification of critical issues, the next step involves the meticulous planning and implementation of solutions designed to resolve these problems and enhance the network's efficiency and modernization. Each solution will be implemented with detailed documentation of the updated network configurations, providing a clear reference for future upgrades. The project will conclude with a summary of the total costs incurred, alongside a thorough review of all elements affected by the modernization efforts.

1.3 Thesis Structure

Introduction – This section begins by outlining the fundamental reasons this topic is significant and articulates the objectives we aim to accomplish through this project.

Theoretical Framework – At the start, we define the essential components and strategies required for modern network and outline the primary approach to achieving the desired infrastructure.

Current State Analysis – In this part, we examine the existing network configuration, discussing its current layout, usage, and components to understand the baseline from which improvements will be made.

Solution and Implementation Design – Armed with knowledge of the current issues, we will devise a blueprint for a new and enhanced network. This phase involves creatively applying the theoretical framework to construct a sophisticated network infrastructure.

Evaluations and Discussions – This section involves a critical assessment of the proposed solutions relative to the existing system, exploring the potential impacts, advantages, and challenges associated with the implementation.

Conclusion – The conclusion summarizes the activities undertaken, the discoveries made, and the significance of these findings. It also considers future prospects for further improvements or alternative approaches that could be explored.

References – This acknowledges the sources of information and insights utilized throughout the project, giving credit where it is due.

2 Theoretical Framework

When designing a new network, it's important to start by defining what the network is for, like sharing files or facilitating communication, and how big it needs to be. This ensures the network will work well for its users and can handle the expected workload. Protecting sensitive information is a big deal, so setting up the right security from the start is a must. The network's layout and the equipment used should fit the network's size and need to be reliable and ready to grow. Planning for how much data will move through the network and making sure it can grow with the organization is critical. Strong security steps, like using firewalls and making data unreadable to outsiders, help keep everything safe. It's also smart to have a plan for when things go wrong to keep downtime short. Following laws, keeping costs in check, choosing the right companies to work with, and keeping up with new technologies are all part of making a network that's strong now and can adapt to what comes next.

2.1 Purpose and Objectives

The primary goal of the network is to act as a central hub for efficient data sharing and communication within the company, enhancing teamwork and swift decision-making by providing immediate access to vital infrastructure. Integrating protocols and other collaboration platforms, the network is designed to improve communication, supporting productivity and seamless workflows across different teams. By centralizing resources, the aim is to streamline operations, ease IT management, and improve security, ensuring an efficient and secure working environment.

2.2 User Needs and Applications

To meet company’s diverse requirements, the network design needs to include VLAN segmentation for efficient traffic management, QoS rules to prioritize critical applications, and a high-bandwidth infrastructure to support intensive tasks. Additionally, the design needs to be scalable to accommodate growth and offer both wireless and wired connectivity options, ensuring a versatile network environment for all users.

2.3 Network Topology and Infrastructure

Network topology refers to the arrangement and interconnection of various network components, including routers, switches, and devices, defining how they communicate. The infrastructure encompasses the physical and virtual resources, such as cabling, wireless access points, and network protocols, that support the flow of data across the topology. Choosing the right topology and infrastructure design is crucial for ensuring network performance, reliability, and scalability to meet any needs.

2.3.1 Network components and their roles

Routers: Serve as the backbone of any network by directing data traffic between different networks. They determine the best route for data packets to travel from their source to their destination across interconnected networks.

Switches: Act as the central hub within a single network, connecting various devices like computers, printers, and servers. They receive incoming data packets and redirect them to their intended device within the same network.

Access Points (APs): Allow devices to connect to the network wirelessly, extending the network's reach without the need for physical cables. They bridge the gap between wired networks and wireless devices.

Modems: Facilitate the connection between a computer (or local network) and the internet by converting digital data from a computer into a format suitable for transmission over analog communication lines like telephone or cable networks.

Ethernet Cables: The most common wired option for connecting devices within a network, suitable for local area networks (LANs).

Fiber Optic Cables: Used for high-speed data transmission over longer distances, ideal for wide area networks (WANs) or backbone connections within large networks.

Wireless (Wi-Fi): Enables devices to connect to the network without physical cables, using radio waves to transmit data.

Servers: Powerful computers that store, send, and process data for other computers (clients) on the network. They host applications, databases, websites, and other services.

Clients: Devices that access the services provided by servers. This includes personal computers, smartphones, and tablets.

Together, these components form the ecosystem of a network, ensuring seamless data flow, accessibility to network resources, and maintaining the overall health and security of the network environment.

2.3.2 Network Topology

“When building a network infrastructure, its necessary to decide on a good and reliable topology.
Network Topology represents the arrangement of network setup and how each node and link relate to each other and their connections” - 1* (Priya Pedamkar 2023, Chapter 1, Key Highlights). It's like the blueprint that shows how all the devices on the network are connected.

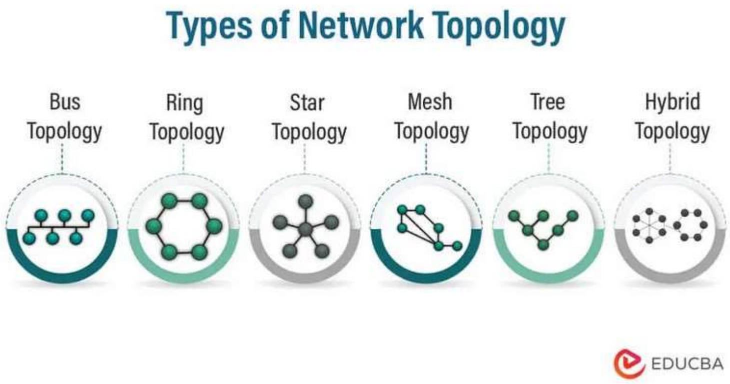


Figure 1 Screenshot of the Types of Network Topology. Priya Pedamkar. 2023.

Bus Topology: All devices are linked to a single central cable, simplifying the setup and reducing cable use, but network failure occurs if the main cable fails and performance drops as more devices connect.

Ring Topology: Devices are arranged in a circle, allowing data to flow in one direction, which speeds up processing, though the failure of a single device disrupts the entire network and makes it difficult to modify.

Star Topology: Each device connects directly to a central hub, enhancing reliability as individual link failures don't affect others and easing the addition of new devices, yet the entire network collapses if the hub fails and it requires extensive cabling.

Mesh Topology: Devices are interconnected, offering excellent reliability and redundancy with multiple data paths, but the cost is high due to the extensive need for cables and ports.

Tree Topology: Combines elements of star and bus topologies, facilitating network expansion and scalability, but complexity increases and a failure in the main bus or root hub impacts the entire network.

Hybrid Topology: Integrates various topology types to optimize advantages and mitigate drawbacks, though this customization leads to increased complexity and cost.

Choosing the right topology depends on what the network needs to do, how big it is, how much is the budget, and how crucial it is that it stays up and running without any issues. Each topology brings its own set of pros and cons to the table, affecting everything from speed and reliability to how much of a headache it will be to maintain.

Local Area Network

A LAN is basically a bunch of computers and devices hooked up together in a local area. They let all devices within it talk to each other, share important information, files and use the same applications. In the following picture there are key components of LAN architecture.

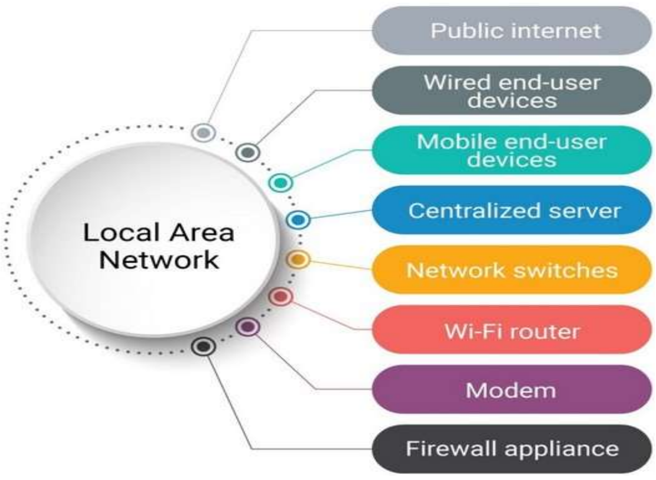


Figure 2 Screenshot of the Key Components of LAN Architecture. Chiradeep BasuMallick. 2022.

Virtual Local Area Network (VLAN) in a LAN it’s a technology that allows a physical network to be divided into multiple logical networks, enabling devices to be grouped together in broadcast domains on factors like department or function, rather than physical location. This segmentation boosts network performance by reducing unnecessary traffic and enhances security by isolating sensitive segments.

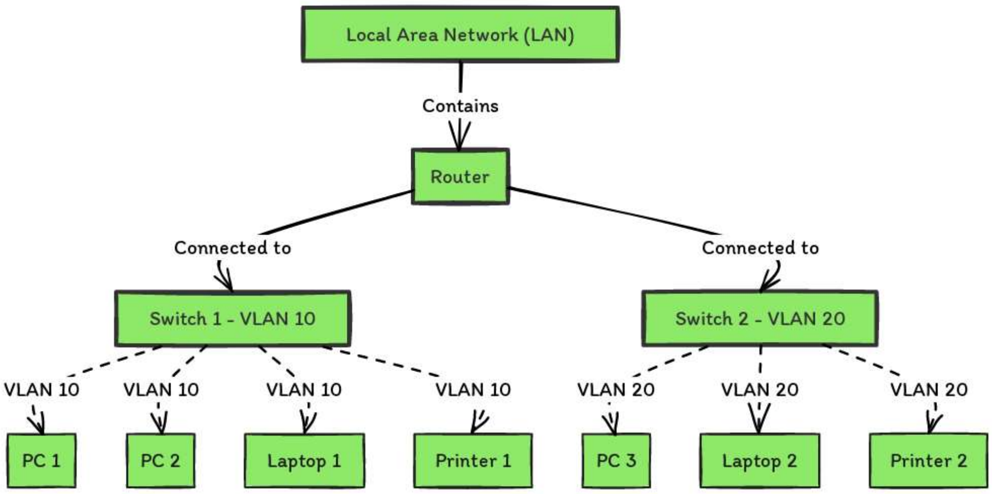


Figure 3 Representation of VLAN inside LAN.

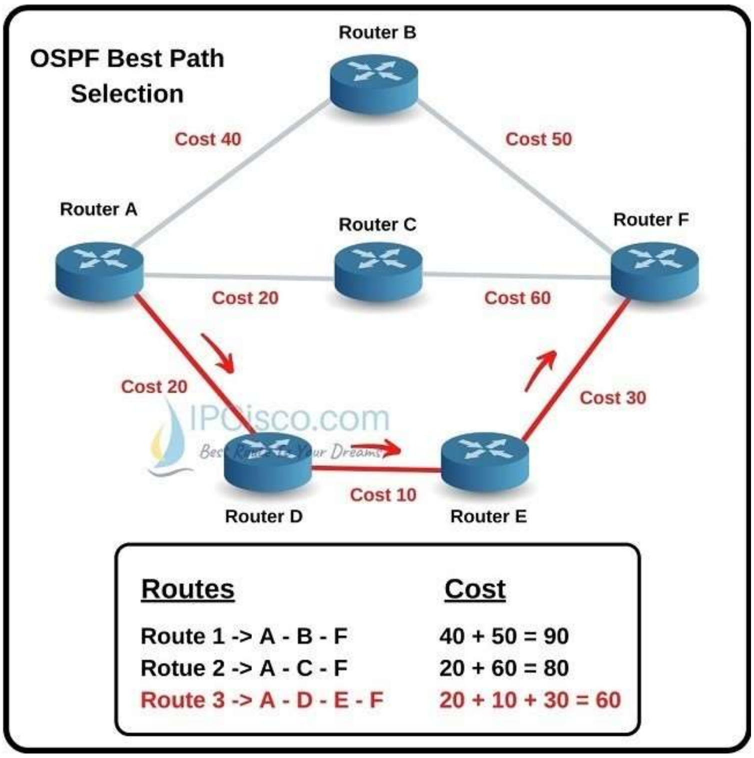
Table 1 Advantages and disadvantages of VLAN and VLAN.

	Advantages:	Disadvantages:
LAN	+ High data transfer rates ideal for intensive applications. + Enables resource sharing, improves operational efficiencies. + Low latency advantageous for real-time applications. + Easier security management due to localized network.	- Restricted to a small geographical area. - High initial infrastructure and maintenance costs. - Scalability can be complex and costly. - Single points of failure impacts whole network.
VLAN	+ Reduces network bottleneck by logically segmenting traffic. + Enhances security by isolating network segments. + Offers flexible and efficient network management by grouping devices. + Optimizes existing infrastructure, leading to cost savings.	- Increased complexity in setup and management. - Potential for security gaps due to misconfigurations. - Scalability challenges as network demands grow. - Added latency due to inter-VLAN routing requirements.

As you can see in the Table 1, a combination of LAN and VLAN technologies provides a well-organized framework for network design, offering both the physical infrastructure for connectivity and the logical architecture for optimized performance and security.

Open Shortest Path First

By systematically evaluating all possible routes to construct the shortest path tree for each node, OSPF ensures that data packets traverse the most efficient, cost-effective paths. This adaptability to network changes and ability to balance load while minimizing latency makes OSPF integral to the design of scalable, high-performance networks. In the following Picture 3, you can see a representation of the way algorithm works.



Routes	Cost
Route 1 -> A - B - F	40 + 50 = 90
Rotue 2 -> A - C - F	20 + 60 = 80
Route 3 -> A - D - E - F	20 + 10 + 30 = 60

Figure 4 Screenshot of OSPF Shortest Path First Algorithm. IPCisco. 2024.

The protocol’s ability to hierarchically segment large networks into areas further enhances efficiency and stability, optimizing resource allocation by localizing traffic and reducing routing table size, thus saving both processing time and memory.

2.4 Security Measures

For a company planning to set up a network that accommodates all users, with considerations for both wired and wireless connectivity, shared resources, and separate VLANs. A comprehensive understanding of theoretical security information is crucial. The following key theoretical security concepts and measures that should be considered.

2.4.1 Network Segmentation and Isolation

Dividing a network into smaller, manageable parts, known as network segmentation and isolation, is a key tactic in making networks both safer and faster. By breaking down a big network into small segments, we limit the amount of traffic and the chance of security problems, which makes it easier to handle the network and fix any issues that come up.

Segmentation - means splitting the network into separate areas, or segments. This can help keep important data safe by putting it in its own section away from the rest of the network. It also makes the network run smoother because each part only deals with its own traffic, cutting down on unnecessary data flow, it helps meet strict rules about how certain types of data need to be handled.

To create these segments VLANs are used, which group devices into their own virtual networks even if they're not physically connected the same way, or by subnetting, which organizes devices based on their IP addresses.

Subnetting

“A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.” - 2* (What is a subnet. Cloudflare. 2024)

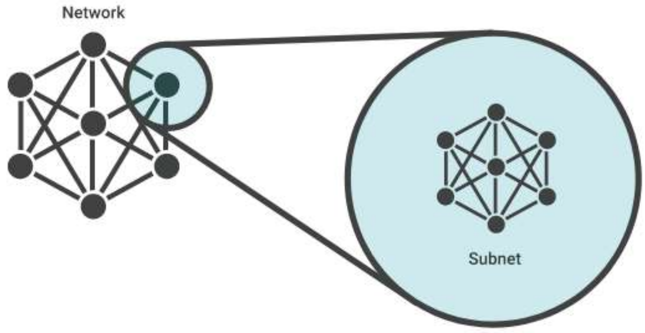
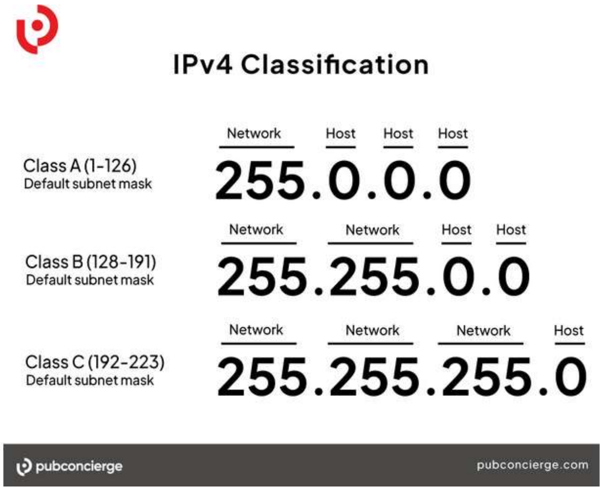


Figure 5 Screenshot of Subnet. Cloudflare. 2024.

This is a method used to split a single IP network into several smaller networks, known as subnets, enhancing network performance, security, and IP address management. It adjusts the network mask to carve out these subnets from a larger network. An IP address, marking each device on a network, consists of a network and a host portion, with the subnet mask defining the division between these two parts. Each subnet is identified by a unique network address and can communicate internally using a broadcast address.



IPv4 Classification

	Network	Host	Host	Host
Class A (1-126) Default subnet mask	255	0	0	0
	Network	Network	Host	Host
Class B (128-191) Default subnet mask	255	255	0	0
	Network	Network	Network	Host
Class C (192-223) Default subnet mask	255	255	255	0

Figure 6 Screenshot of IPv4 Classification. Carol Zafiriadi. 2024.

The main reasons for subnetting include reducing network traffic by confining broadcasts within subnets, which helps in easing congestion. It also boosts security by allowing network segments to be isolated, controlling access, especially to sensitive parts of the network. Subnetting makes for a more efficient allocation of a limited number of IP addresses, particularly valuable for IPv4 addresses. It also simplifies network management by breaking down large networks into smaller, more manageable chunks.

The process involves determining the number of required subnets and hosts, selecting an appropriate subnet mask to create the desired subnets, and then calculating the specific network and broadcast addresses for each subnet. Devices within each subnet are assigned IP addresses that fall within that subnet's address range. For example, changing a Class C network's subnet mask from 255.255.255.0 to 255.255.255.192 can create four subnets, each supporting 62 devices. Subnetting is a key networking practice that aids in creating efficient, secure, and manageable network environments.

Isolation

It goes a step further by really controlling how segments talk to each other. This can be done physically, by using completely separate networks, or logically, by setting rules about how devices on the same network can communicate. This helps tailor security measures to each segment's needs, keeps problems contained to just one area, and controls who can access what parts of the network.

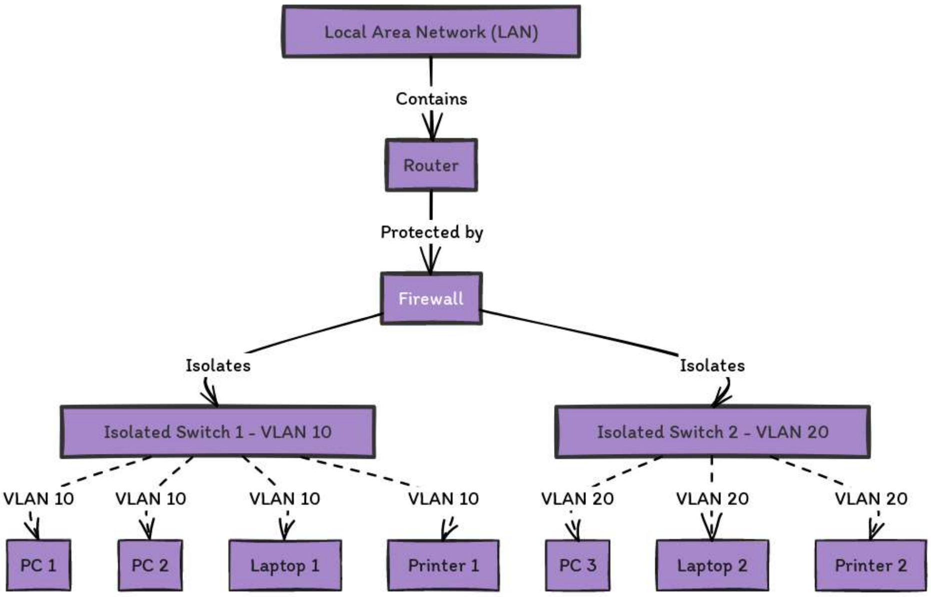


Figure 7 Representation of Isolation.

To do this, we can use firewalls or rules (known as ACL) to decide what traffic is allowed between segments. Also, we will use different physical networks for different purposes, like keeping guest Wi-Fi separate from the main corporate network, to achieve a high level of separation.

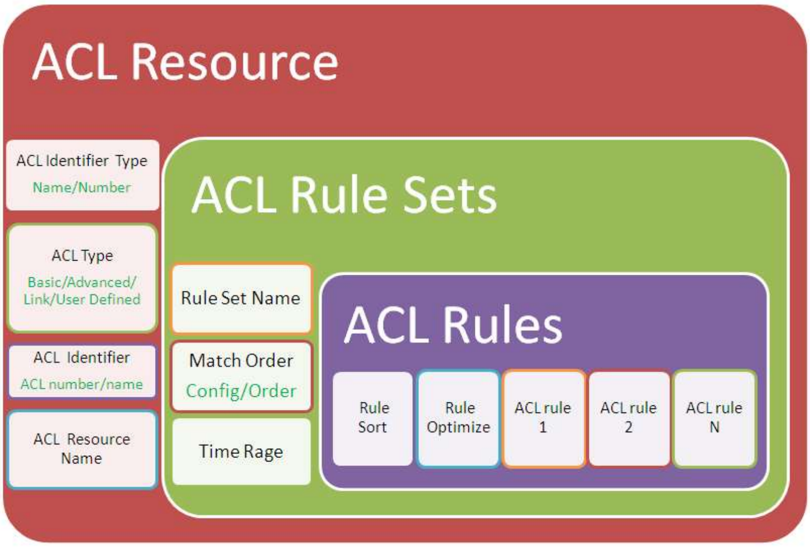


Figure 8 Screenshot of ACL Representation. Hewlett Packard Enterprise Development LP. 2016.

The Picture 6 is a representation of ACL structure in a hierarchical format with three main levels:

ACL Resource: At the top level, it describes attributes such as ACL Identifier Type (Name/Number), ACL Type (Basic/Advanced/Link/User Defined), ACL Identifier (ACL number/name), and ACL Resource Name.

ACL Rule Sets: The middle level, encapsulated within the ACL Resource, lists attributes for defining rule sets. It includes Rule Set Name, Match Order (Config/Order), and Time Range for when the rules are applied.

ACL Rules: At the bottom level, individual rules within a set are defined. This includes Rule Sort, Rule Optimize, and a series of individual rules labeled from ACL rule 1 through ACL rule N, indicating there can be multiple rules within a set.

The colors and the blocks visually represent the structure and relationships between these components, showing that ACL Rules are part of ACL Rule Sets, which in turn comes under the ACL Resource.

Overall, using network segmentation and isolation makes networks more secure and efficient. This approach is crucial in complex setups, keeping things running smoothly and safely is a top priority. Carefully setting up these segments and controlling how they interact can greatly cut down on security risks while keeping the network speedy and reliable.

2.4.2 **The Principle of Least Privilege (PoLP**)

“The principle of least privilege (POLP) is a concept in computer security that limits users' access rights to only what is strictly required to do their jobs. POLP can also restrict access rights for applications, systems and processes to only those who are authorized. This principle is also known as the access control principle or the principle of minimal privilege” - 3[*] (principle-of-least-privilege-POLP. Alexander S. Gillis. 2023)

This principle is applied in a few ways:

- **For Users**: People should only have access to the parts of a system that are necessary for their work.
- **For Systems and Apps**: These should run with the least amount of privilege needed, so if there's a security issue in one area, it doesn't put the whole system at risk.
- **Time Limits**: Sometimes, extra access is only needed for a short time, so it's given temporarily and then taken away.

To put this principle into practice, roles can be created with specific permissions, and users are assigned these roles based on their job needs. Another strategy is to grant special permissions only when needed and only for a limited time. Regular checks are also important to make sure that access levels are still appropriate, especially if someone's job changes or they leave the company.

“Following this principle helps reduce the chance of security issues, because it limits how much damage can be done if something goes wrong. The processing of personal data must always be based on law. Compliance with the regulations on the protection of personal data is supervised by an independent authority.” - 4[*] (Data Protection. Finland. 2024.)

The challenge is to balance security with making sure that these restrictions don't get in the way of people doing their jobs, especially in complex IT environments. But despite the challenges, maintaining the Principle of Least Privilege is key to keeping systems safe and secure.

2.4.3 Data encryption

In networking, data encryption is vital for keeping information safe as it moves across connections, especially on public networks like the internet. Encryption makes sure that data is confidential and unchanged from start to finish, protecting it from unauthorized snooping or tampering.

Key points of data encryption:

- **Encryption Protocols**: Important protocols include TLS for web connections, IPSec for VPNs, and SSH for secure remote commands, each playing a crucial role in network security.
- **VPN Encryption**: VPNs use encryption to create a secure passage over public networks, keeping sensitive data safe from external threats, essential for remote work and data protection.
- **Wireless Security**: Wi-Fi networks use standards like WPA2 to prevent eavesdropping by encrypting data between devices and access points.
- **Secure Communication**: Protocols like S/MIME and PGP, along with encrypted messaging services, keep emails and messages private, ensuring they're read only by intended recipients.

Encryption across network layers

At the application layer, end-to-end encryption ensures data is secured from its origin to its final destination. The transport layer sees protocols like TLS encrypting data for applications, providing a secure transmission over the network. At the network layer, IPSec secures all traffic, making it a to-go for VPNs connecting different network sites.

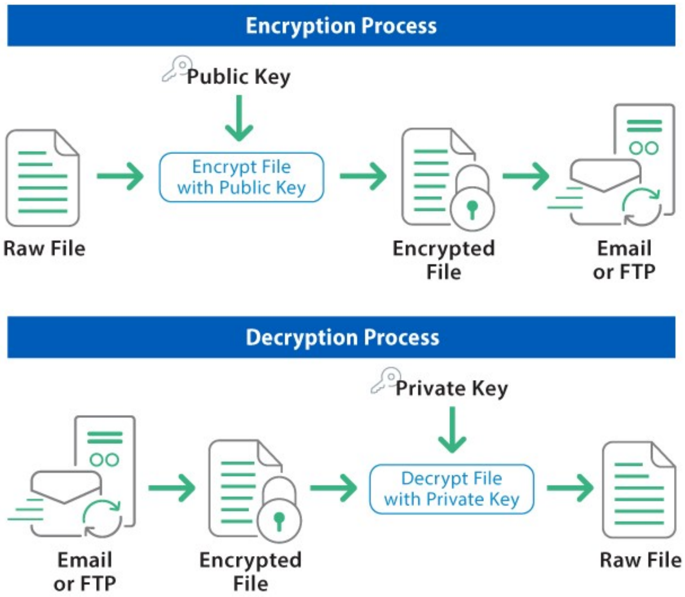
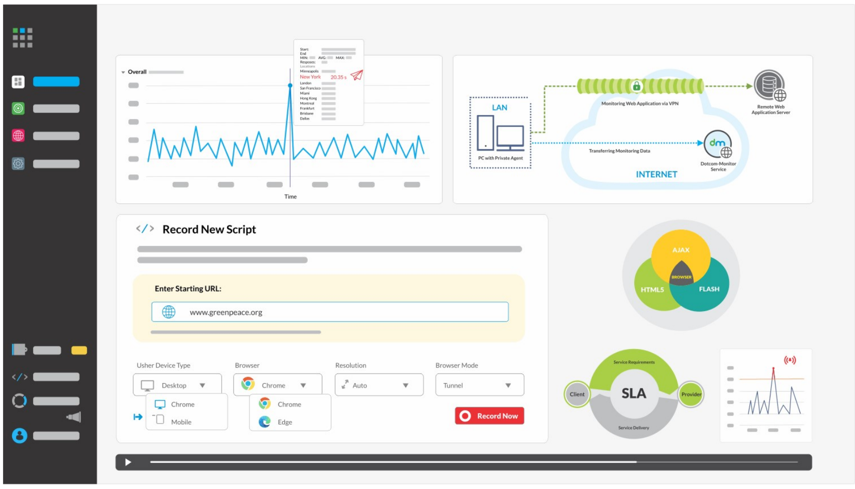


Figure 9 Screenshot of Encryption Process. Fortra LLC. 2024.

Overall, network data encryption is foundational to maintaining secure and trusted communications, safeguarding data from security threats and ensuring privacy across networks.

2.4.4 Monitoring

Monitoring in network and system management is essential for keeping an eye on IT components to ensure they're running smoothly, securely, and reliably. This involves using tools to collect data on performance, security, availability, and system events, helping IT teams stay informed about their infrastructure's status and address potential issues early on.



Record New Script

Enter Starting URL: www.greenpeace.org

Usher Device Type: Desktop

Browser: Chrome

Resolution: Auto

Browser Mode: Tunnel

Figure 10 Screenshot of Monitoring View. Dotcom-Monitor. 2024.

Essential monitoring areas:

- **Performance**: This tracks how well networks, servers, and apps are doing, focusing on metrics like bandwidth, latency, and response times.
- **Security**: The goal is to spot threats and weak spots by checking network traffic and logs for signs of unauthorized access or malware, aiming for quick threat response.
- **Availability**: Monitoring ensures users can access services and resources, looking at system uptime and service functionality to avoid downtime.
- **Fault and Event**: This involves keeping tabs on system errors and significant events to identify and fix problems quickly.

Effective monitoring improves successful IT operations, offering the insights necessary to keep tech environments healthy and secure. By having a solid monitoring approach a company can guarantee the smooth operation of their critical systems and services. Some common network monitoring tools include SNMP and Syslog.

2.4.5 Firewalls

Firewalls serve as crucial network security key points, that regulate incoming and outgoing traffic based on set security rules, acting as a shield between secure networks and external ones like the internet. They check traffic to decide if it should be allowed or blocked, helping against unauthorized access and cyber threats.

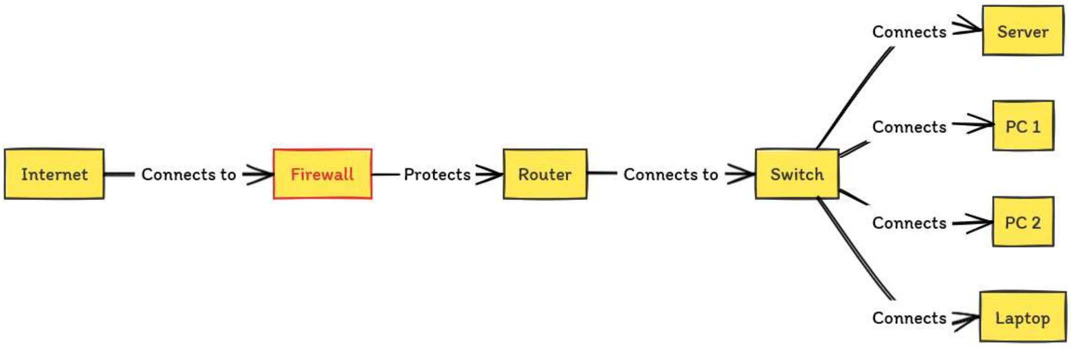


Figure 11 Representation of Firewall.

Firewall categories

Packet Filtering - Basic type that checks data packets at the network level based on IP addresses, ports, and protocols.

Stateful Inspection - More advanced, tracking active connections and considering the traffic's context for enhanced security.

Proxy Firewalls - Work at the application layer, inspecting content and blocking harmful material, such as malware.

Next-Generation Firewalls - Combine traditional firewall capabilities with extra features like deep packet inspection and intrusion prevention.

Web Application Firewalls - Focus on protecting web applications by filtering HTTP traffic to thwart web-based attacks.

Firewall implementation strategies encompass deploying physical hardware units to guard the network gateway, installing software-based firewalls on individual devices for localized protection, and integrating cloud-based firewalls for scalable and flexible network security. These layers work in concert to create a comprehensive defense mechanism against cyber threats.

To safeguard internal networks by managing traffic based on rules, stop data breaches by blocking unauthorized access and detect, then stop malicious traffic. Firewalls are a foundational security measure, and their effectiveness is amplified when paired with other security protocols, proper setup, and ongoing updates protecting the network infrastructure.

2.4.6 Secure remote access

Secure Remote Access allows individuals to connect to networks, systems, or applications from afar while keeping the accessed data and resources secure. This is especially crucial for businesses with remote workers. The goal is to provide seamless, efficient, and safe connectivity, guarding against unauthorized entries and security threats.

Essentials of secure remote access

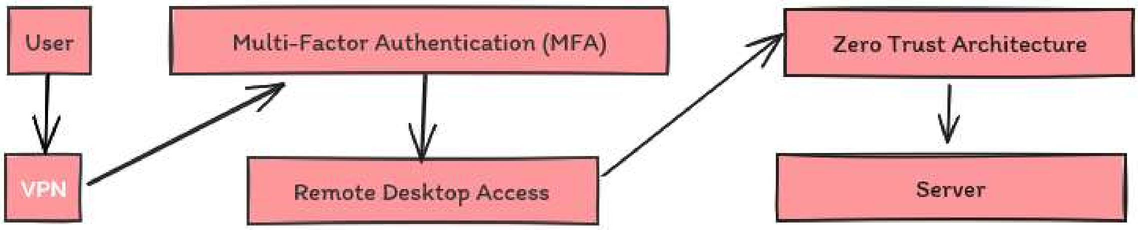


Figure 12 Representation of Secure Remote Access.

Secure remote access is founded on the implementation of VPNs which create a secure, encrypted tunnel for data, multi-factor authentication which adds an extra layer of security beyond passwords, remote desktop services that allow users secure access to a distant computer's interface, and zero trust network access policies that require verification of all users and devices before granting network access.

Secure remote access is vital for protecting company data, ensuring only authorized, encrypted access to sensitive information. It supports operational agility, allowing employees to remain productive from any location, also assists in meeting data security and privacy regulations, safeguarding sensitive information as per legal standards. Secure remote access is indispensable, providing the necessary balance between operational flexibility and security to protect organizational assets.

2.4.7 Regular security audits and compliance

Regular security audits and compliance checks are like health check-ups for an organization's IT security, making sure everything is up to date and strong against potential threats. These reviews look at security rules, how well security tools like firewalls and antivirus programs are working, and if the company is following laws and standards that apply to its industry, like GDPR for privacy information.

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that applies across the European Union (EU) and the European Economic Area (EEA). Its primary goal is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Critical elements of GDPR involve empowering individuals with the ability to access, delete, and move their personal information. It obligates entities to protect this data by obtaining explicit consent and implementing advanced security practices, along with the requirement to quickly report any data breaches. The regulation impacts businesses both inside and outside the EU, particularly those engaging with EU citizens or analyzing their behaviors. Therefore, adherence to GDPR is crucial for any organization processing the personal data of EU individuals, highlighting the global significance of data privacy and protection.

There are different ways to do these checks:

- **Internal Audits**: The company's own team checks everything internally.

- **External Audits**: Outside experts come in to give an unbiased look.
- **Penetration Testing**: This is like a practice attack to see how well defenses hold up.
- **User Access Reviews**: Making sure only the right people have access to certain information.

Audits are essential as they identify security vulnerabilities before they escalate, demonstrate compliance with security standards to build trust, prevent legal issues and safeguard reputation, and strengthen long-term security through continuous improvement.

To keep everything in line, companies use special tools to watch their systems all the time and regularly look at reports on how well they're doing. They might follow certain guidelines like ISO to shape their security and compliance efforts.

International Organization for Standardization (ISO), develops and publishes a wide array of standards that ensure quality, safety, and efficiency across various industries and sectors worldwide.

"The security aspect of data protection is analyzed based on the major requirements of the General Data Protection Regulation and mapped to the relevant controls of the ISO/IEC 27001/27002 standards." - 5[*] (Does personal data protection matter for ISO 9001 certification and firm performance? Emerald Publishing Limited. 2023)

"Encryption of personal data has additional benefits for controllers and/or order processors. For example, the loss of a state-of-the-art encrypted mobile storage medium which holds personal data is not necessarily considered a data breach, which must be reported to the data protection authorities. In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount a fine is imposed as per Art. 83(2)(c) of the GDPR." - 6[*] (Encryption. GDPR. 2024)

In short, keeping up with security audits and compliance is crucial for keeping an organization IT environment safe and trustworthy, ensuring it meets both internal standards and external regulations.

2.5 Disaster recovery and business continuity

Disaster Recovery (DR) and Business Continuity (BC) are vital parts of an organization's approach to dealing with unexpected disruptions, focusing on different recovery and continuity aspects.

DR is all about getting systems back online after incidents like natural disasters or cyber-attacks. It involves data backups, clear recovery objectives (RPO and RTO), and having alternate IT operation sites ready.

BC covers maintaining or quickly restarting all business activities, not just IT, in the face of major disruptions. It includes analyzing how disruptions affect business (BIA), creating wide-ranging plan.

Integrating DR and BC into a unified strategy enhances company’s resilience, ensuring IT recovery aligns with broader business goals. This is crucial for minimizing downtime, mitigating operational risks, and meeting industry regulations, ultimately protecting the organization's reputation and assets.

2.6 Emerging technologies and vendor selection

Emerging Technologies:

Emerging technologies are the peeks of IT innovation and can offer a lot of advantages, like improved efficiency, and enhanced security. Vendor selection is the process of choosing providers for these technologies, a critical step that affects the quality and reliability of the deployed infrastructure.

- **Artificial Intelligence and Machine Learning**: AI and ML are revolutionizing data analysis, automation and predictive systems, improving cybersecurity, user service and operational efficiency.
- **Internet of Things (IoT):** IoT devices are becoming more needed in the workspace, expanding connectivity and data collection capabilities across various devices and environments.

- **5G Technology:** 5G networks offer vastly improved speed and connectivity, which can enable advancements like enhancing mobile connection capabilities.
- **Cloud Computing and Serverless Architectures:** Cloud services continue to evolve, with serverless computing allowing companies to run applications without managing the underlying infrastructure.

Vendor Selection:

Nowadays the selection of vendors for technology involves several considerations, since it’s very competitive area. A need to be always on top is a necessity, and these points are the things you need to look out for:

Expertise and Reliability - Vendors should demonstrate a history of reliable service and proven expertise in their technologies.

Compatibility and Integration - It's crucial that new technologies integrate seamlessly with existing systems without necessitating extensive customization.

Security and Compliance - New technologies must adhere to stringent security standards and aid organizations in maintaining regulatory compliance.

Scalability and Flexibility - Technologies should be capable of scaling with the business and adaptable to evolving needs.

Support and Maintenance - Effective vendor support and clear maintenance agreements are essential for resolving potential issues.

Cost-Effectiveness - Technology investments should be budget-friendly and offer a favorable return on investment without compromising quality.

Innovation Potential - Vendors should be committed to innovation and the continual enhancement of their offerings.

When evaluating emerging technologies and vendors, it's vital for companies to perform thorough due diligence, including product demonstrations and adaptations with existing systems. This helps ensure that the selected vendors and technologies will meet the organization's current needs and support future growth.

2.7 Data collection and analysis:

To collect and analyze data about the current network infrastructure, following theoretical framework and having well-structured approach, will focus on these key points:

Inventory Collection - Compile a detailed inventory of all network assets, including routers, switches, firewalls, servers, and other network devices, as well as software versions and configurations.

Performance Baselines - Establish performance baselines by collecting data on current network usage, throughput, latency, error rates, and other relevant performance metrics.

Security Posture Review - Review the current security measures, including firewall configurations, access control lists, and security protocols. Analyze security logs to identify potential vulnerabilities or past incidents.

Compliance Auditing - Ensure that the current network setup complies with applicable regulations and standards, such as GDPR, HIPAA, or industry-specific requirements.

Technology Research - Investigating emerging technologies and solutions that could address the identified gaps and meet the modernization requirements.

By systematically collecting and analyzing data across these areas, we can ensure that the modernization plan is well-informed, strategic, and aligned with the organization's goals.

3 Current state analysis

Using theoretical framework as a template, review of all network infrastructure.

3.1 Company overview

The company in question specializes in business application development, providing business solutions to an international clientele. With a workforce of 40 employees, its located in Lithuania, the team is a blend of IT personal - DevOps engineers, system administrators, support staff, front-end and back-end developers who are the backbone of the company's product development efforts. These technical experts work to design, develop, and maintain innovative applications that cater to the diverse needs of business clients.

In addition to the technical team, the company has a group of traders who rely heavily on the company's IT infrastructure to execute trades and manage financial transactions efficiently. This aspect of the business highlights the company's involvement in development market and the need for high-performance computing and real-time data processing capabilities.

As an entity, the company faces the challenge of catering to clients while maintaining high standards of service and product quality. Its international operations necessitate adherence to regulatory requirements and the need for a scalable and secure IT infrastructure that can support growth without compromising on performance or security.

The office stands as a strategic hub for the company's development and day to day work. As the company continues to expand, the need for growth is necessary.

3.2 Network topology

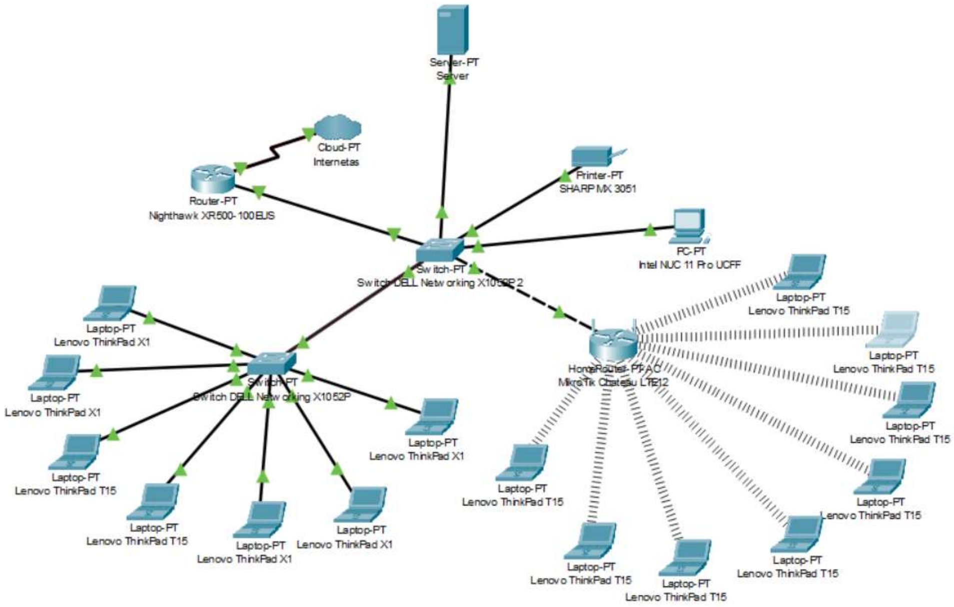


Figure 13 Current Network Topology (Made using Cisco Packet Tracer)

In the network topology is , there are several key components interconnected, forming the infrastructure of a local area network (LAN). Here's a breakdown based on the elements:

3.2.1 Components

Routers "Nighthawk XR500" and "MicroTik Chateau LTE12" serves as the gateway between the local network and external networks, like the internet or users connecting via VPN.

Table 2 Router Information

Router Model:	**Nighthawk XR500**	**MicroTik Chateau LTE12**
Role:	Local Network Gateway	Internet & VPN Gateway
IP Address:	10.0.0.1	10.0.1.1
Subnet Mask:	255.255.255.0	255.255.255.0
Default Gateway:	ISP Gateway	LTE Gateway

DHCP Range:	10.0.0.2 - 10.0.0.254	10.0.1.2 - 10.0.1.254
DNS Servers:	1.1.1.1	1.1.1.1
Additional Features:	QoS, Firewall, Traffic Monitoring	VPN, QoS, Firewall, Traffic Monitoring
Ports:	2x USB 3.0, 1x Wan and 4 x Lan Gigabit Ethernet	5 x Gigabit Ethernet , USB-A 2.0
Power:	Internal, 1x 450W	Internal, 1x 450W

Switches: Network switches “DELL Networking X1052P” are used to connect various devices within the LAN, enabling them to communicate with each other.

Table 3 Switches Information

Switch Model:	**DELL Networking X1052P(A)**	**DELL Networking X1052P(B)**
Role:	Network Connections (LAN, VLAN)	Network Connections (LAN, VLAN)
IP Address:	10.0.2.1	10.0.3.1
Default VLAN ID	10	20
Connected Devices	7 Laptops, 1 Switch	2 Routers, 1 Server, 1 Switch, 1 Printer
VLAN IP Range	10.0.10.1-10.0.10.254	10.0.20.1-10.0.20.254
DNS Servers:	1.1.1.1	1.1.1.1
Ports:	Layer 2+, 24 x 10/100/10002 x Gigabit SFP, 1 USB	Layer 2+, 24 x 10/100/10002 x Gigabit SFP, 1 USB
Power:	Internal, 1x 450W	Internal, 1x 450W

Server: A “Think System SR250 Rack Server” is a dedicated machine for hosting services, which include file sharing, application hosting, and other services.

Table 4 Server Information

Server Model:	**Think System SR250 Rack Server**
Role	Application/Database Server
Processor	Intel Celeron G4900 2C+1 3.1GHz 54W
OS:	Linux
RAM	64GB, 2666Mhz
Storage	4x256GB SSD, 10x HDD 1TB
IP Address	10.0.30.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.30.1
VLAN ID	30
DNS Servers	10.0.30.10, 10.0.30.11
Ports	1x USB 2.0, 3x USB 3.1, 1x Serial COM, 1x VGA. 1x RJ-45

Wireless Access Points: “Mikrotik Chateau LTE12” had integrated access point, it enables wireless devices to connect to the network.

Table 5 Wireless Access Point Information

SSID:	Office WIFI
Password:	Uderstate2#Saigus19

Encryption:	WPA2-PSK
Frequency:	2,4 HZ

End-User Devices: Various laptops create business environment where mobility and portability are important. The network supports numerous users, through both wired and wireless connections.

Table 6 Computer Information

Name:	**Lenovo ThinkPad T15**	**Lenovo ThinkPad X1**	**Intel NUC 11 Pro UCFF**
Processor:	Core i5-10310U 4x8, 1,7GHz, 6 MB	Core i5-10310U 4x8, 1,7GHz, 6 MB	Core i5-1145G7 4x8, 2.6 GHz, 8 MB
Graphic card:	Intel UHD Graphics, NVIDIA® GeForce MX330	Intel Iris Xe Graphics	Intel Iris Xe Graphics
Memory:	32 GB 2133 MHz	16 GB 2133 MHz	16 GB 2133 MHz
Storage:	512 GB	256 GB	256 GB
OS:	Windows 11	Linux , Windows 11	Windows 11
Ports:	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2 Gen x 2, Ethernet (RJ-45), HDMI 1.4b, USB-C 3.2 x 2.	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2 Gen x 2, HDMI 1.4b, USB-C 3.2 x 2.	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2, HDMI 1.4b, USB-C 3.2.
IP address:	10.0.20.3-254\24	10.0.10.2-254\24	10.0.20.3\24
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway:	10.0.20.1	10.0.10.1	10.0.20.1
DNS Servers:	1.1.1.1	1.1.1.1	1.1.1.1, 8.8.8.8

Printer: There's a network printer “SHARP MX-3071”, which allows users to print from a centralized device over the network.

Table 7 Printer Infotmation

Name:	**SHARP MX-3071**
Function:	Industrial Printer
Ports:	RJ-45 Ethernet, USB 2.0 x2, wireless 802.11 a/b/g/n
IP address:	10.0.40.2
Subnet Mask:	255.255.255.0
Default Gateway:	10.0.40.1

Cables: The whole building is already wired using raised flour method and all the cables come to one space, where they are labeled by room name and id, so there is no need to focus on wires.

Table 8 Cable information

Cable Type:	**Purpose:**	**Location:**	**Specs:**
Cat6 Ethernet	Connecting PCs to Switches	Office LAN	Up to 1Gbps
Cat6a Ethernet	Switch to Switch connections	Office LAN	Up to 10 Gbps
Cat6 Ethernet	Switch to Router connections	Office LAN	Up to 1Gbps
Cat6a Ethernet	Connecting servers to Switch	Server LAN	Up to 10 Gbps
Single-Mode Fiber	Long distance to ISP connection	Building WAN	Up to 10 Gbps

Power Cables	Providing power to devices	All Environments	Unique by device

These are all the physical component that make the network infrastructure.

3.3 Security measures

Security for a network is a key part, moving forward we will showcase all the configurations found in the current network infrastructure.

3.3.1 Network segmentation and isolation

VLAN segmentation

Table 9 VLAN Information

VLAN ID	Purpose	IP Range	Subnet Mask	Default Gateway
10	IT VLAN	10.0.10.1 - 10.0.10.254	255.255.255.0	10.0.10.1
20	User VLAN	10.0.20.1 - 10.0.20.254	255.255.255.0	10.0.20.1
30	Server VLAN	10.0.30.1 - 10.0.30.254	255.255.255.0	10.0.30.1
40	Printer VLAN	10.0.40.1- 10.0.40.254	255.255.255.0	10.0.40.1

VLAN 10 (IT VLAN): This VLAN is dedicated to devices and users belonging to IT team. It isolates traffic from the rest of the network for security and bandwidth purposes.

VLAN 20 (User VLAN): Similar to VLAN 10, this VLAN is exclusive to users, ensuring their traffic is segregated from other network segments.

VLAN 30 (Server VLAN): Server is placed in a separate VLAN to limit access to critical infrastructure and to enhance performance by reducing broadcast traffic to server interfaces.

VLAN 40 (Printer VLAN): Printer and other peripheral devices are grouped in this VLAN to isolate their traffic and to manage access to these resources.

Each VLAN is associated with a specific subnet, providing logical IP segmentation that aligns with the VLAN structure, simplifying IP management and enhancing security by limiting the broadcast domain size.

Access Control Lists (ACLs)

Table 10 ACL Information

- Permit TCP and UDP from IT VLAN (10.0.10.0/24) to all VLANs for network management and monitoring - Deny all inbound traffic from other VLANs to IT VLAN (10.0.10.0/24) except for responses to established connections
- Permit TCP and UDP from User VLAN (10.0.20.0/24) to Server VLAN (10.0.30.0/24) on ports 80 (HTTP) and 443 (HTTPS) for accessing internal applications - Permit TCP and UDP from User VLAN (10.0.20.0/24) to Printer VLAN (10.0.40.0/24) for printing services - Deny all direct traffic from User VLAN (10.0.20.0/24) to IT VLAN (10.0.10.0/24)
- Permit necessary management protocols (e.g., SSH port 22) from IT VLAN (10.0.10.0/24) to Server VLAN (10.0.30.0/24) - Deny all non-management traffic from IT VLAN (10.0.10.0/24) to Server VLAN (10.0.30.0/24) - Deny all inbound traffic from other VLANs not explicitly permitted
- Permit TCP port 9100 from User VLAN (10.0.20.0/24) and IT VLAN (10.0.10.0/24 to Printer VLAN (10.0.40.0/24) for printing services - Deny all inbound traffic from other VLANs to Printer VLAN (10.0.40.0/24) except the User VLAN and IT VLAN

3.3.2 The Principle of Least Privilege (PoLP)

The network is organized into specialized VLANs to control access and enhance security.

- The IT VLAN is reserved for network administrators and IT staff for managing infrastructure.
- The User VLAN provides employees with internet and essential internal resources but restricts administrative capabilities.
- Server VLAN access is job-specific, limiting exposure to sensitive systems.
- Printer VLAN is open to users for printing purposes only, with IT managing printer configurations.

Network devices are set up to allow management solely from the IT VLAN, with strong password policies and disabled unused ports for added security. User access to applications and files is strictly role-based, ensuring staff access only what's necessary for their work. Remote access is secured through a VPN with strong encryption and multi-factor authentication. Servers run only essential services to minimize vulnerabilities. Firewalls enforce traffic rules to ensure only necessary business traffic flows through the network. Regular audits and monitoring of access logs help maintain correct user privileges and detect any unusual activity. This structured approach, grounded in the Principle of Least Privilege, minimizes insider threats and accidental misconfigurations, maintaining a secure and functional network environment.

3.3.3 Data encryption

All data transmitted across the network is encrypted using protocols such as TLS for web traffic, SSH for remote administration, and IPsec for network layer encryption.

VPN services are used for remote access, with strong encryption protocols such as OpenVPN and L2TP/IPsec.

Email transmissions are secured using SSL/TLS encryption for SMTP, POP3, and IMAP protocols.

All wireless communications are protected using WPA2-PSK encryption to secure Wi-Fi traffic.

Sensitive data stored on servers or computers is encrypted using disk encryption technologies by 3rd party software “VeraCrypt”

Backup data is encrypted using AES-512 encryption before being stored on backup media or off-site storage.

All encryption practices comply with industry standards and regulations such as GDPR - ISO/IEC 27001.

Regular audits are conducted to ensure compliance with encryption policies and standards.

3.3.4 Monitoring

Most of the monitoring done in the company is by using a 3rd party software, but the key points that are checked regulary:

Device Uptime - Tracking the uptime of switches, routers, and firewalls to detect unexpected reboots or downtime.

Interface Status - Monitoring the status of network interfaces to check if they are up/down and bandwidth utilization.

Error Rates - Looking for high error rates on network interfaces which could indicate physical issues with cables or hardware failures.

Server Availability - Using simple ping tests to ensure servers are reachable.

Resource Utilization - Monitoring CPU, memory, disk, and network utilization to detect potential bottlenecks or capacity issues.

System Logs - Checking server logs for warnings or errors that could indicate problems.

Firewall Logs - Analyzing firewall logs to detect denied connections or unusual traffic patterns.

Authentication Logs - Checking for failed login attempts that could indicate an attack.

External Connectivity - Monitoring the latency and packet loss to services and the internet.

Printer Status - Checking that network-connected printers are online and have paper, toner, etc.

Keeping an eye on these points helps to mitigate potential issues, and resolve them quickly.

3.3.5 Firewalls

Table 11 Firewall Information

Rule #	Source	Destination	Source Port	Destination Port	Protocol	Action
1	10.0.10.0/24	Any	Any	Any	Any	Allow
2	10.0.20.0/24	Any	Any	80, 443	TCP	Allow
3	10.0.30.0/24	Any	Any	Any	Any	Allow
4	10.0.40.0/24	Any	Any	80, 443	TCP	Allow
5	Any	10.0.10.0/24	Any	Any	Any	Deny
6	Any	10.0.20.0/24	Any	Any	Any	Deny
7	Any	10.0.30.0/24	Any	Any	Any	Deny
8	10.0.10.0/24	10.0.30.0/24	Any	22, 3389	TCP	Allow
9	10.0.20.0/24	10.0.40.0/24	Any	9100	TCP	Allow
10	Any	10.0.40.0/24	Any	Any	Any	Deny
11	10.0.100.0/24	10.0.30.0/24	Any	22, 3389	TCP	Allow
12	10.0.100.0/24	10.0.30.0/24	Any	Any	Any	Allow

These rules are designed to:

- **Allow** all traffic originating from the IT VLAN (rule #1), acknowledging that IT needs broad access for management and monitoring.

- **Allow** only web traffic from the User VLAN (rule #2), reflecting a common requirement to enable web access for users.
- **Allow** all traffic originating from the Server VLAN (rule #3) for potential services that need to connect out to the internet or other internal resources.
- **Allow** HTTP/HTTPS traffic from the Printer VLAN for potential firmware updates or cloud printing services (rule #4).
- **Deny** unsolicited inbound traffic to IT, User, and Server VLANs (rules #5, #6, and #7), as a measure to prevent unauthorized access.
- **Allow** administrative protocols like SSH (for secure shell access) and RDP (for remote desktop) from the IT VLAN to the Server VLAN (rule #8), which are needed for server management.
- **Allow** printing services (rule #9) from the User VLAN to the Printer VLAN using the common printing port 9100.
- **Deny** all other inbound traffic to the Printer VLAN to ensure that printing resources cannot be accessed by unauthorized users (rule #10).
- **Allow** VPN users to initiate SSH (port 22) and RDP (port 3389) connections to servers for management purposes (rule #11).
- **Allow** This rule is broader and allows all traffic from VPN-connected clients to access the Server VLAN. (rule #12).

3.3.6 Secure remote access

To connect to company infrastrcuture you will need a VPN. All user profiles are generated by IT team and setup using 3rd party app OpenVPN Connect application, that allows users to connect to network infrastructure. Depending on the case, some profiles have a pre-determinated password or a MFA generated one.

Table 12 VPN Information

Feature	Description
VPN Service Type	OpenVPN
VPN IP Range	10.0.100.0 - 10.0.100.255
Subnet Mask	255.255.255.0

Feature Encryption	**Description** AES-256
Authentication	RSA Certificates / PSK (Pre-shared Key)
Protocol	TCP / UDP
Port	443/1194
Client Config	Profiles generated by IT.

3.4 Regular security audits and compliance

The company engages in regular security audits and compliance checks to ensure that its network and systems adhere to specific security standards and legal requirements. These audits are conducted by an external audit firm and cover a comprehensive range of checks. The audits assess regulatory compliance with standards like GDPR, review security policies, and evaluate physical and data protection measures to ensure sensitive data is securely encrypted and backed up. The process includes vulnerability assessments, penetration testing to probe network defenses, and risk assessments to gauge the potential impact of identified vulnerabilities. Additionally, the company reviews its system logs and audit trails for any suspicious activities, checks the physical security of its infrastructure, and evaluates the security protocols of third-party vendors. The effectiveness of the employee security training programs is also assessed to ensure all staff are well-informed about security best practices. Finally, the company rigorously tests its incident response plan to guarantee it remains effective and up-to-date, with thorough documentation maintained for all procedures. These audits not only help in identifying and solving any security issues but also ensure that the company remains compliant with all necessary regulations, with audits typically occurring annually or following significant changes to the network.

3.4.1 Disaster recovery and business continuity

The company's disaster recovery (DR) setup is robust, featuring a UPS system connected directly to the server infrastructure to provide an additional hour of uptime during electrical failures, ensuring critical systems remain operational as backup power solutions are activated. Additionally, the building is equipped with diesel generators that automatically start during power outages, powering the entire building with only a brief transition downtime. This setup is part of a comprehensive DR and business continuity (BC) strategy that includes systematic data backups—daily, weekly, and monthly—with all data encrypted and securely stored to minimize data loss to a 24-hour window. This dual-layered power backup approach, along with stringent data security measures, safeguards the company’s operations against power outages and data breaches, maintaining data integrity and operational continuity even under adverse conditions.

3.5 Emerging technologies and vendor selection

The company actively seeks out emerging technologies to incorporate into its infrastructure and business strategies, aiming to optimize quality and processes. In the realm of vendor selection, the company places a strong emphasis on achieving a balance between price and quality. A crucial criterion in this selection process is the level of support vendors provide, particularly for integrating and managing new technologies. Given the company's reliance on various third-party software solutions to drive operational excellence, the support offered is essential for smooth implementation and maintenance, ensuring that these tools consistently deliver high performance and contribute to the company's success.

3.6 Observations and analysis

Topology Type: The star topology, with all devices connected to central switches, which are then connected to a router.

Cable Management: The structured cabling approach, where each device is connected back to a central point (the switches), minimizing cable clutter and simplifying maintenance.

Scalability: The use of network switches means that the network is designed to be scalable, allowing for easy addition of new devices without significant restructuring, however there are some problems regarding network load, since the company is growing the need for a better availability is needed.

Security: Security measures such as firewalls within the router, access control lists in the switches, encrypted wireless communication, encrypted devices and data, meets the needs of a secure infrastructure.

Redundancy: There are some issues with networking redundancy, but the main infrastructure has no serious problems, since there is a UPS, for the server and the whole building has a diesel generator at the stand by in case of power outages. Data is constantly backed up, stored locally and in the cloud for quick recovery.

Accessibility: The mix of wired and wireless connections means the network is designed for flexibility in user connectivity, accommodating different user preferences and mobility requirements.

3.6.1 Infrastructure assessment

The company's network infrastructure is meticulously designed to support its operational needs, incorporating advanced hardware and networking strategies to ensure efficiency and security. The network setup includes two primary routers: the “Nighthawk XR500”, serving as the local network gateway, and the “MicroTik Chateau LTE12”, handling internet and VPN gateway functionalities. These routers, along with “DELL Networking X1052P” switches, facilitate a structured connection between various devices within the network, supporting a range of VLAN configurations tailored to specific group needs, such as IT, users, servers, and printers.

The network's server, a “Think System SR250 Rack Server”, is dedicated to hosting critical applications and data storage, ensuring high availability and reliability. To maintain network integrity and security, access to different network segments is carefully managed through VLANs, with stringent access control lists (ACLs) regulating traffic flows to prevent unauthorized access and ensure data security. Moreover, the network leverages well designed security measures including firewalls, encrypted data transmission, and comprehensive security protocols for remote access, ensuring that all interactions within the network are secured and monitored.

Additionally, the network infrastructure is designed for resilience, featuring raised floor cabling for easy maintenance. Regular security audits, network monitoring, and compliance checks ensure that the network remains secure and operates at peak efficiency. The company’s proactive approach in integrating new technology and maintaining security standards exemplifies its commitment to safeguarding data and providing reliable service to all users.

3.7 Challenges and limitations:

The analysis of the infrastructure has uncovered several key challenges and limitations that necessitate immediate attention to ensure the sustainability and efficiency of operations. Despite the foundational strengths observed, issues with network congestion and wireless coverage where found. These constraints not only hamper the system's ability to meet current demands but also restrict future growth and adaptation in a rapidly evolving technological landscape. Addressing these findings is crucial for enhancing the infrastructure's connectivity and readiness for future challenges.

Network Congestion: The network suffers from congestion during peak usage times, which results in slow data transfers and delayed response times. These performance bottlenecks are primarily due to insufficient routing capabilities and limited bandwidth which strains the network under heavy load.

Wireless Coverage: Areas of the workplace experiences inconsistent wireless connectivity, creating zones where network access is unreliable. This issue affects mobile device and users who connect wirelessly, leading to decreased productivity and frustration due to dropped connections and poor signal strength.

Addressing these areas is a must, since they effect the workflow, and moving forward, necessity for a solution and its implementation, that will help us fight these issues is unavoidable.

4 Solution and implementation

Overall the current network efficiency and security are paramount to maintaining productivity and safeguarding sensitive information. However, the current network setup is facing significant challenges that hinder its performance and reliability. During peak usage times, the network becomes congested, leading to slow data transfers and delays, largely due to inadequate routing capabilities and limited bandwidth. Furthermore, the wireless coverage within the workplace is inconsistent, causing connectivity issues that disrupt mobile and wireless device users. These zones of unreliable network access not only decrease productivity but also fuel user frustration.

4.1 Network Congestion

For network congestion issue, we plan to add an extra router, which will help distribute the traffic load and enhance the overall network performance and redundance. Integrating this router effectively into the current setup requires remodeling of the network. This expansion is designed to support future scalability seamlessly without overwhelming the existing network components.

Details of new device

Table 13 Router Ubiquiti EdgeRouter 12 specifications

Router Model:	Ubiquiti EdgeRouter 12
Power Input:	10 - 240VAC, 50/60 Hz, 20 - 30V
Processor:	4-Core 1 GHz, MIPS64
Memory:	1 GB DDR3 RAM
Ports:	(1) RJ45 Serial Port (10) 10/100/1000 RJ45 Ports (2) 1 Gbps SFP Ports

4.2 Enhanced Wireless Access:

Deploying six access points (APs) is a positive step towards improving network coverage and handling increased demand from wireless devices. To fully leverage these new APs, the network’s wireless configuration will be optimized to prevent overlapping channels and ensure security standards are maintained across all wireless communication.

Details of new devices

Table 14 Aruba AP 25 Specifications

Access Point Model:	Aruba AP 25
Max active users:	100+
Data rates:	5374 Mbps
Power:	802.3at (class 4), 20.1WMax, or 12Vdc
Radios:	2.4 GHz 802.11ax (Wi-Fi 6); 5 GHz 802.11ax (Wi-Fi 6)
Ports:	**100/1000/2500 Base-T auto-sensing MDI/MDX Ethernet port**

4.3 Resource Requirements

Successfully executing this network modernization, will require a carefully structured approach to resource allocation across three critical phases: project planning, acquisition of new resources, and project implementation.

The Project Planning stage is critical, requiring substantial time and meticulous strategic planning to ensure that every component of the plan is practical and in line with the organization's broader goals. Essential elements of this phase include the involvement of a skilled network engineer with a deep understanding of network operations, who can evaluate and test the existing infrastructure to pinpoint its shortcomings. Additionally, gathering feedback from users is crucial to identify daily challenges and areas needing improvement. This stage also necessitates the development of clear timelines, the identification of potential risks, and the establishment of specific, measurable objectives to guide the project's progression and ensure its success.

As the project transitions into the acquisition of new resources, significant financial investments become critical. This includes the procurement of new hardware and software, along with potential upgrades to the existing infrastructure. From a human resource perspective, the focus will be on the network engineer, who will play a central role throughout all project phases.

The final phase focuses on the actual rollout of the project, where resources shift towards operational execution. This includes manpower for setting up the infrastructure, conducting thorough testing to ensure everything works as planned, and gathering input from users to address any issues during and after the implementation. Continuous adjustments are necessary to optimize operations based on the issues that occur.

Overall, the resource requirements for this project span across various domains, requiring a blend of technical, human, and financial assets to ensure successful completion and integration into the existing company’s structure.

Table 15 New equipment price list

No.	**Product Name**	**Qty.**	**Price, Euro**	**Total, Euro**
1.	Ubiquiti EdgeRouter 12	**1**	**275**	**275**
2.	Aruba AP 25	**6**	**220**	**1320**
			Total, Euro:	**1595**
			VAT 24%	**382.8**
			Grand Total, Euro:	**1977.8**

4.4 Updated Network Topology

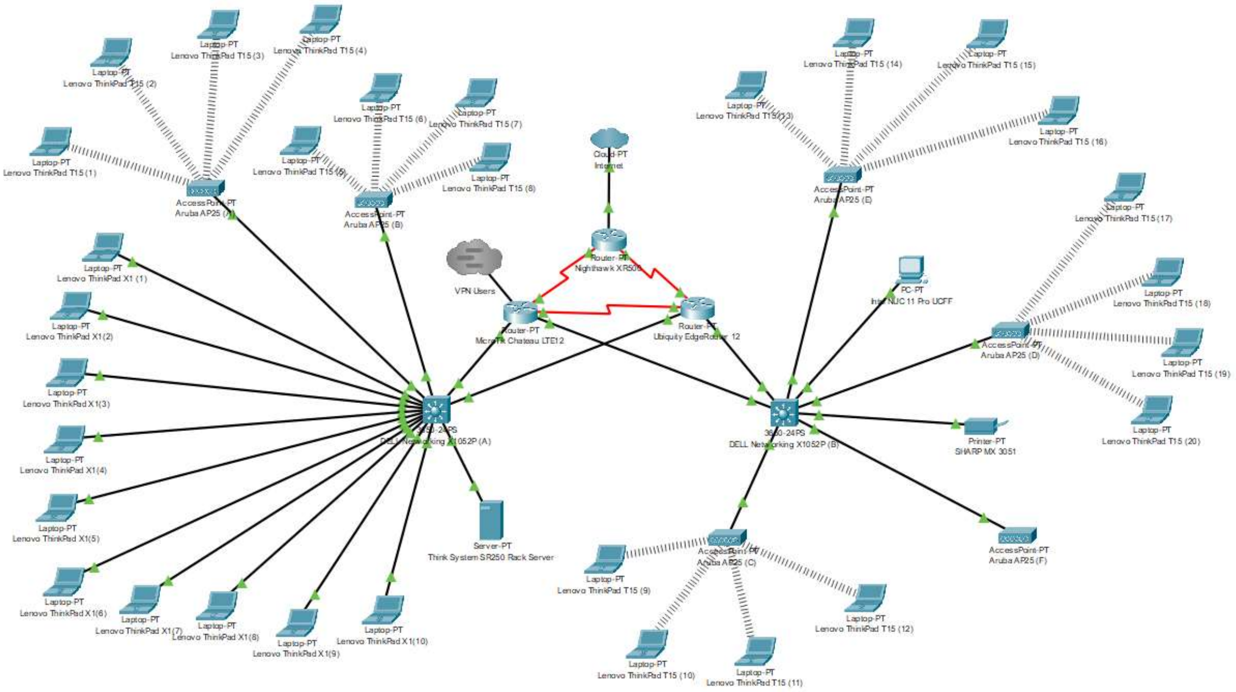


Figure 14 Updated Network Topology (Made using Cisco Packet Tracer)

In the updated network topology, there are several new components interconnected, forming the infrastructure of a local area network (LAN). Here's an updated breakdown based on the new updated elements and their configurations:

4.4.1 Components:

The network contains - **“**Nighthawk XR500”, “MicroTik Chateau LTE12” and “EdgeRouter 12” routers that serve as the gateway between the local networks and external network, like the internet or communication between inner components.

Table 16 Updated Routers Information

Router Model:	**Nighthawk XR500**	**MicroTik Chateau LTE12**	**Ubiquity EdgeRouter 12**

Role:	Local Network Gateway	Internet & VPN Gateway	Connects internal VLANS
IP Address:	10.0.1.1	10.0.1.2	10.0.1.3
Subnet Mask:	255.255.255.255	255.255.255.255	255.255.255.255
Next Hop for Outbound Traffic:	ISP Gateway	10.0.1.1	10.0.1.1
DNS Servers:	1.1.1.1	1.1.1.1	1.1.1.1
Additional Features:	QoS, Firewall, Traffic Monitoring	VPN, QoS, Firewall, Traffic Monitoring	QoS, Firewall, Traffic Monitoring
Ports:	2x USB 3.0, 1x Wan and 4 x Lan Gigabit Ethernet	5 x Gigabit Ethernet , USB-A 2.0	RJ45 Serial Port, 10 x RJ45 Ports, 2 x 1 Gbps SFP Ports
Power:	Internal, 1x 450W	Internal, 1x 450W	External AC/DC Adapter

Network switches “DELL Networking X1052P” are used to connect various devices within the LAN, enabling them to communicate with each other. They have VLAN’s configured inside them that makes devices grouped and better to manage.

Table 17 Updated Switches Information

Switch Model:	**DELL Networking X1052P(A)**	**DELL Networking X1052P(B)**
Role:	Network Connections (LAN, VLAN)	Network Connections (LAN, VLAN)
IP Address:	10.0.2.1	10.0.3.1
VLAN’s ID:	10, 20, 40, 60	30, 50, 60
Connected Devices:	18 Computers, 2 Access points,	13 Computers, 4 Access Points,

	1 Server, 2 Routers.	1 Printer, 2 Routers.
VLAN's IP Ranges:	10.0.10.1 - 10.0.10.254, 10.0.20.1 - 10.0.20.254, 10.0.40.1 - 10.0.40.254, 10.0.60.1 - 10.0.60.254.	10.0.30.1 - 10.0.30.254, 10.0.50.1 - 10.0.50.254, 10.0.60.1 - 10.0.60.254.
Ports:	Layer 2+, 24 x 10/100/10002 x Gigabit SFP, 1 USB	Layer 2+, 24 x 10/100/10002 x Gigabit SFP, 1 USB
Power:	Internal, 1x 450W	Internal, 1x 450W

A "Think System SR250 Rack Server" is a dedicated machine for hosting services, which include file sharing, application hosting, and other features that help the company's workflow. It also has local mail server setup for internal communications.

Table 18 Updated Server Information

Server Model:	**Think System SR250 Rack Server**
Role	Application/Database Server
Processor	Intel Celeron G4900 2C+1 3.1GHz 54W
OS:	Linux
RAM	64GB, 2666Mhz
Storage	4x256GB SSD, 10x HDD 1TB
IP Address	10.0.40.2
Subnet Mask	255.255.255.0
Default Gateway	10.0.40.1
VLAN ID	30

DNS Servers	1.1.1.1
Ports	1x USB 2.0, 3x USB 3.1, 1x Serial COM, 1x VGA. 1x RJ-45

Wireless Access Points Aruba AP 25 covers whole building for wireless access, it allows users to connect to the network without the worry of losing connection.

Table 19 AP's Information

Access Point Model:	Aruba AP 25
Max active users:	100+
Data rates:	5374 Mbps
Power:	802.3at (class 4), 20.1WMax, or 12Vdc
Radios:	2.4 GHz 802.11ax (Wi-Fi 6); 5 GHz 802.11ax (Wi-Fi 6)
Ports:	100/1000/2500 Base-T auto-sensing MDI/MDX Ethernet port (E0)

Table 20 Wireless Access Details

SSID:	Office WIFI
Password:	Uderstate2#Saigus19
Encryption:	WPA2-PSK
Frequency:	2,4 HZ

To gather more detailed information redarding AP deployment and accessability, the building plan was used to create Wi-Fi heatmap with the help of Ekkhau tool.

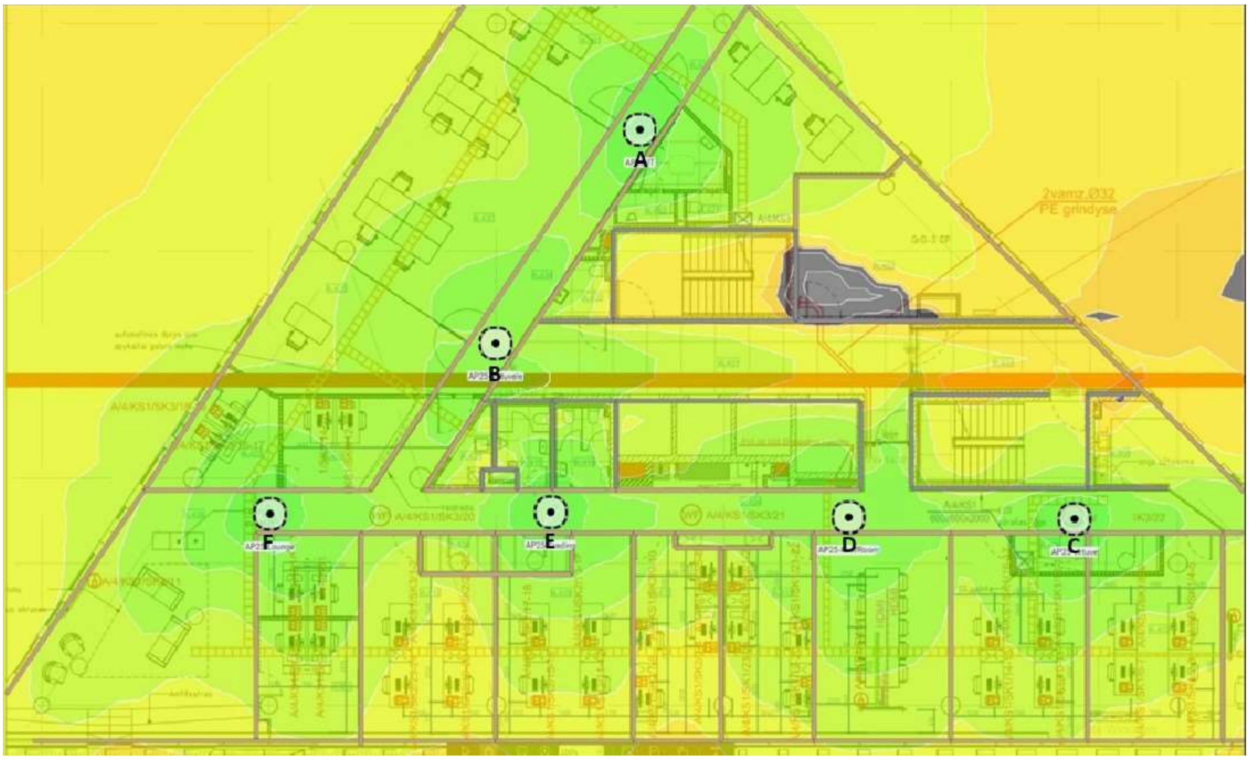


Figure 15 Representation of AP's Heatmap.

In this network environment, a variety of laptops facilitate a balance between mobility and stability, catering to diverse user requirements. Network architecture supports a multitude of users through both wired and wireless connections, thus providing the flexibility necessary for users to tailor their experiences according to their specific needs. This adaptability is crucial component for optimizing both the accessibility and efficiency of network resources, thereby enhancing overall user productivity and satisfaction.

Table 21 Updated Computer Information

Name:	**Lenovo ThinkPad T15**	**Lenovo ThinkPad X1**	**Intel NUC 11 Pro UCFF**
Processor:	Core i5-10310U 4x8, 1,7GHz, 6 MB	Core i5-10310U 4x8, 1,7GHz, 6 MB	Core i5-1145G7 4x8, 2.6 GHz, 8 MB
Graphic card:	Intel UHD Graphics, NVIDIA® GeForce MX330	Intel Iris Xe Graphics	Intel Iris Xe Graphics

Memory:	32 GB 2133 MHz	16 GB 2133 MHz	16 GB 2133 MHz
Storage:	512 GB	256 GB	256 GB
OS:	Windows 11	Linux , Windows 11	Windows 11
Ports:	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2 Gen x 2, Ethernet (RJ-45), HDMI 1.4b, USB-C 3.2 x 2.	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2 Gen x 2, HDMI 1.4b, USB-C 3.2 x 2.	Wi-Fi 6 AX201, 802.11ax 2x2, Bluetooth 5.1, USB 3.2, HDMI 1.4b, USB-C 3.2.
IP address:	10.0.20.12-254\24 10.0.30.4-254\24	10.0.10.2-254\24	10.0.30.3\24
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway:	10.0.10.1, 10.0.20.1	10.0.10.1	10.0.30.1
DNS Servers:	1.1.1.1	1.1.1.1	1.1.1.1

There's a network printer “SHARP MX-3071”, which allows users to print from a centralized device over the network.

Table 22 Updated printer infotmation

Name:	**SHARP MX-3071**
Function:	Industrial Printer
Ports:	RJ-45 Ethernet, USB 2.0 x2, wireless 802.11 a/b/g/n
IP address:	10.0.50.2
Subnet Mask:	255.255.255.0
Default Gateway:	10.0.50.1

The whole building is already wired using raised flour method and all the cables come to one space, where they are labeled by room name and id, so there is no need to focus on wires. In addition the new AP will be connected and place in the sealing since it has the same principle as raised floor.

Table 23 Updated cable information

Cable Type:	**Purpose:**	**Location:**	**Specs:**
RS-232	Connecting Routers	Communication Closet	20 Kbps
Cat6 Ethernet	Connecting PCs to Switches	Under Flour boards	Up to 1 Gbps
Cat6 Ethernet	Switch to Router connections	Communication Closet	Up to 1 Gbps
Cat6a Ethernet	Connecting server to Switch	Communication Closet	Up to 10 Gbps
Single-Mode Fiber	Long distance to ISP connection	Building WAN	Up to 10 Gbps
Power Cables	Providing power to devices	All Environments	Unique by device

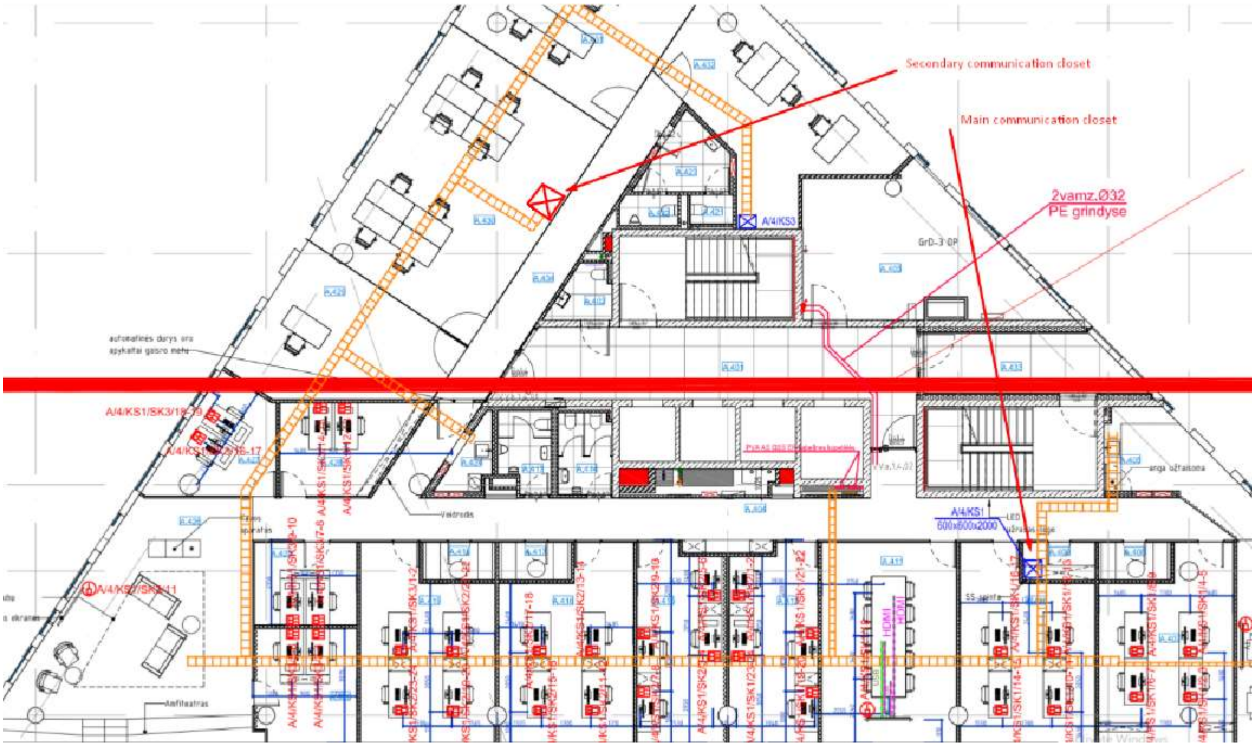


Figure 16 Representation of companys building flor plan.

These are all the physical component that make the updated network infrastructure.

4.5 Updated security measures:

After the update to network infrastructure, key network configurations where changed. Following information is detailed information on the changes.

4.5.1 Network segmentation and isolation

VLAN segmentation

Updated VLAN’s will help with network access and control.

Table 24 New VLAN information

VLAN ID	Purpose	IP Range	Subnet Mask	Default Gateway
10	IT Wired	10.0.10.1 - 10.0.10.254	255.255.255.0	10.0.10.1

20	IT Wireless	10.0.20.1 - 10.0.20.254	255.255.255.0	10.0.20.1
30	Users	10.0.30.1 - 10.0.30.254	255.255.255.0	10.0.30.1
40	Server	10.0.40.1 - 10.0.40.254	255.255.255.0	10.0.40.1
50	Printer	10.0.50.1 - 10.0.50.254	255.255.255.0	10.0.50.1
60	VPN	10.0.60.1 - 10.0.60.254	255.255.255.0	10.0.60.1

VLAN 10 (IT Wired): This VLAN is dedicated to devices and users belonging to IT team that are connected to the infrastructure via cable. It isolates traffic from the rest of the network for security and accessibility purposes.

VLAN 20 (IT Wireless): Similar to VLAN 10, this VLAN is exclusive to IT users who use AP to connect to network, they have the same capability's but have limited access to specific parts of the network that they don't need.

VLAN 30 (Users): This VLAN helps limit access to critical infrastructure and to enhance security by only allowing the basic access for users work purposes.

VLAN 40 (Server): Server is placed in a separate VLAN to limit access to critical infrastructure and to enhance performance by reducing broadcast traffic to server interfaces.

VLAN 50 (Printer): Printer VLAN is made to isolate traffic and to manage access to resources.

VLAN 60 (VPN): VPN VLAN is made to isolate traffic from users that access the infrastructure remotely and to manage access to specific resources.

Each VLAN is associated with a specific subnet, providing logical IP segmentation that aligns with the VLAN structure, simplifying IP management and enhancing security by limiting the broadcast domain size.

Access Control Lists (ACLs)

Table 25 New ACL Information

Permit TCP and UDP from IT Wired VLAN (10.0.10.0/24) to All VLANs
Deny All Inbound Traffic from Other VLANs to IT Wired VLAN (10.0.10.0/24) Except for Responses to Established Connections
Permit TCP and UDP from IT Wireless VLAN (10.0.20.0/24) to Server VLAN (10.0.40.0/24) on Ports 80 (HTTP) and 443 (HTTPS)
Permit TCP and UDP from IT Wireless VLAN (10.0.20.0/24) to Printer VLAN (10.0.50.0/24) for Printing Services
Deny All Direct Traffic from IT Wireless VLAN (10.0.20.0/24) to IT Wired VLAN (10.0.10.0/24)
Permit Necessary Management Protocols (SSH Port 22) from IT Wired VLAN (10.0.10.0/24) to Server VLAN (10.0.40.0/24)
Permit traffic from Users VLAN (10.0.30.0/24) to Server (10.0.40.0/24) and Printer (10.0.50.0/24). Restrict all other access.
Deny All Non-Management Traffic from IT Wired VLAN (10.0.10.0/24) to Server VLAN (10.0.40.0/24)
Deny All Inbound Traffic from Other VLANs Not Explicitly Permitted
Permit TCP Port 9100 from IT Wired VLAN (10.0.10.0/24) to Printer VLAN (10.0.50.0/24) for Printing Services
Deny All Inbound Traffic from Other VLANs to Printer VLAN (10.0.50.0/24) Except from User and IT Wired VLANs
Permit Access from VPN VLAN (10.0.60.0/24) to Server VLAN (10.0.40.0/24)
Deny All Other Traffic from VPN VLAN (10.0.60.0/24) to Other VLANs

These ACLs ensure a secure, functional, and well-segregated network, enhancing both security and performance by precisely defining and restricting traffic flows based on operational needs and security best practices.

4.5.2 Firewalls:

Table 26 Updated Firewall information

Rule #	Source	Destination	Source Port	Destination Port	Protocol	Action
1	10.0.10.0/24	Any	Any	Any	Any	Allow
2	10.0.20.0/24	10.0.40.0/24	Any	80, 443	TCP	Allow
3	10.0.20.0/24	10.0.50.0/24	Any	9100	TCP	Allow
4	10.0.30.0/24	10.0.40.0/24	Any	80, 443	TCP	Allow
5	10.0.30.0/24	10.0.50.0/24	Any	9100	TCP	Allow
6	10.0.60.0/24	10.0.40.0/24	Any	Any	Any	Allow
7	Any	10.0.10.0/24	Any	Any	Any	Deny
8	Any	10.0.20.0/24	Any	Any	TCP	Deny
9	Any	10.0.30.0/24	Any	Any	TCP	Deny
10	Any	10.0.40.0/24	Any	Any	Any	Deny
11	Any	10.0.50.0/24	Any	Any	TCP	Deny
12	Any	10.0.60.0/24	Any	Any	Any	Deny

These updated rules are designed to:

Rule 1: Allows the IT Wired VLAN full access to any destination for monitoring and management purposes.

Rules 2 & 3: IT Wireless VLAN is allowed access to the Server VLAN for web services (HTTP/HTTPS) and to the Printer VLAN for printing services (TCP port 9100).

Rules 4 & 5: Users VLAN is granted access to the Server for web services and the Printer for printing, reflecting basic operational needs.

Rule 6: VPN VLAN is granted access only to the Server VLAN, securing remote access to essential services.

Rules 7 to 12: These deny rules ensure that unsolicited inbound traffic is blocked to the IT, IT Wireless, Users, Server, Printer, and VPN VLANs respectively, securing them against unauthorized external access.

This structured approach not only aligns with VLAN setup but also reinforces network's security by specifically tailoring access permissions and restrictions. This ensures compliance with best practices while supporting essential network functions and services.

4.5.3 Secure remote access:

To connect to companys infrastrcuture you will need a VPN. All user profiles are generated by IT team and setup using 3rd party app OpenVPN Connect, that allows users to connect to infrastructure.

Table 27 New VPN Information

Feature	Description
VPN Service Type	OpenVPN
VPN IP Range	10.0.60.0 - 10.0.60.255
Subnet Mask	255.255.255.0
Encryption	AES-256
Authentication	MFA (Multi-factor Authentication)
Protocol	TCP / UDP
Port	1194
Client Config	Profiles generated by IT.

4.6 Summary:

The modernized network infrastructure has been significantly enhanced to improve organizational performance and reliability through several strategic updates. The network topology has been adjusted to better support redundancy and seamless access throughout the network, effectively reducing potential failure points and optimizing data flow. Advanced techniques in network segmentation and isolation, including refined subnetting strategies, the implementation of VLANs, and meticulous configuration of ACLs, enhance security and manage traffic more efficiently. Updated firewall rules further secure the network against external threats, while a revamped secure remote access system ensures safe and reliable connectivity for remote users. These updates collectively create a more efficient network environment, resolving issues such as network congestion and inconsistent wireless access, thereby supporting the overall productivity and security of the organization. These improvements not only enhance the network's capabilities but also support the broader goals of the organization.

The following table represents the cost of the network modernization, from work done to resources used. The cost of maintenance of this network is not accounted for, since the company has its own IT staff who will look over the network fixing any issues that occur, and if there any plans of doing any more changes new project will be formed to achieve desired goals.

Table 28 Projects implementation cost.

No.	**Work Done**	**Worked Hours**	**Hourly Wage Euro/h**	**Total, Euro**
1.	Infrastructure Review	40	25	1000
2.	Solution Design	20	25	500
3.	Solution Implementation	30	25	750
4.	Testing	15	25	375
5.	Documentation	20	25	500
6.	User Training	10	25	250
			Grand Total, Euro:	3375

Table 29 Grand total for the project completion.

No.	**Service**	**Price, Euro**
1.	**Network resources**	**1977.8**

2.	**Project completion**	3375
3.	**Maintenance**	**0**
	Grand Total, Euro:	**5352**

5 Evaluation and discussion

The redesigned network adopts a hierarchical model with clearly defined core, distribution, and access layers, greatly enhancing performance by optimizing bandwidth distribution and routing efficiency. This structured approach allows for better implementation of security policies and more effective segregation of network segments containing sensitive information. As a result, the network offers more reliable connectivity and quicker access to resources, thereby boosting user productivity. In contrast, the previous design featured a less organized, flat network topology, which led to unnecessary traffic and bottlenecks. Additionally, the lack of proper segmentation made it challenging to consistently implement and enforce security measures, negatively impacting both reliability and user productivity.

Implementing a hierarchical network design introduces significant complexity, requiring meticulous configuration and continuous maintenance, which leads to higher initial costs and potential scalability challenges if not carefully planned. The complexity of the design complicates troubleshooting efforts, especially if network staff lack the necessary training. Future expansions might also encounter difficulties if scalability isn’t integrated into the initial design phase.

The transition to a hierarchical network model marks a significant advancement over the previous flat network topology, addressing many of its inefficiencies and security shortcomings. While new design introduces complexity and requires greater investment in terms of time and resources, the benefits - enhanced network performance, improved security, and better resource accessibility, that justify the initial challenges. It is crucial that future expansions and upgrades maintain this structured approach and that staff receive ongoing training to manage the sophisticated network effectively. As the organization continues to grow, adapting the network to accommodate new technologies and increased demand will be essential for sustaining high performance and productivity.

6 Conclusion

After an extensive theoretical exploration of network infrastructure concepts, we conducted a thorough assessment of our current network setup. This assessment was guided by a solid theoretical framework that helped clearly understand and document the nuances of the company’s network infrastructure, presenting these findings to ensure all users/readers have a full grasp of the existing systems and their limitations.

Our detailed analysis pinpointed two primary issues - network congestion and limited wireless access. Addressing these challenges, we embarked on a redesign of the network infrastructure to enhance redundancy and security. Utilizing simulation tools like Cisco Packet Tracer, we modeled the proposed network changes to visualize and plan the new configuration effectively. Additionally, we employed the "Ekahau" tool to generate wireless access heat maps, providing a clear visual representation of the improvements in wireless coverage. This approach not only helped in visualizing the enhancements but also in fine-tuning the deployment strategy to cover previously underserved areas.

We then meticulously configured the updated network elements based on our theoretical groundwork and practical findings. Following these updates, a concise summary and a detailed cost analysis were conducted, laying out the financial implications of the network modernization project. Finally, we evaluated the implemented upgrades, discussing potential trade-offs compared to the old infrastructure. This comprehensive process not only resolved key operational bottlenecks but also positioned us to leverage advanced network capabilities, ultimately leading to a more secure and efficient network environment that aligns with modern business needs and technological advancements.

Furthermore, this project contributes significantly to the field of computer network modernization. By integrating cutting-edge theoretical insights with practical application, we have developed a model that exemplifies best practices in network redesign. This project serves as a valuable case study for the industry, demonstrating effective strategies for overcoming common networking challenges and deploying new technologies. Our approach ensures that the network infrastructure is not only optimized for current needs but is also scalable and adaptable to future technological advancements, setting a new standard for network design and management in the process.

Building on the success of the current network modernization project, several avenues for future research and potential extensions could be explored to further enhance network capabilities and prepare for emerging technological trends.

Here are some suggestions that could be implemented later on:

Integration of Software-Defined Networking (SDN): Future research could focus on the integration of SDN to provide more agile and centrally managed networking solutions. SDN can significantly improve network flexibility and ease the management of network resources, allowing for dynamic provisioning and fine-grained network control.

Adoption of Network Function Virtualization (NFV): Investigating the deployment of NFV could provide insights into how virtualizing network functions as opposed to deploying traditional hardware devices could enhance scalability and reduce costs. NFV offers rapid deployment of new network services, which is crucial for adapting to changing business needs.

Enhanced Security Protocols: With cybersecurity threats evolving rapidly, further research into advanced security protocols and encryption methods would be vital. This could include the development of AI-driven security systems that predict and neutralize threats before they impact the network.

Quantum Networking: Looking into quantum networking and how it can be utilized for ultra-secure communications could set the stage for future-proofing the network against sophisticated cyber-attacks and ensuring privacy in data transmission.

Energy Efficiency: Researching more energy-efficient network systems would not only reduce operational costs but also contribute to sustainability goals.

Techniques could include optimizing server utilization and adopting energy-saving policies.

These research topics not only aim to extend the capabilities of the current network modernization project but also align with broader technological advancements, ensuring that the network remains resilient, secure, and capable of supporting future digital transformations.

7 References

Pedamkar, P. 2023. Types of Network Topology. Chapter 1, Key Highlights. Available at: https://www.educba.com/types-of-network-topology/ [Accessed 4 Jan 2024].

Cloudflare. 2024. What is a subnet? Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/ [Accessed 23 Jan 2024].

Gillis, A. S. 2023. Principle of least privilege - POLP. Available at: https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP [Accessed 26 Jan 2024].

Finland. 2024. Data protection. Available at: https://tietosuoja.fi/en/data-protection [Accessed 11 Mar 2024].

Emerald Publishing Limited. 2023. Does personal data protection matter for ISO 9001 certification and firm performance? Available at: https://www.emerald.com/insight/content/doi/10.1108/IJPPM-07-2022-0345/full/html [Accessed 6 Jan 2024].

GDPR. 2024. Encryption. Available at: https://gdpr-info.eu/issues/encryption/ [Accessed 6 Jan 2024].

Pedamkar, P. 2023. Screenshot of the Types of Network Topology. Available at: https://www.educba.com/types-of-network-topology/ [Accessed 4 Jan 2024].

BasuMallick, C. 2022. Screenshot of the Key Components of LAN Architecture. Available at: https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network [Accessed 6 Jan 2024].

IPCisco. 2018-2024. Screenshot of OSPF Shortest Path First Algorithm. Available at: https://ipcisco.com/lesson/ospf-cost-and-spf-algorithm/ [Accessed 11 Jan 2024].

Cloudflare. 2024. Screenshot of Subnet. Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/ [Accessed 23 Jan 2024].

Zafiriadi, C. 2024. Screenshot of IPv4 Classification. Available at: https://www.pubconcierge.com/blog/subnetting-101-free-ipv4-cheat-sheet [Accessed 23 Jan 2024].

Hewlett Packard Enterprise Development LP. 2016. Screenshot of ACL Representation. Available at: https://techhub.hpe.com/eginfolib/networking/docs/IMC/v7_3/5200-2890/content/469316870.htm [Accessed 27 Jan 2024].

Fortra LLC. 2024. Screenshot of Encryption Process. Available at: https://www.goanywhere.com/products/goanywhere-mft/encryption/open-pgp [Accessed 2 Feb 2024].

Dotcom-Monitor. 2024. Screenshot of Monitoring View. Available at: https://www.dotcom-monitor.com/ [Accessed 5 Feb 2024].

Network Component Specifications:

Netgear. n.d. Nighthawk XR500. Available at: https://www.netgear.com/support/product/xr500/#docs [Accessed 20 Feb 2024].

EdgeRouter 12. n.d. Available at: https://media.dustin.eu/media/d200001004272951/edgerouter-12-document.pdf [Accessed 20 Feb 2024].

MicroTik. n.d. Chateau LTE12. Available at: https://mikrotik.com/product/chateau_lte12#fndtn-specifications [Accessed 20 Feb 2024].

DELL. n.d. Networking X1052P. Available at: https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/Dell_Networking_X-Series_Spec_Sheet.pdf [Accessed 20 Feb 2024].

Lenovo. n.d. Think System SR250 Rack Server. Available at: https://pubs.lenovo.com/sr250/server_specifications [Accessed 20 Feb 2024].

Lenovo. n.d. ThinkPad T15 Gen 1. Available at: https://psref.lenovo.com/syspool/Sys/PDF/ThinkPad/ThinkPad_T15_Gen_1/ThinkPad_T15_Gen_1_Spec.PDF [Accessed 20 Feb 2024].

Lenovo. n.d. ThinkPad X1 Gen 10. Available at: https://psref.lenovo.com/syspool/Sys/PDF/ThinkPad/ThinkPad_X1_Carbon_Gen_10/ThinkPad_X1_Carbon_Gen_10_Spec.pdf [Accessed 20 Feb 2024].

ASUS. n.d. Intel NUC 11 Pro UCFF. Available at: https://www.asus.com/displays-desktops/nucs/nuc-kits/nuc-11-pro-kit/techspec/ [Accessed 20 Feb 2024].

List of Applications Used:

Cisco. n.d. Cisco Packet Tracer. Available at: https://www.netacad.com/courses/packet-tracer [Accessed 20 Mar 2024].

BlocksAndArrows. n.d. Available at: https://www.blocksandarrows.com/ [Accessed 20 Mar 2024].

Ekahau. n.d. Available at: https://www.ekahau.com/ [Accessed 20 Mar 2024].

List of Tables:

List of Figures: