Rytis Šakalys

PASSIVE OPTICAL ACCESS CYBER SECURITY PROJECT OF KAUNAS UNIVERSITY OF APPLIED SCIENCES ADMINISTRATIVE BUILDING

Bachelor’s thesis

Bachelor of Engineering

Information Technology

2023

XAMK

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Rytis Šakalys
Thesis title	Passive Optical Access Cyber Security Project of Kaunas University of Applied Sciences
Commissioned by	
Year	2023
Pages	49 pages, 1 page of appendices
Supervisor(s)	Matti Juutilainen

ABSTRACT

A cyber security project for passive optical access in the administrative building of Kaunas University of Applied Sciences has been presented, replacing copper networks with faster, more reliable and more efficient networks based on optical and wireless technologies, while strengthening the network's cyber security. Current technologies for data transmission over copper and optical interfaces were presented and compared with each other, as well as the strengths and weaknesses of these technologies. PON and GPON technologies and their operational features were reviewed. The basics of cyber security were presented. The design part of the project included an overview of the current situation, a conceptual network model, a scan of the target information system and an overview of the results achieved. The technical parameters of the passive optical network were calculated, cyber incident monitoring equipment was presented, network redundancy and reliability parameters were calculated. At the end of the design part, the optical network equipment was selected and deployed and wireless coverage schemes were presented in the brief. The experimental part of the project consisted of modelling the design of the passive optical network, carrying out tests and describing the necessary improvements. Finally, the work concluded with a presentation of the results (conclusions) of the whole project.

Keywords: fibre-optic, cybersecurity, networking, GPON

CONTENTS

1 INTRODUCTION

The final thesis presents the implementation of the passive optical access cyber security project organized at Kaunas University of Applied Sciences. This project will eliminate the weaknesses of copper-based networks and strengthen cybersecurity comprehensively. The project will provide users with an extremely fast, affordable and secure network based on fibre-optic interfaces.

Most of the equipment used for the implementation of the project is hardware - optical cables and their control terminals (OLT), optical signal splitters and cassettes, Wi-Fi 6 routers, ONU devices and more. In addition, software products will be used to enhance cyber security, such as NStalker - a web application security scanner. Cisco Packet Tracer will be used to simulate the design part.

The project will be operated from a stationary OLT station, which will allow separate control of the main data link and the backup link, allowing reconfiguration of the predefined signal level splitting parameters of the optical network, and thus also changing the reliability values.

The main objective of this thesis work is to perform a cyber security project of passive optical access in the administrative building of Kaunas University of Applied Sciences, which would include an analysis of the current state of cyber security, calculations of the technical parameters of the new network, and the design of a network reservation scheme.

2 ANALYTICAL PART

This part will focus on the presentation of optical and copper technologies, comparing them with each other and reviewing their operational characteristics, strengths and weaknesses. The analytical part of the project will finalize with a presentation of the concepts of cyber security and cyberspace and an introduction to the vulnerability scanning tool N-Stalker.

2.1 Current network topology

The majority of local area networks (LANs) are based on a common infrastructure of copper interfaces across the whole network area (Figure 1).

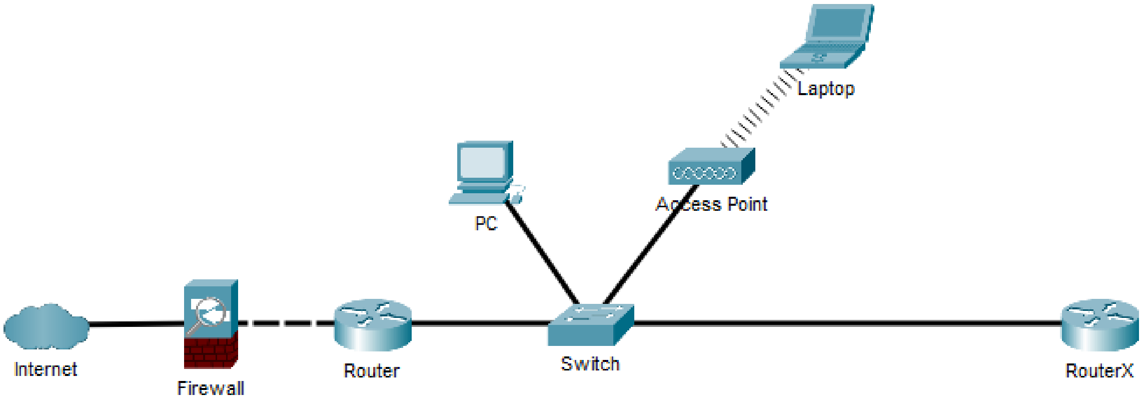


Figure 1 Conceptual model of the network

The most typical network model consists of routers, switches, access points, PCs and personal laptops brought in by students or instructors. The network has a default-gateway router (Router), as well as an outgoing and incoming packet filter - a firewall. Additional routers are used to eliminate signal attenuation. The entire infrastructure is connected to the Internet as an exit to the outside. The network uses Cat5 and Cat5e interfaces.

Networks that use Ethernet cables of Category 5 or lower are considered to be outdated. Today's computer networks use at least Category 6 interfaces, and more complex networks that wish to take advantage of the technological capabilities of modern copper cabling use Category 7 Ethernet interfaces.

A switch is a device that connects links or segments in a network. It forwards the received data packet exactly to the destination port. The port assigned to the destination port is selected based on the hardware address (MAC), which are stored in the address tables on the device.

A router is a network device that not only segments traffic, but also connects separate networks to become a peering device. The router reads the IP address of the destination of the packet and forwards the data to the proper subnet after selecting the appropriate route. A routing table is used to select the route. It is quite common practice that these devices are also used for exiting to the outside network.

Wireless access point is a device for connecting wireless devices to a network. Normally, this device is connected to another device on the network to which it forwards wireless signals (Mann, 2022).

A firewall is a separate network device that controls the communication of the network components behind it with the outside (the Internet). The device operates by applying predefined traffic rules that restrict traffic on the network (Cisco, n.d.).

End-user devices (PCs and laptops) are used to receive, process and provide management of request information on local and external networks. Typically, desktop computers are used by staff such as lecturers, assistants and other people delivering methodological material. Laptops are used by students.

2.2 Implementing LANs

The specifics of how the different interfaces - copper and optics - work and the different types of interfaces are presented separately in the following sections. Finally, the differences, strengths and weaknesses of these technologies are summarized.

2.2.1 Copper technology

The origins of this technology cannot be found in computer networks, but in the construction of telecommunications (telephone) lines. The introduction of copper lines in the second half of the 19th century had a significant impact on the development of copper computer networks, which eventually took over the main flow of information exchange from the wired telephone.

The working of copper cables is quite simple - the source network device (the sender) converts the transmitted information into an electrical signal, which reaches the destination device via electromagnetic waves, where it is decoded back to its original form. The purpose of data conversions is to form sets of bits (frames) according to a certain template that is recognized by both the sender (source) and the receiver (destination).

There are 2 groups of copper cables that are mostly used in networks (Figure 2):

- Twisted pair cable
- Coaxial cable

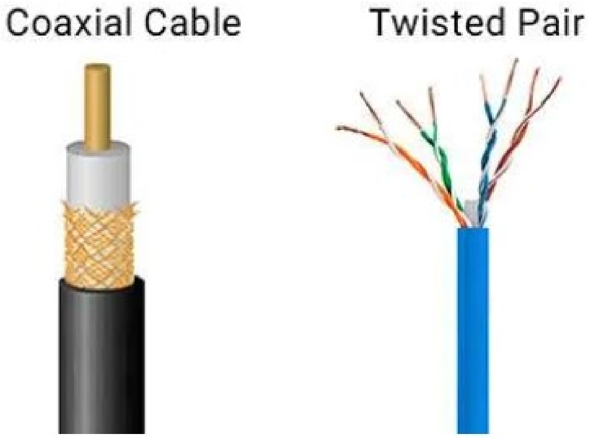


Figure 2 Copper cables

The concept of a twisted pair is that it is two copper wires twisted together, which reduces internal and external electrical interference and signal distortion.
The most commonly used types of twisted-pair cables are:

- Unshielded twisted pair (UTP) – the most common type of cable to be used, which is not surrounded by an anti-screening shield (Figure 3)

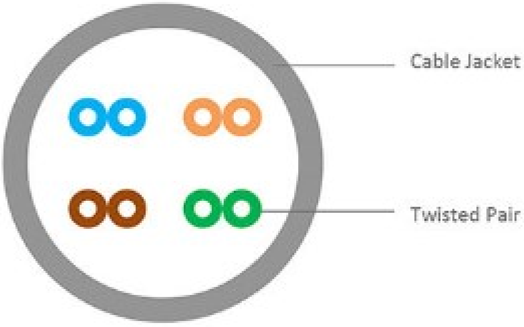


Figure 3 UTP cable positioning

- Shielded twisted pair (STP) – a type of cable that is surrounded by an anti-screening shield (Figure 4)

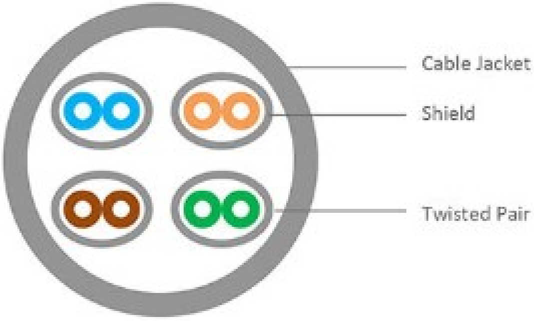


Figure 4 STP cable positioning

Ethernet cables are divided into categories. Cables are divided into these categories according to the specifications of their bandwidth, data rate and shielding. There are currently 8 known Ethernet cable groups (categories), but the focus here is on the Cat5-7 categories:

- Cat5/5e - Cat5 cable was introduced in 1995 and has a peak transmission speed of only up to 100 Mbps. It is particularly popular in FastEthernet networks as it can successfully transmit video and audio signals over distances of up to 100 metres. Cat5e - an enhanced version of Cat5, this version has much higher transfer rates (up to 1000 Mbps) due to the use of a larger number of twists which increases resistance to external noises

- Cat6/6a - cable introduced in 2000. This cable is technically similar to its predecessor Cat5e, but due to its improved shielding and bandwidth, this category of cable is capable of achieving speeds of up to 10 Gbps over short distances (up to 37 metres). 2009 augmented category 6 cable (Cat6a) with 500 MHz bandwidth launched

- Cat7/7a - was ratified in 2002. This category of cable is similar in its performance to Cat6a cable, but with a GG45 connector type and even better shielding protection. Cat7a cable can provide transfer rates of up to

40 Gbps over distances of 50 metres and up to 100 Gbps over distances of up to 15 metres.

2.2.2 Fibre optic technology

Like every innovative technology, the fibre optic transmission medium [environment] was invented to increase the speed and distance of data transmission, while reducing the amount of interfering information in the data packets - noise.

An optical fibre is a cable made of a highly transparent material (it is almost always glass) that carries light pulses. A certain number of optical fibres (e.g. - 24, 48, 96, 144...) in a single plastic polymer shell, with or without additional elements to give strength to the cable, is called a fibre optic cable. To compare the size of a single fibre, an adult human hair has a diameter of ~80 µm [micrometres], while the core of an optical fibre is only 8-100 µm without the top shell. Thus, the medium [environment] through which the information is transmitted is more than 8 times thinner than a human hair.

Currently, fibre optics are made from silicon oxide (SiO2), sometimes with the addition of impurities such as boron (B), titanium (Ti), germanium (Ge) or others. As mentioned earlier, a single optical fibre is made up of a core of 8-100 µm and covered with a polymer-protective layer (Figure 5).

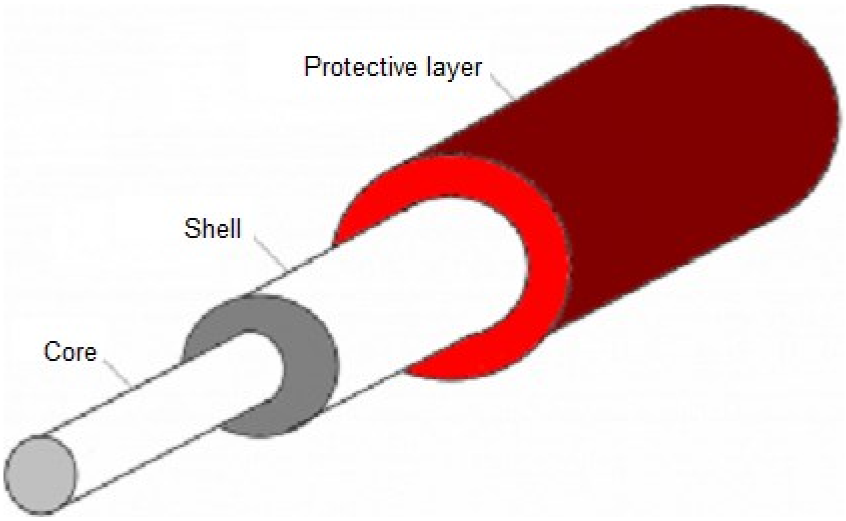
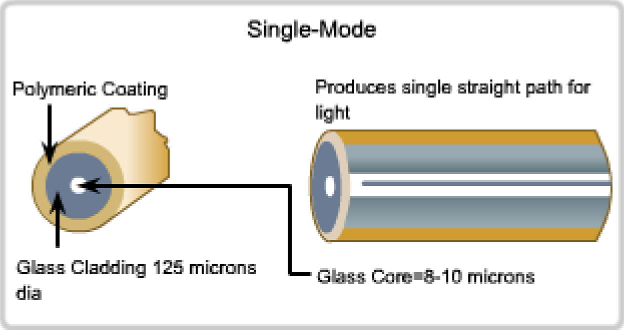


Figure 5 Optical cable structure

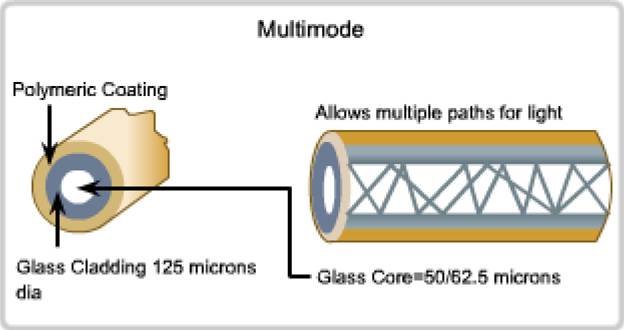
The two optical cables are the following:

- Single Mode Fiber (SMF) – This type of interface is used in long-distance optical networks. The cable has an effective coverage distance of up to 100 kilometres and a speed of 10 Gbps


Single-Mode
Polymeric Coating
Produces single straight path for light
Glass Cladding 125 microns dia
Glass Core=8-10 microns

  - SMF cable features:
    - Single colour light source
    - Small diameter core
    - Low dispersion
    - Light source – laser

- Multiple Mode Fiber (MMF) – Due to the small effective coverage distance (up to 10 kilometres), these interfaces are used in local networks. Data transfer rate - 100 Gbps


Multimode
Polymeric Coating
Allows multiple paths for light
Glass Cladding 125 microns dia
Glass Core=50/62.5 microns

  - MMF cable features:
    - Several rays of light
    - Larger diameter core
    - Higher dispersion
    - Light source - LED

The core and probably the most important hardware devices that maintain the efficient operation of an optical network:

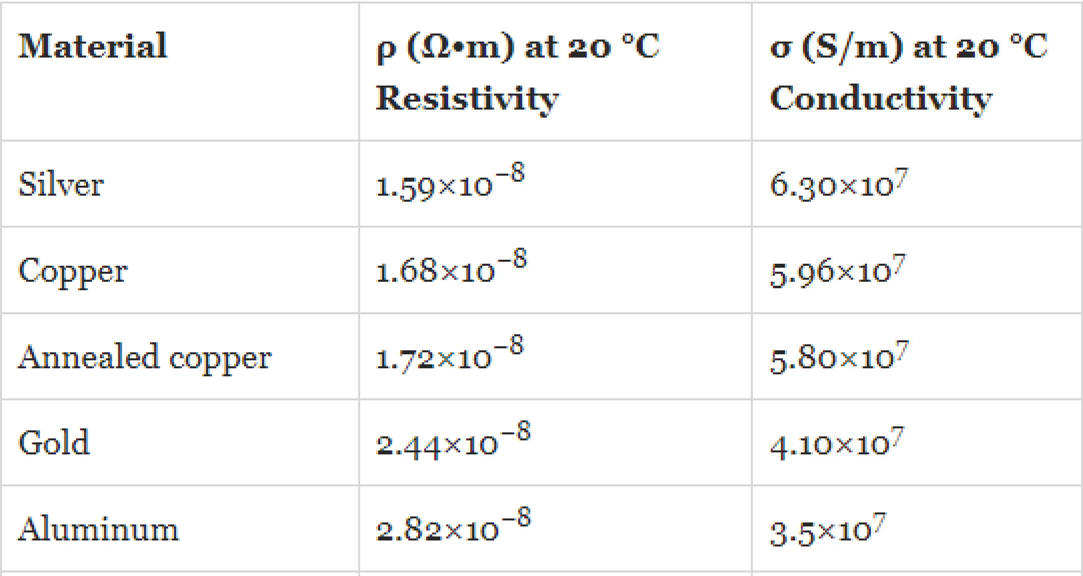
- Optical Line Terminal (OLT) – typically an optical network control station that belongs to an Internet Service Provider (ISP) and is responsible for managing, converting and controlling the optical signal processes in the network

- Small Form-factor Pluggable (SFP) – a small hot-swappable module designed to work on an OLT device. It is a direct optical cable connection to the management station, offering reliability and high-speed connectivity

- Optical Network Unit (ONU) – an endpoint device on the end-user side that operates as a modem but is dedicated specifically to optical networks

2.2.3 Advantages and drawbacks

One of the main reasons why copper is used for networking is its electrical conductivity - copper is the second most electrically conductive metal after silver as seen in Figure 6 (Helmenstine 2019). This helps the wire to handle higher electrical loads. Additionally, copper can offer a really low resistance to electric current - resistivity. These conductor properties make an important contribution to the quality of electrical signals transmitted in today's copper-based networks.



Material	ρ (Ω•m) at 20 °C Resistivity	σ (S/m) at 20 °C Conductivity
Silver	1.59×10^{-8}	6.30×10^{7}
Copper	1.68×10^{-8}	5.96×10^{7}
Annealed copper	1.72×10^{-8}	5.80×10^{7}
Gold	2.44×10^{-8}	4.10×10^{7}
Aluminum	2.82×10^{-8}	3.5×10^{7}

Figure 6 Resistivity and conductivity at 20°C (Source: thoughtco.com).

Another advantage of copper is that it has good heat resistance. This property prevents problems with overloading. Due to the combination of these properties, copper has good protection against rusting, although the conductor itself may become stained and dark in colour, but these external changes do not affect performance.

An important mechanical property of copper is flexibility. This allows the interfaces to be bent in different directions without any significant risk of damage, but it must be remembered that this property can also significantly limit the lifetime of the cable. Copper is also well known to a wide audience, being a conductor used since the second half of the 19th century and having well-known performance, properties and limits.

In addition to its solid advantages, copper as a conductor in networks also has some major drawbacks. The main disadvantage in networks that use copper cables is electromagnetic radiation, which can cause network equipment to malfunction. This problem results in interference to the electrical signal being transmitted and becomes a particular problem when the equipment on the network requires signal stability for the transmission of information, for example in telecommunications (Johnson 2018).

Due to a combination of technical and mechanical characteristics, copper interfaces cannot provide a high quality signal level over distances longer than 100 metres. In many cases, the transmitted information becomes distorted, the receiver does not get the full part of the transmitted information, and it cannot be further processed.

Moreover, the distortion of the transmitted signal creates a real need for additional network equipment on transmission lines to strengthen the signal and prevent distortion. The deployment of these additional devices increases the costs, as the investment is not only in new network equipment but also in the electricity it consumes.

There are also serious weaknesses on the cybersecurity side. Just recently, a cyber-attack that exploits technical weaknesses in UTP cables was presented at a conference in the U.S. The principle of the attack, named 'EtherOops', is that it manages to insert a malicious packet into the main packet being sent under the cover of external factors affecting the cable. This step helps the packet to "sneak through" and remain unnoticed by network security measures such as firewalls, NAT, IPS, etc. This attack is based on electrical interference and damaged, malfunctioning copper cables. When a cable is exposed to these causes, a network packet that sneaks in changes the bit layout inside, thus allowing its own structure to be disrupted and the malicious code to initiate its action. Although the effectiveness of this attack has so far only been tested in the laboratory (Vincent 2020).

Another major security disadvantage is that it is relatively easy to eavesdrop on copper-based packets transmitted over network interfaces. It is possible to gain access to network traffic, to see the IP addresses of the source, destination, connection details or even the content itself, if it is not encrypted. A wide range of software products allow such access, some of which are open source and completely free.

One of the main advantages of fibre optic cables is their extremely low signal attenuation. Compared to the most popular copper UTP cable used for internet transmission, the difference in attenuation is clear (Figure 7).

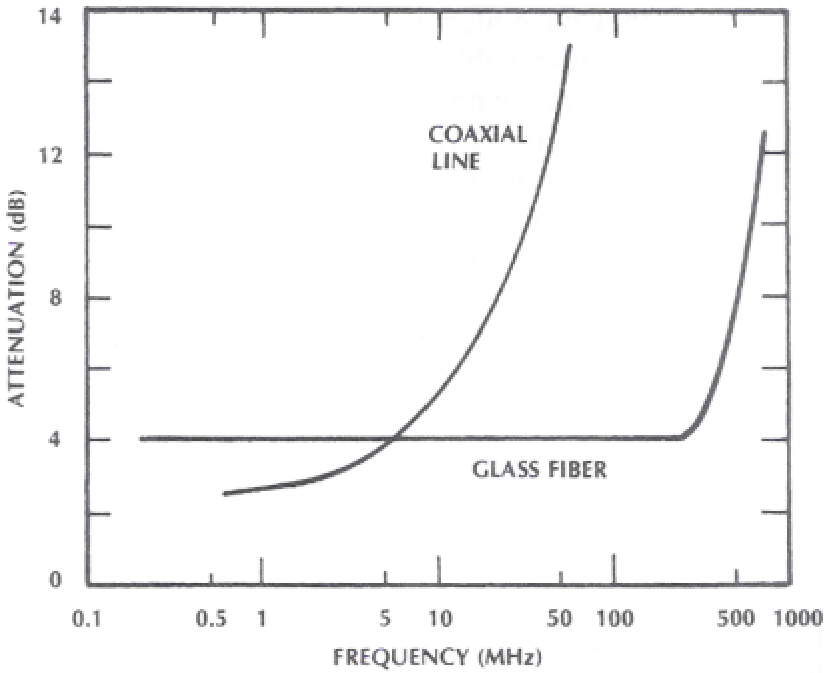


Figure 7 Attenuation of a 1 km length of coaxial cable and glass fiber cable (Source: ijtra.com).

The limit of a UTP cable that can still transmit data is about 100 metres. In contrast, there is no surprisingly strong signal attenuation when a standard fibre-optic cable is laid over a distance of 100 kilometres (Babani et al. 2014). Not to mention intercontinental fibre optic cables running thousands of kilometres along the seas and oceans. Fibre-optic cables are also resistant to external electromagnetic noise.

From a security point of view, optical interfaces are much more resistant to sniffing (eavesdropping) attacks compared to copper interfaces. The explanation for this feature is very simple: optical networks simply do not emit sound because, as mentioned earlier, they operate using light pulses rather than electromagnetic waves (Pascucci 2013).

Another key advantage of fibre-optic cables is the unexploited potential. It is estimated that the current fibre-optic cables should have a "working" life of 25-30 years. This will be enough time to ensure that fibre-optic cables do not become morally outdated. In current networks, the data transmission rate over the optical channel is not limited by the technical parameters of the fibre optic, but by the electronic circuits of the terminal equipment. Therefore, in order to increase transmission speeds, the back-end equipment will have to be replaced in the next 25-30 years.

It is also possible to increase the transmission rate by generating several or more signals of different wavelengths in a single optical fibre at the same time. This can increase the transmission rate by several times more, or make use of a single optical fibre by connecting several or a few dozen different terminals.
One of the most important advantages of optical technologies in the current context is their extremely good energy efficiency. The intermediate network devices do not require electricity, which keeps electricity costs extremely low
Another of the many advantages of fibre optic cables is the speed and stability of the connection. As already mentioned, today the transmission speed is not dependent on the fibre optic but on the electronic circuits of the terminal equipment.

However there are drawbacks in every place, and optical networks are not an exception. They are still relatively expensive and quite complicated to install and maintain. There are also disadvantages on the mechanical side - compared to copper cables, optical interfaces are much more vulnerable to tension and bending (Šimelis 2015).

2.3 PON and GPON technologies

A Passive Optical Network or **PON** (ITU-T G.983) is a network system that uses fibre optic cables to transmit light pulses to the end user, thereby providing broadband internet access. It is called passive because it operates within predefined parameters and works on a point-to-multi-point basis and, most importantly, the entire system operates with **electricity-free** network traffic splitters.

This system is distinguished by the mobility of the service, as the connection can be provided to the user's preferred destination, which can vary (Figure 8):

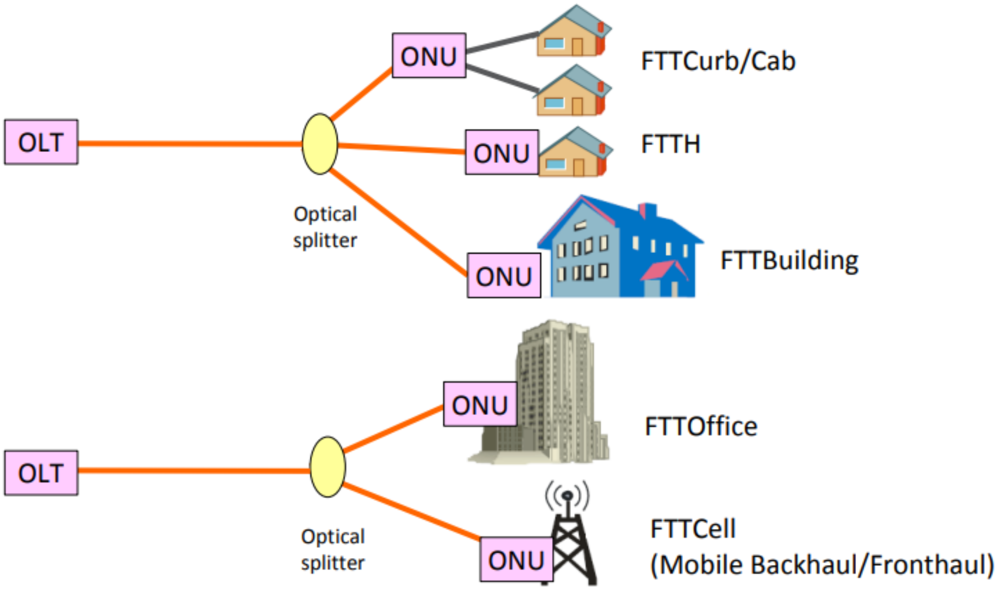


Figure 8 Application areas of PON

- Fiber-to-the-building (FTTB)
- Fiber-to-the-curb (FTTC)
- Fiber-to-the-home (FTTH)
- Fiber-to-the-premise (FTTP)

Coarse wavelength division multiplexing, or **CWDM** (ITU-T G.694.2), is a technology that enables optical networks to transmit multiple light signals at different wavelengths over a single optical fibre strand. CWDM supports up to 18 simultaneous wavelength channels transmitted over a fibre strand. These channels are separated by approximately 20nm in the 1271-1611nm operating range (Optcore 2022).

GPON will be realised using both (PON and CWDM) technologies. Gigabit-capable passive optical access or **GPON** (ITU-T G.984.3) is a PON-based technology which, as its name indicates, is applicable to optical networks operating at higher data rates (bandwidth). This technology provides speeds of up to 2.488 Gbps upstream and up to 1.244 Gbps downstream. The technology is well suited for use in internal building networks, with good overall bandwidth and bandwidth efficiency due to the use of packets of variable length.

2.4 GPON in internal networks

Due to the high use of copper in indoor networks, network interfaces are characterised by poor network extensibility, with coverage distances of up to 100 metres without intermediate devices. To cover larger distances, network devices must be connected in a serial way. This is where the need for additional signal amplifiers at intermediate nodes becomes necessary. Network devices connected in serial are directly dependent on each other, not only for the replication of the transmitted signal, but also for electrical power supply glitches.

A GPON solution would eliminate these issues. Based on the advantages of optical technologies discussed earlier (2.2.3) and the approaches of PON and GPON technologies (2.3), it can be assumed that this would not only be an innovative, but also a long-life, extremely fast, secure and reliable optical network.

The implementation of optical technologies makes it easy to increase the reliability of computer networks through a circular network structure (Figure 9).

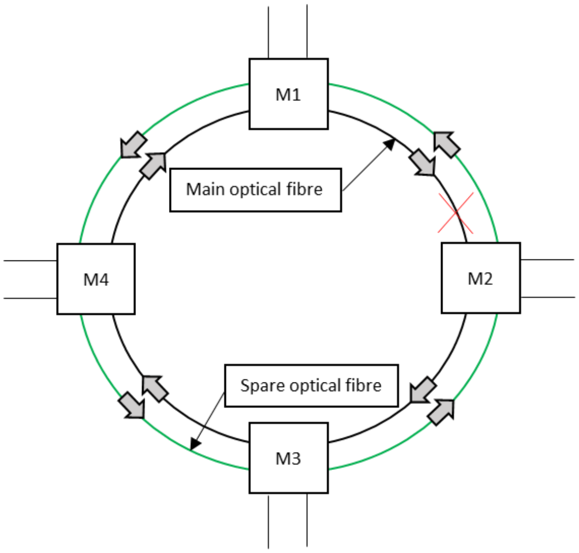


Figure 9 Circular network structure

A circular computer network scheme consists of interfaces that provide main and spare traffic, and intermediate control or traffic-sharing devices. Assume that the first device M1 manages the main fibre of the computer network, while the remaining intermediate nodes in the network may perform traffic-sharing functions. The management of the back-up network is the responsibility of the third device M3. The main traffic is carried in a clockwise direction and the backup traffic in a counterclockwise direction.

The ring uses two fibres to transmit and receive data. There is always a main bypass direction and a spare bypass direction in the ring. Suppose the direction M1=>M2=>M3=>M4 is the main direction and the opposite direction M1=>M4=>M3=>M2 is the backup direction. If the main direction is disrupted, the data transmission from node M1 to all other nodes is stopped, but the backup route remains and the data transmission is not stopped.

A building does not always have a corridor-based structure, which can make it very difficult to realize a circular network structure. In this case, a upstream network structure is proposed (Figure 10).

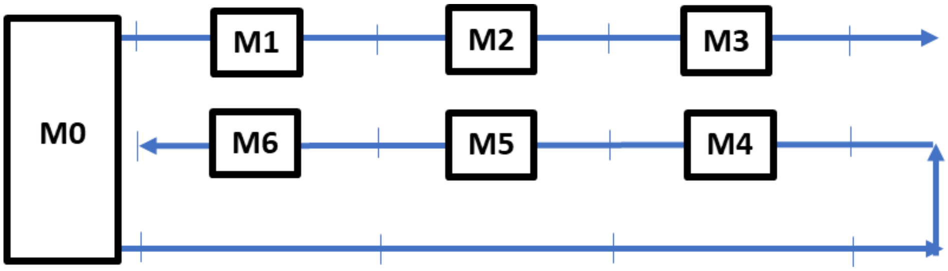


Figure 10 Structure of the upstream network

The main data stream is carried over first optical fibre. To ensure network availability, the upstream traffic must necessarily be carried on a separate (second) physical fibre. An additional (third) optical fibre is used to carry the starting traffic to the far end. It should be noted that the third optical fibre must be independent of the first two (Inovacijų taikymas technologijose 2022, 185-190).

The facilities in Kaunas University of Applied Sciences are arranged in a corridor-based structure, so a circular network configuration is suitable.

2.5 Wireless network technology

Wireless networks are computer networks that use wireless links to communicate between different devices on the network, i.e. they do not use twisted pair, fibre optic, or any other type of cable. Radio waves are used to transmit information between sender and receiver. The first data network was called ALOHAnet, which was developed in the second half of the 20th century.

The most popular standard for wireless local area networks is IEEE 802.11 - also known as Wi-Fi. The main function of the standard is to define the signal transmission methods for wireless local area networks at the physical OSI layer. The standard has 12 channels at 2.4GHz and 40 channels at 5GHz. The CSMA/CA method is used for data transmission, where each frame must be approved, otherwise a collision is assumed to have occurred (McClelland 2017).

The 802.11 standard has been updated more than a few times since its release, but the most recent versions are the following:

- 802.11n (Wi-Fi 4) – adopted in 2008, maximum speeds from 72 to 600 Mbps, operating at both 2.4Ghz and 5GHz

- 802.11ac (Wi-Fi 5) – adopted in 2014, maximum speeds from 433 to 6933 Mbps, works only at 5GHz

- **802.11ax (Wi-Fi 6/6E)** – adopted in 2019/2020, maximum speeds from 573 to 9608 Mbps, this version was available in 3 frequencies: 2.4GHz, 5GHz and 6Ghz (Wi-Fi 6E only)

- 802.11be (Wi-Fi 7) – expected release in 2024, maximum speeds from 1376 to 46120 Mbps, this version is expected to operate on 3 frequencies

2.6 Cybersecurity

Cybersecurity is a set of legal, organisational and technical information distribution measures designed to detect, analyse, respond to, prevent and, in the event of a cyber incident, to restore the normal operation of electronic communications networks, information or industrial process control systems. The development of information and communication technologies at the beginning of the 21st century has been followed by an increase in cyber incidents and unauthorized access to information systems to interrupt or modify the functioning of information systems, to destroy, damage, delete or alter electronic information, to restrict access to it, i.e. to appropriate, disclose, disseminate or otherwise exploit non-public electronic information to persons who do not have the legal right to access it.

Cyber security is particularly important for the information infrastructure - the electronic communications network, the industrial process control system, electricity grids, gas pipelines and other systems - the disruption of which would cause significant damage to the national security, the national economy, and the interests of the state and society. In 2016, NATO declared cyberspace as one of its operational areas (which means that the digital world is becoming as much a battlefield as land, water or air) (VLE, n.d.). The US Department of Defence defines cyberspace as one of five interconnected spaces. The other four are land, atmosphere, oceans and seas, and space (Cyberspace Operations, 2013)

Cyberspace is a constantly changing electromagnetic environment in which information is created, retrieved, stored, modified, removed, exchanged, used, shared, disseminated and physical resources are disturbed. Cyberspace covers the physical infrastructure, computer systems, networks of computer systems, networks of networks, access nodes, composite data. Cyberspace has individual (institutional), national and international dimensions.

N-Stalker is a widely used vulnerability scanning and web security assessment software product. It is capable of detecting current, future SQL injection, cross-site scripting (XSS) and other exploitable vulnerabilities**.** The key advantage of this software over its analogues is that the standard version allows users to view a vulnerability report, which provides solutions and other useful information, such as a description of why the vulnerability is a problem, how it could affect the system's performance, and what threats are being faced (Cogito, n.d.).

3 OPTICAL AND WIRELESS NETWORK DESIGN AND SECURITY

This part presents the design side of the final work. Floor plans, wiring diagrams, server scans, technical parameter calculations, cyber incident and analysis software, etc. This part ends with the selection of the equipment for the passive optical network.

3.1 Current situation of facilities layout

The building is divided into four floors. The classrooms on the first floor are quite tightly packed, with a majority of cramped classrooms that are used for lecturers' offices or their equipment (Figure 11). There is a lot of partitioning on this floor, so it can be assumed that the installation of the wireless devices would satisfy the demand and would cover the classrooms.

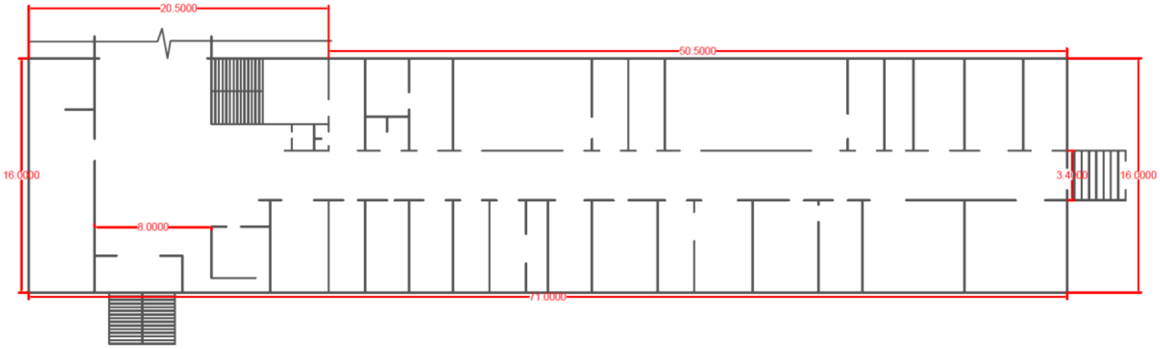


Figure 11 Layout of the first floor areas

The classrooms on the second floor of the building are larger than those on the first (Figure 12). The layout of the spaces on the second floor is similar to that on the third and fourth floors. It is expected that the network load on these floors may be significantly higher due to the number of student users in the rooms.

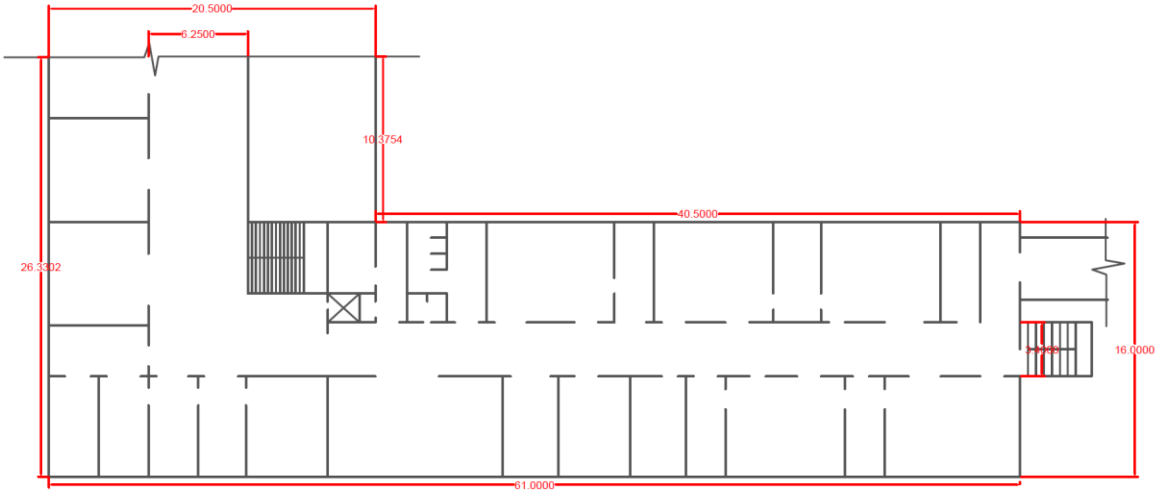
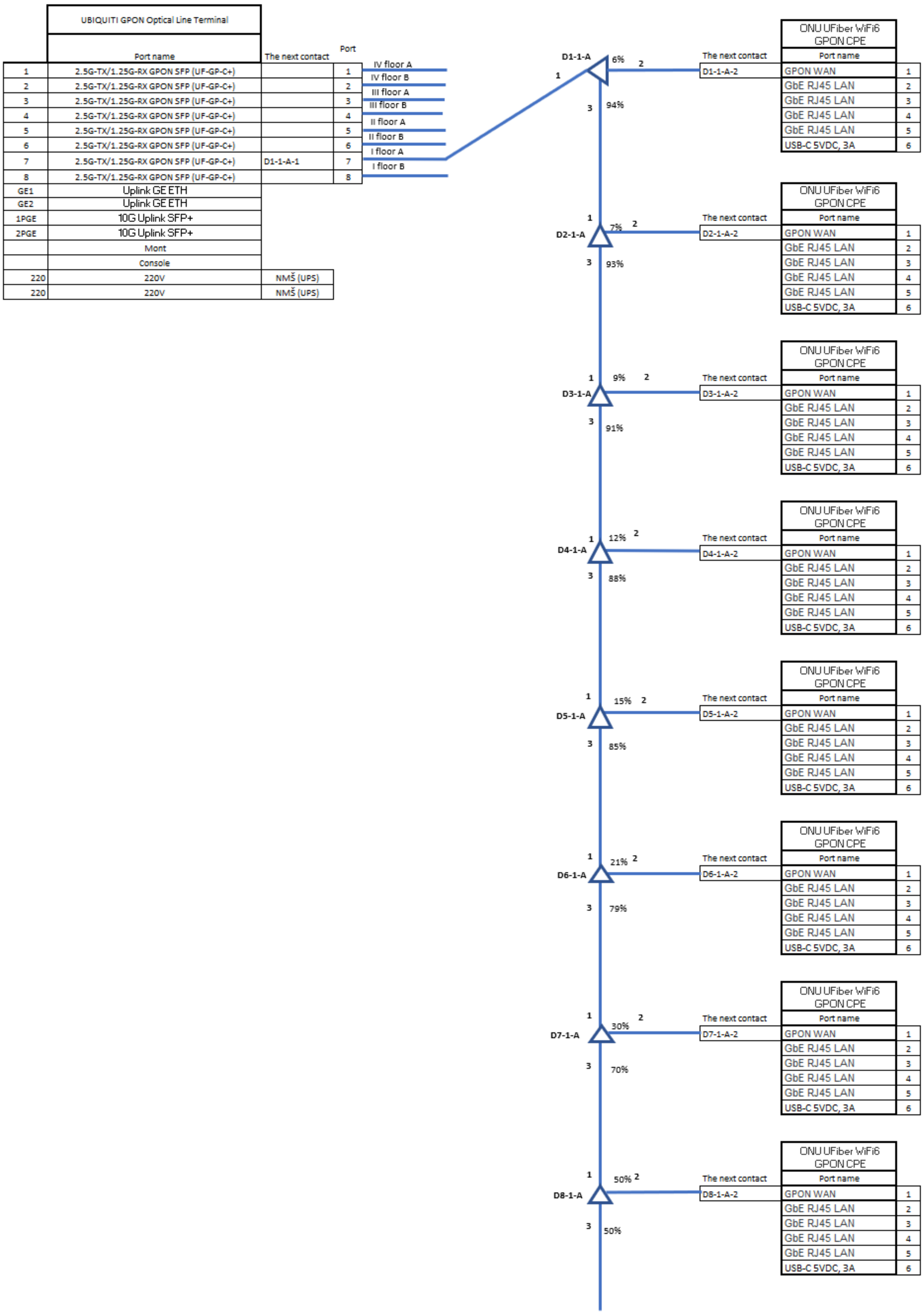


Figure 12 Layout of the second, third and fourth floors

In order to implement an effective, innovative passive optical access cybersecurity project, the layout of the premises could be the first aspect to be considered, which could have a significant impact not only on the result of the project as a whole, but also on its future development.

3.2 Developing a conceptual network model

The conceptual design of the optical network is carried out by designing the mounting scheme of the network (Figure 13). This scheme is based on the layout of the facilities (3.1).



	UBIQUITI GPON Optical Line Terminal		
	Port name	The next contact	Port
1	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		1
2	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		2
3	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		3
4	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		4
5	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		5
6	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		6
7	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)	D1-1-A-1	7
8	2.5G-TX/1.25G-RX GPON SFP (UF-GP-C+)		8
GE1	Uplink GE ETH		
GE2	Uplink GE ETH		
1PGE	10G Uplink SFP+		
2PGE	10G Uplink SFP+		
	Mont		
	Console		
220	220V	NMŠ (UPS)	
220	220V	NMŠ (UPS)	

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D1-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D2-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D3-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D4-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D5-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D6-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D7-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

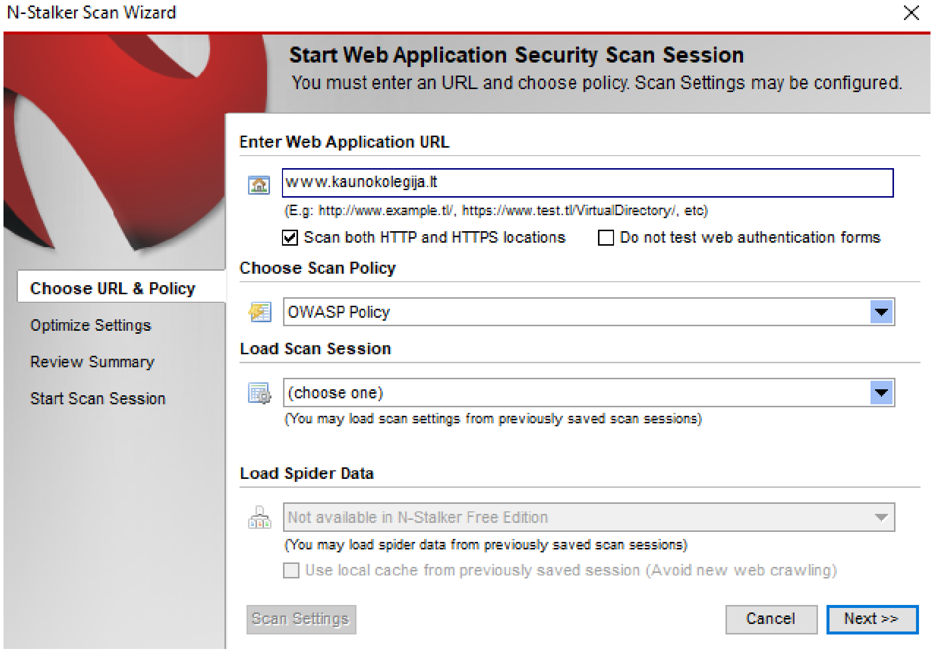
	ONU UFiber WiFi6 GPON CPE	
The next contact	Port name	
D8-1-A-2	GPON WAN	1
	GbE RJ45 LAN	2
	GbE RJ45 LAN	3
	GbE RJ45 LAN	4
	GbE RJ45 LAN	5
	USB-C 5VDC, 3A	6

Figure 13 GPON mounting scheme

The scheme starts with the main control unit of the entire optical network - the UBIQUITI GPON network router. The ports of this device are shown on the left side of the figure: 8 OLT optical lines, GE interfaces, inputs for uninterruptible power supply (UPS) connections. As the building has 4 active floors, the number of fibre optic lines in the control station (OLT) is ideal for designing not only the main traffic, but also the back-up traffic - this means 2 fibre optic lines are allocated per floor. The mounting diagrams for the second, third and fourth floors are similar in terms of connections and equipment quantities. The 8 network splitters (each labelled D1-1-A, D2-1-A, D3-1-A, etc.) in the network spread the signal over the whole network. The splitters divide the delivered traffic into different signal level ratios - 94:6, 93:7 etc. In this way, equal signal level attenuation for end-users is ensured across the network. The signal travels from the splitters to the UFiber GPON CPE Wi-Fi 6 wireless network routers via a GPON WAN port. These routers are the ones that can offer network access flexibility to end-users as they have 4 RJ-45 GigabitEthernet connections.

3.3 Information system vulnerability scanning

The identification of information system vulnerabilities starts with the selection of a scanning policy (Figure 14). The OWASP (Open Web Application Security Project) is used, which is based on the competences, observations and insights gathered by the software security community. This policy defines the most pressing vulnerabilities in today's systems of all types, some of which are: disclosure of sensitive data, inappropriate configuration of software protection, lack of more strict application of access controls, etc., so that the scope of system scanning and identification of vulnerabilities will be much wider. Since the target is the administrative building of the Kaunas University of Applied Sciences, the scanning target will be the college's main web address kaunokolegija.lt (IP 46.255.211.130).



Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Enter Web Application URL

www.kaunokolegija.lt

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

☑ Scan both HTTP and HTTPS locations ☐ Do not test web authentication forms

Choose Scan Policy

OWASP Policy

Load Scan Session

(choose one)

(You may load scan settings from previously saved scan sessions)

Load Spider Data

Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

☐ Use local cache from previously saved session (Avoid new web crawling)

Figure 14 Target and scan type selection

Once the tool has passed all intermediate scanning stages, the results are presented to the user. The results can be accessed either through the user interface or by generating an RTF or PDF report by the tool. The Executive Report also presents the results in a graphical model of charts, with graduated levels of vulnerabilities recorded - high-level vulnerability, medium-level vulnerability, low-level vulnerability, and preventive/informative level. It is recommended to choose stand-alone reports as they are not directly dependent on the software being installed on the operating system and provide much more detailed and comprehensive information. After the vulnerability scanning is completed, the results of the scans are presented (Figure 15).

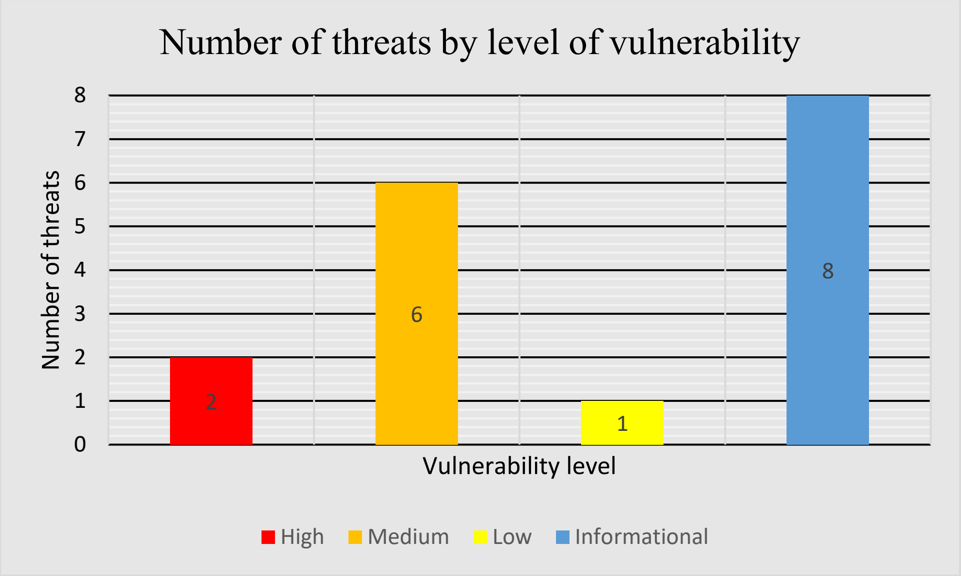


Figure 15 Vulnerability tool generated diagram

As the Figure 15 above shows, the potential threats identified present the current state of the system graphically, with 2 high-level, 6 medium-level, and 1 low-level vulnerabilities identified. The informational column included in the chart often defines inconsistencies in the system that do not have a significant impact on the system at the current time, but need to be corrected immediately for the overall prevention of information system security.

3.4 Calculating the technical parameters of a passive optical network

Optical signal splitters are used to calculate the technical parameters of a passive optical network. A scheme of 1:2 optical splitters, signal power losses and split losses nodes connected in series is presented (Figure 16). Symbols in the diagram are: E - optical line signal power losses, D1 - splitter number in the queue, C11 and C10 - signal attenuation of the splitter's branch optical line, 1 - branch line number.

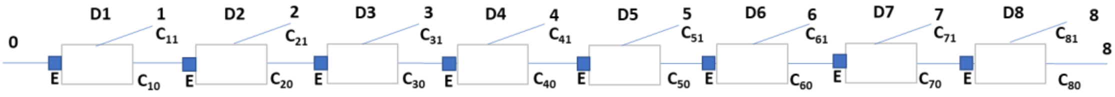


Figure 16 Splitters connected in series on an optical line

By calculating the values of the signal division coefficients of the optical splitters in advance, it is possible to match the signal attenuation measured at the outputs of the splitters (C11, C21, etc.). This can be done by means of signal power loss nodes placed before the splitters. The attenuation of the branch is equal to the total attenuation of the rest of the line, e.g. at output C11 the attenuation of the signal is equal to the total attenuation of D2-D8. Based on this methodology for calculating and comparing the signal attenuation, the attenuation data at the splitter branches of the entire optical line are measured (Table 1).

Table 1 Measured values at optical line nodes

Nodes	D1	D2	D3	D4	D5	D6	D7	D8
Signal attenuation, dB	12,94	12,94	12,94	12,94	12,94	12,94	12,94	12,94
Splitter division coefficient	94:6	93:7	91:9	88:12	85:15	79:21	70:30	50:50

The technical characteristics of optical splitters in an optical network vary. The outputs of the primary and intermediate splitters contain both optical and power lines (Figure 17). One of the splitter branch lines delivers traffic to the wireless stations (Output 2) and the other delivers traffic to the next splitter in the network (Output 3).

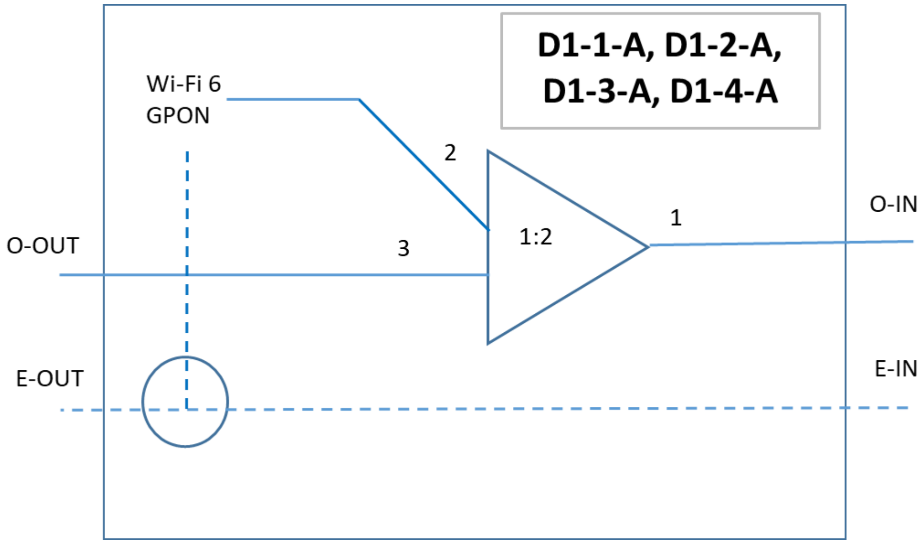


Figure 17 Scheme of the primary and intermediate splitter of an optical line

The final network splitter does not have these outputs due to no demand at the end of the line (Figure 18).

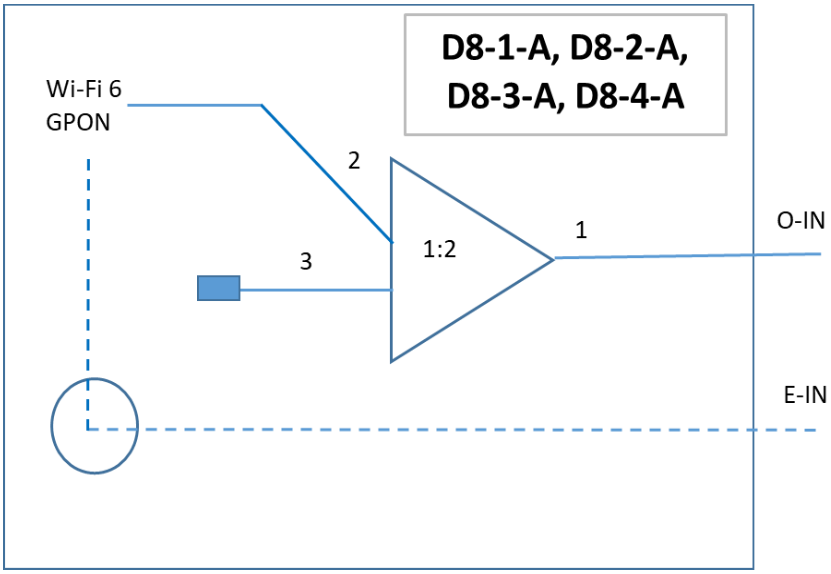


Figure 18 Scheme of the optical line end divider

An attenuator (Output 3) is placed on the branch line of the splitter to reduce reflections in the network.

3.5 Benchmarking of cyber incident monitoring and analysis software

The benchmarking of cyber incident monitoring and analysis software uses *SolarWinds*, *ManageEngine*, *Sumo Logic* and *Zabbix* products. Each of them will be evaluated according to their compliance with the set criteria and the weighting of the criteria will be determined by a scale of scores ranging from 1 to 10. The product specifications that meet the criteria set out and that have the highest weighting will be awarded the highest scores. Other less important criteria will be scored accordingly. At the end of the evaluation, one product with the highest score will be selected. The benchmarking analysis shows that the selected products clearly go hand in hand with each other (Table 2).

Table 2 Comparison of cyber incidents and analysis products

No.	Criterion to be evaluated	Criterion weight [1-10]	Names of compared products			
			SolarWinds SEM	ManageEngine	Sumo Logic	Zabbix
1.	Monitoring of incidents	10	10	10	10	10

2.	Personalisation of tasks	9	9	8	9	10
3.	Comprehensiveness of analysis	8	10	10	9	9
4.	User interface (UI)	7	8	9	9	7
5.	Support for regular updates	6	10	9	9	8
6.	Preparation of reports	5	10	10	8	9
7.	Availability of community support	4	9	10	8	9
8.	Open-source support	3	1	5	10	9
9.	Linux OS support	2	10	9	9	10
10.	Availability of simulation of situations	1	8	8	7	7
		Total:	494	500	497	494

Out of the maximum possible score of 550, the two lowest scoring cyber incident monitoring and analysis software products were *SolarWinds SEM* and *Zabbix*. *Sumo Logic* came 2nd overall with 497 points, while *ManageEngine*, which scored a few points more than the latter, came 1st.

Based on the results of the comparative analysis, *ManageEngine* is the software product that most closely meets the criteria for monitoring and analyzing cyber incidents.

3.6 Network reservation and calculation of reliability parameters

Reservation of the network and high reliability of the services provided are key to successful and efficient optical networks. A diagram of the network infrastructure interconnection is shown, which consists of the main and back-up network lines, with the red mark representing the main flow line and the green mark representing the back-up line (Figure 19). In this case, the back-up line contains hardware and software analogous to the main line, with the only node - the backup power supply - used to provide power to both sections in the event of a failure of the main power supply. The core task of the back-up line is to ensure the uninterrupted flow of data over the network.

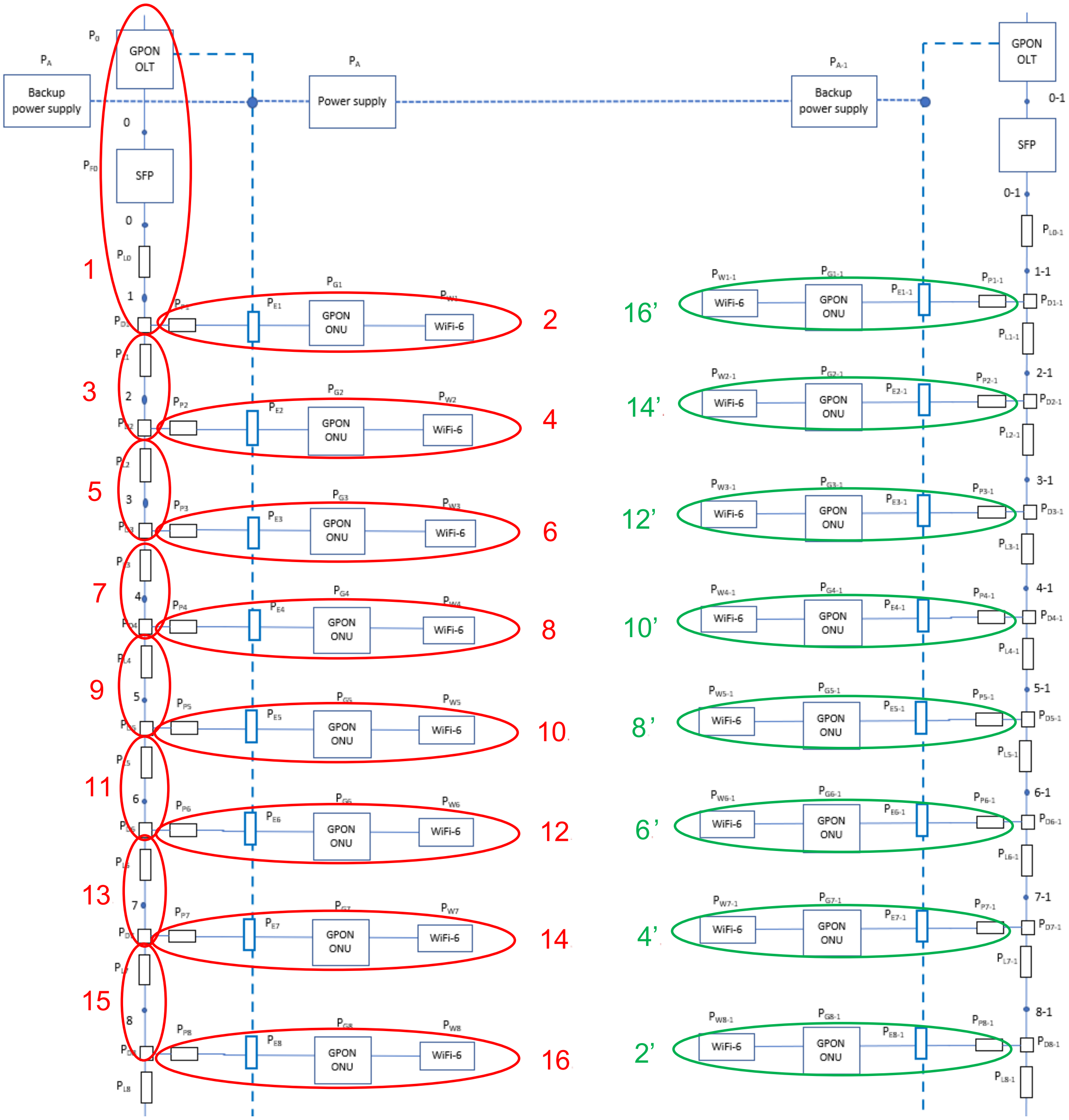


Figure 19 Network infrastructure connection scheme

The real reliability of intermediate devices in a passive optical network is expressed as a number less than 1 but very close to 1. For illustrative purposes and for ease of calculation, the reliability values for all nodes are unified and equated to 0,99. The reliability calculations for the sections of the network equipment marked with a red outline correspond to the numerical values of the outline markings. The formulas used for the calculations are set out in Appendix 1.

$$P1 = P_0 * P_{F0} * P_{L0} * P_{D1} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606; \quad (1)$$

$$P2 = P_{P1} * P_{E1} * P_{G1} * P_{W1} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606; \quad (2)$$

Hence, the total reliability of these two calculated network sections is equal:

$$P1{,}2 = P1 * P2 = 0{,}9606 * 0{,}9606 = 0{,}9228; \quad (3)$$

Based on the sequential calculation methodology, the following network sections are calculated.

$$P3 = P1 * P_{L1} * P_{D2} = 0{,}9606 * 0{,}99 * 0{,}99 = 0{,}9415;$$

$$P4 = P_{P2} * P_{E2} * P_{G2} * P_{W2} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

Based on the above calculations, it can be concluded that the reliability of the entire section is equal:

$$P3{,}4 = P3 * P4 = 0{,}9415 * 0{,}9606 = 0{,}9044;$$

Currently available calculations provide an overview of the reliability values at the back-end Wi-Fi 6 routers. Thus, a wireless device with a P_{W1} tag will achieve a reliability value of 0.9228. The P_{W2} tagged device has a reliability value of 0.9044. The reliability values will continue to decrease for serially connected devices.

$$P5 = P3 * P_{L2} * P_{D3} = 0{,}9415 * 0{,}99 * 0{,}99 = 0{,}9228;$$

$$P6 = P_{P3} * P_{E3} * P_{G3} * P_{W3} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

Overall reliability of the whole section is equal:

$$P5{,}6 = P5 * P6 = 0{,}9228 * 0{,}9606 = 0{,}8864;$$

The following sections of the network shown in the diagram are then calculated.

$$P7 = P5 * P_{L3} * P_{D4} = 0{,}9228 * 0{,}99 * 0{,}99 = 0{,}9044;$$

$$P8 = P_{P4} * P_{E4} * P_{G4} * P_{W4} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

$$P7{,}8 = P7 * P8 = 0{,}9044 * 0{,}9606 = 0{,}8688;$$

$$P9 = P7 * P_{L4} * P_{D5} = 0{,}9044 * 0{,}99 * 0{,}99 = 0{,}8864;$$

$$P10 = P_{P5} * P_{E5} * P_{G5} * P_{W5} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

$$P9{,}10 = P9 * P10 = 0{,}8864 * 0{,}9606 = 0{,}8515;$$

As mentioned earlier, the reliability values tend to fall with each step of the calculation.

$$P11 = P9 * P_{L5} * P_{D6} = 0{,}8864 * 0{,}99 * 0{,}99 = 0{,}8688;$$

$$P12 = P_{P6} * P_{E6} * P_{G6} * P_{W6} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

$$P11{,}12 = P11 * P12 = 0{,}8688 * 0{,}9606 = 0{,}8346;$$

$$P13 = P11 * P_{L6} * P_{D7} = 0{,}8688 * 0{,}99 * 0{,}99 = 0{,}8515;$$

$$P14 = P_{P7} * P_{E7} * P_{G7} * P_{W7} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

$$P13{,}14 = P13 * P14 = 0{,}8515 * 0{,}9606 = 0{,}8180;$$

$$P15 = P13 * P_{L7} * P_{D8} = 0{,}8515 * 0{,}99 * 0{,}99 = 0{,}8346;$$

$$P16 = P_{P8} * P_{E8} * P_{G8} * P_{W8} = 0{,}99 * 0{,}99 * 0{,}99 * 0{,}99 = 0{,}9606;$$

$$P15{,}16 = P15 * P16 = 0{,}8346 * 0{,}9606 = 0{,}8017;$$

The obvious decreasing trend in reliability values is illustrated graphically (Figure 20).

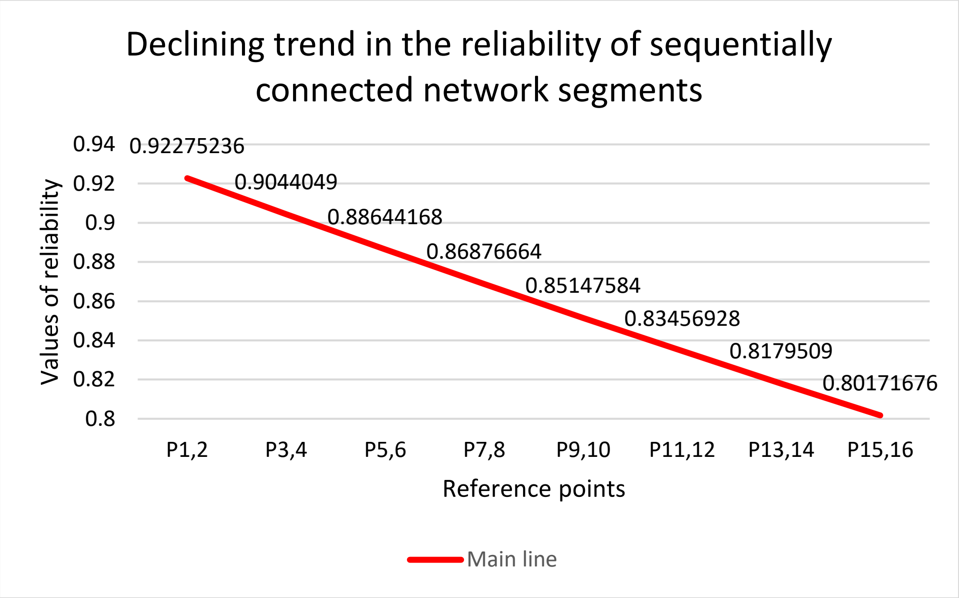


Figure 20 Decreasing reliability values of a series-connected main line

The situation changes dramatically when a reserve line appears, analogous to the main line. The sections of this line are marked with green outlines. The reliability values of the sections on the backup line are swapped due to the recalculation of the network signal split, a solution that provides a high level of reliability for devices that are already connected in parallel. The reliability values for the marked sections of the network remain the same, 16=16', 15=15', etc. The impact of the reserve line is shown down below.

$$P'1 = 1 - (1 - P1{,}2) * (1 - P15', 16') = 1 - (1 - 0{,}9228) * (1 - 0{,}7701) = 0{,}9823;$$

$$P'2 = 1 - (1 - P3{,}4) * (1 - P13', 14') = 1 - (1 - 0{,}8688) * (1 - 0{,}7858) = 0{,}9719;$$

$$P'3 = 1 - (1 - P5{,}6) * (1 - P11', 12') = 1 - (1 - 0{,}8515) * (1 - 0{,}8017) = 0{,}9706;$$

$$P'4 = 1 - (1 - P7{,}8) * (1 - P9', 10') = 1 - (1 - 0{,}8346) * (1 - 0{,}8180) = 0{,}97;$$

$$P'5 = 1 - (1 - P9{,}10) * (1 - P7', 8') = 1 - (1 - 0{,}8180) * (1 - 0{,}8346) = 0{,}97;$$

$$P'6 = 1 - (1 - P11{,}12) * (1 - P5', 6') = 1 - (1 - 0{,}8017) * (1 - 0{,}8515) = 0{,}9706;$$

$P'7 = 1 - (1 - P13{,}14) * (1 - P3', 4') = 1 - (1 - 0{,}7858) * (1 - 0{,}8688) = 0{,}9719;$

$P'8 = 1 - (1 - P15{,}16) * (1 - P1', 2') = 1 - (1 - 0{,}7701) * (1 - 0{,}9228) = 0{,}9823;$

To make it easier to understand the positive impact of the backup line on the reliability of the network, the final calculated data are presented graphically (Figure 21).

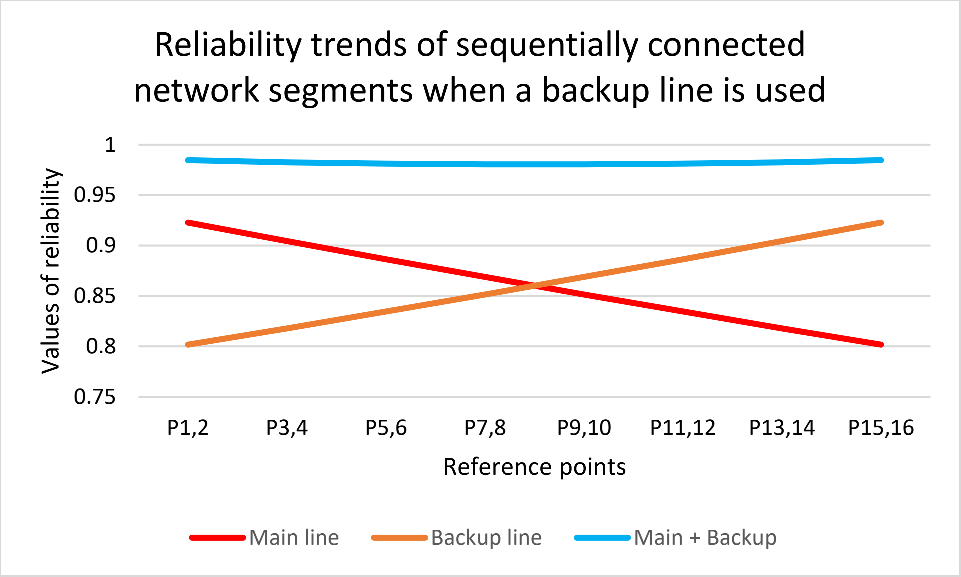


Figure 21 Interaction between main and back-up lines

It is safe to say that network reservation is crucial in the design and deployment of new networks supported by optical technologies.

3.7 Placement of equipment in the floor plan and creation coverage diagrams

Presents diagrams of the location of equipment on floor plans. End-user equipment - laptops - placed on the floor offer network access extensibility without tying end-users to a physical workspace. On the first floor there is a network-wide management station - the OLT unit (Figure 22).

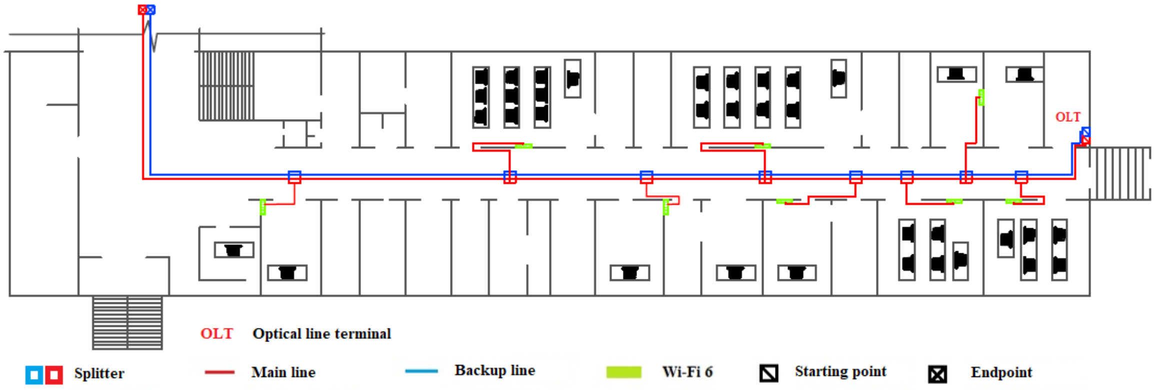


Figure 22 Layout of optical network equipment on the first floor

The *ExtremeNetworks* network hardware simulation and design tool is used to measure the wireless coverage in the target area. The features of the tool allow an accurate representation of the current situation in the building, with a choice of different structures that affect the attenuation of the signal: reinforced concrete structures attenuate by 12 dB, overlays between classrooms by 10 dB, narrow doors by up to 2 dB, etc.

The first floor coverage diagram consists of 8 Wi-Fi 6th generation devices supporting the proposed GPON network (Figure 23). The key objective in the coverage determination is to cover as many areas as possible, where the highest usage and traffic demand is expected. For premises that are only partially covered by wireless coverage and where potential interference may occur, *Ethernet* cables may be targeted.

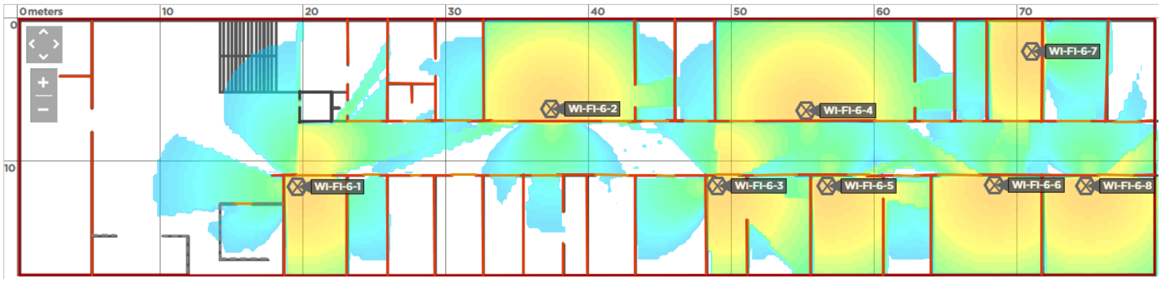


Figure 23 Diagram of wireless coverage on the first floor

The layout of the equipment on the second floor applies to the rest of the floors in the building (Figure 24). In the diagram, there are 8 units of Wi-Fi 6 devices, with

40 workstations dedicated to each of the floors, which are mobile, as on the first floor.

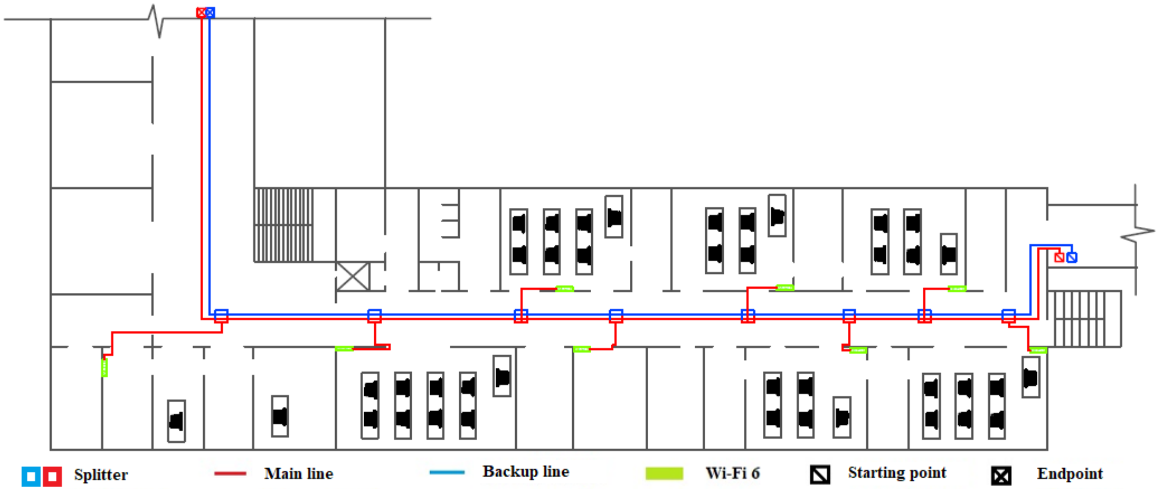


Figure 24 Layout of optical network equipment on the second floor and other floors

The second floor coverage diagram is also used to illustrate the coverage of the wireless signals on the third and fourth floors, using 8 Wi-Fi 6 devices on each floor (Figure 25).

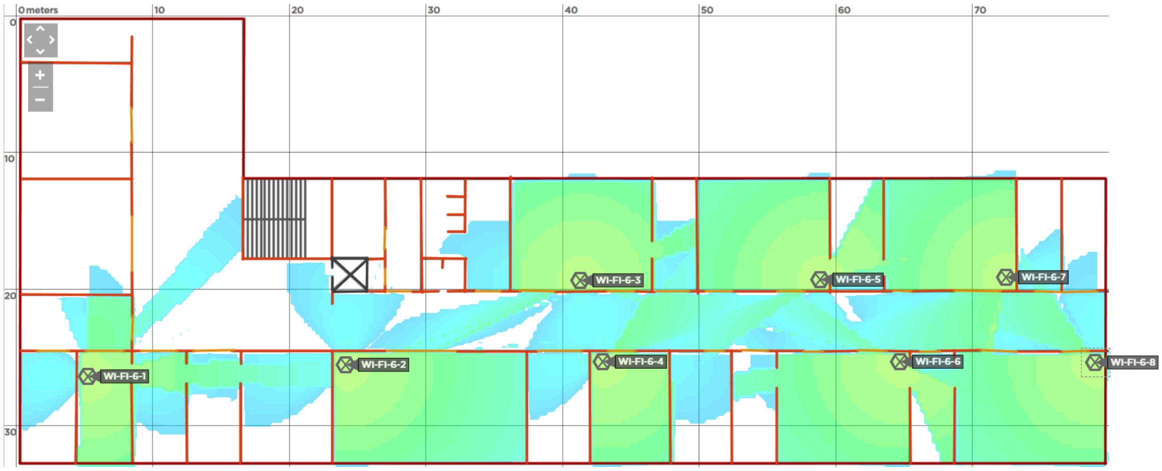


Figure 25 Wireless coverage diagram for the second and other floors

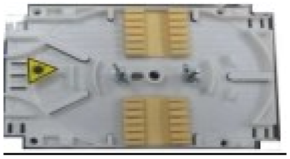
The signal strength colours shown in the coverage diagrams ensure that the most important auditoriums are covered.

3.8 Selection of network equipment

The selection of optical network equipment for the design part is presented in the form of a synopsis (Table 3). The most important information on the submitted network equipment is reviewed and structured, such as the name and purpose of the network device, the web link, the graphical image, the vendor and manufacturer.

Table 3 Passive optical network hardware

No.	Name, purpose	URL	Device appearance	Supplier, manufacturer
Passive optical access project hardware				
1	8x port GPON OLT with 2x SFP+ connectors, up to 2.488 Gbps for upload and 1.244 Gbps for download; Wavelengths: 1490 nm for upstream (TX), 1310 nm for downstream (RX).	https://www.katalita.lt/details/ubiquiti-gpon-optical-network-ufiber-olt.html		Supplier – Katalita Manufacturer - UBIQUITI
2	GPON OLT Class C+ SFP single-mode module, RX, TX wavelengths: 1310/1490nm, for interfaces up to 20 km. Upstream data rate: 1.25 Gbps; Downstream data rate: 2.5 Gbps; TX power range: 3-7 dBm; RX power range: -30 to -12 dBm.	https://www.katalita.lt/details/ubiquiti-gpon-olt-sfp-module-uf-gp-cplus.html		Supplier – Katalita Manufacturer - UBIQUITI
3	Wi-Fi 6 router (802.11ax support). 2402 Mbps at 5GHz, 574 Mbps at 2.4GHz; 4x GigabitEthernet ports, PON connection	https://store.ui.com/collections/operator-ufiber/products/ufiber-wifi6-gpon-cpe		Supplier – UBIQUITI Manufacturer – UBIQUITI
5	Optical cable (Single Mode) 2-fibre G.657A	https://pirk.zaliasis-namas.eu/Optin-kab-SM-2-skaid-AirFlow-S-QOTKSdD-2J-G-657A2.html		Supplier – tfk-telecom and „Žaliasis namas“ Manufacturer – tfk-telecom

6	1x2 optical traffic splitters 90:10, etc. PLC divider 1m with SC/UPC connector	https://pirk.zaliasis-namas.eu/lt/Optiniai-tinklai/Optiniai-dalikliai-spliteriai/PLC-splitter-10-90-1x2-SC-UPC-0-9mm-1m-Daliklis-PLC-1m-su-SC-UPC-jungt.html		Supplier – „Žaliasis namas"
7	Optical cassettes FOS12	https://pirk.zaliasis-namas.eu/lt/Optin-kaset-12-24-skaidul-virinimui-FOS12.html		Supplier – Fossfibreoptics and „Žaliasis namas" Manufacturer - Fossfibreoptics

The hardware components selected for the design of the passive optical access network are well suited for the real-life implementation of the project. The main network controller is able to support high data rates at different wavelengths (upstream ~2,5 Gbps, downstream ~1,3 Gbps), the SFP module keeps the signal strong even up to 20 km of physical interface length. The 802.11ax-capable Wi-Fi 6 router delivers wireless speeds of up to ~2,4 Gbps for upload and ~800 Mbps for download. This router has an additional 4 *GigabitEthernet* ports.

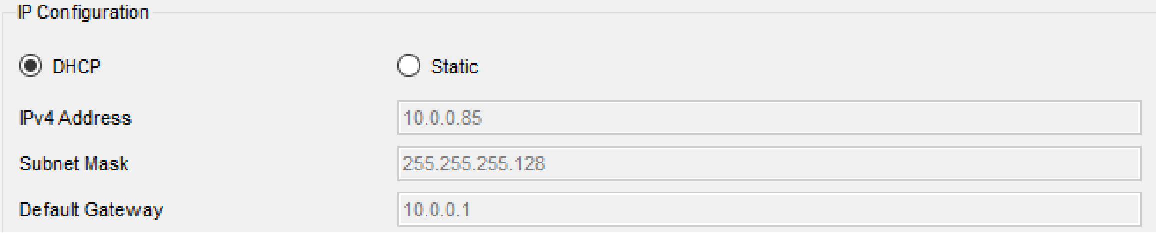
4 LOGICAL NETWORK DESIGN AND SIMULATION

This part of the thesis presents the practical side of the project - subnet addressing, simulation and testing of the new optical network in Cisco Packet Tracer environment, and also presents the necessary improvements.

4.1 Addressing subnets

Addressing of subnets to optical network devices is performed using the *Cisco Packet Tracer* tool. It was decided to assign subnets *10.0.0.0/25* and *10.0.0.128/25* to the local area networks of the first floor and *10.0.1.0/25* and *10.0.1.128/25* to the local area networks of the second floor, each containing 126 addresses for devices. The number of network devices indicates that most of the addresses assigned may not be used at the moment, but this is to ensure the secure expansion of network devices in the future. Automatic assignment of IP addresses and other parameters to end devices (*DHCP*) is enabled throughout the network, and the default gateway for the main first floor fibre optic line is the GPON OLT interface *GigabitEthernet0/0* address *10.0.0.1*. The default gateway for the first floor backup line for the *GigabitEthernet0/1* interface is *10.0.0.129*. For the second floor main line the default gateway is *10.0.1.1/25*, for the reserve line *10.0.1.129/25*. The ISP (in this case LITNET) reaches the optical line terminal (OLT) at *192.168.1.1/30*.

Assigning the network configuration to the end devices. First floor main line end device (Figure 26). First floor backup line end device (Figure 27). Second floor main line end device (Figure 28), and floor backup line end device (Figure 29).

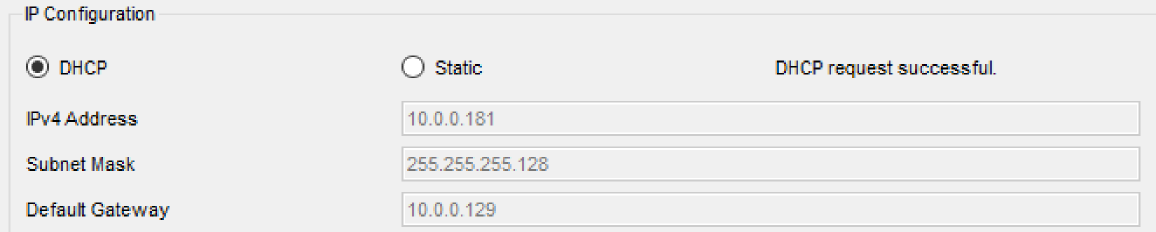


IP Configuration

● DHCP ○ Static

IPv4 Address	10.0.0.85
Subnet Mask	255.255.255.128
Default Gateway	10.0.0.1

Figure 26 Network information for the end-user network of the first floor main optical line

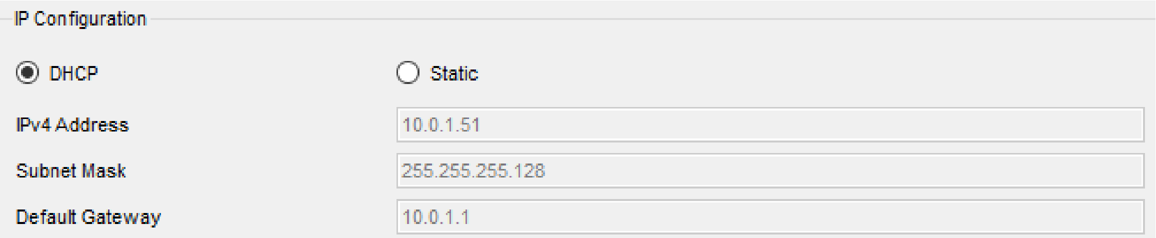


IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address	10.0.0.181
Subnet Mask	255.255.255.128
Default Gateway	10.0.0.129

Figure 27 Network information for the end-user network of the first floor backup optical line

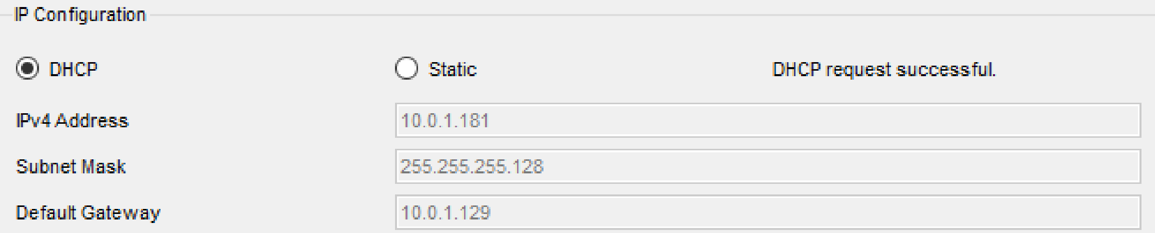


IP Configuration

● DHCP ○ Static

IPv4 Address	10.0.1.51
Subnet Mask	255.255.255.128
Default Gateway	10.0.1.1

Figure 28 Network information for the end-user network of the second floor main optical line



IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address	10.0.1.181
Subnet Mask	255.255.255.128
Default Gateway	10.0.1.129

Figure 29 Network information for the end-user network of the second floor backup optical line

4.2 Simulating a PON project in Cisco Packet Tracer environment

Cisco Packet Tracer software is used to simulate the optical network design (Appendix 1). Internet traffic reaches the building from the LITNET control centre at 10 Gbps. The network uses two lines - the main line and the backup line. As the main control unit has 8 SFP outputs, 2 outputs are allocated to each floor of the building. A simulation of the design of the passive optical network for the building floors is presented (Figure 30, Figure 31). From the network management station (UFiber GPON OLT), the optical signal from the main line travels through G.657A cables to intermediate signal splitters D1-1-A, D2-1-A, where D is the number of the splitter, and 1-A is the identifier of the floor. There, the signal flow is split according to predefined signal splitting parameters. From the splitters, the signal is transmitted to GPON Wi-Fi 6 CPE network routers that support 802.11ax. End-user equipment connects to the network via a wireless link, if necessary via a copper *Ethernet* cable.

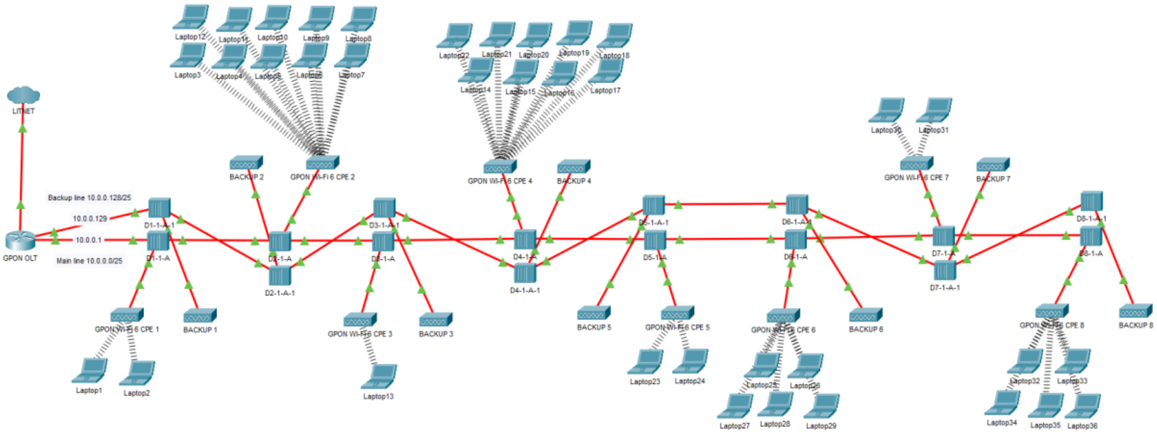


Figure 30 Scheme of a first floor optical network in a Cisco Packet Tracer environment

The *DHCP* service was used to assign network information to the devices on the first and second floors, which makes the administrator's job easier and automates the assignment process.

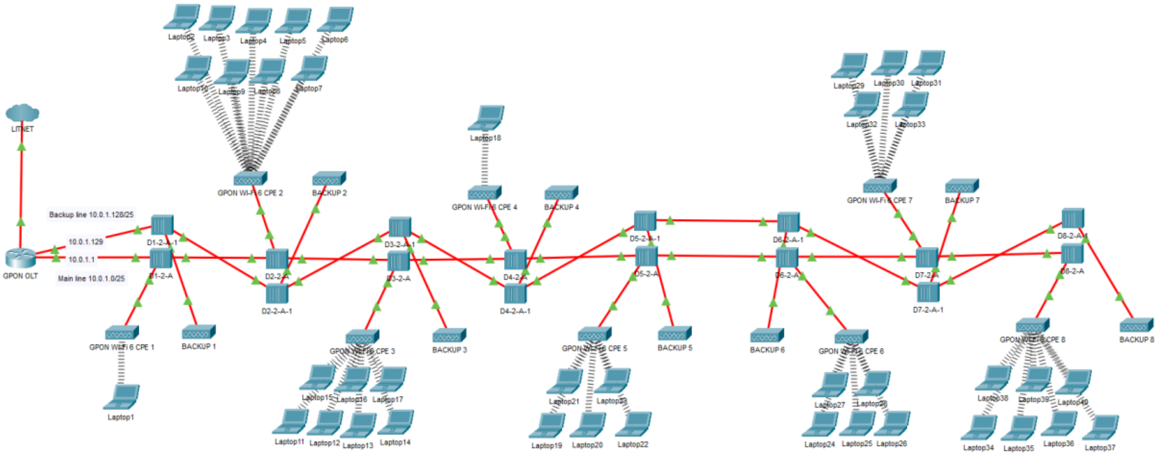


Figure 31 Scheme of a second floor optical network in a Cisco Packet Tracer environment

Excluded-address pools were excluded during the *DHCP* configuration, these addresses will not be assigned during automation. For the first floor this pool was *10.0.0.2* to *10.0.0.50* and *10.0.0.130* to *10.0.0.180*, for the second *10.0.1.2* to *10.0.1.50*, *10.0.1.130* to *10.0.1.180*.

4.3 Simulation testing and necessary improvements

Simulation testing starts with the first floor network scheme. In computer networks, the first test is usually to evaluate the reachability of devices by *ping* packets. This test is carried out between the network management station (OLT) and the furthest device Laptop36 (Figure 32). The packet path of the devices graphically looks as follows:

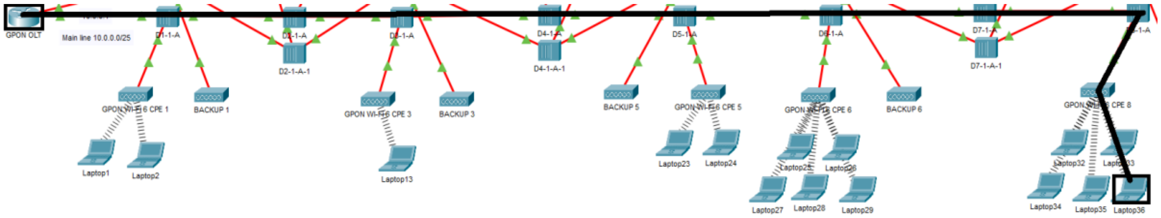
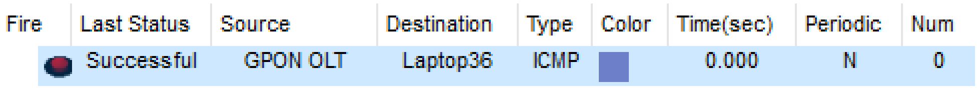


Figure 32 Testing the accessibility of first floor main line equipment

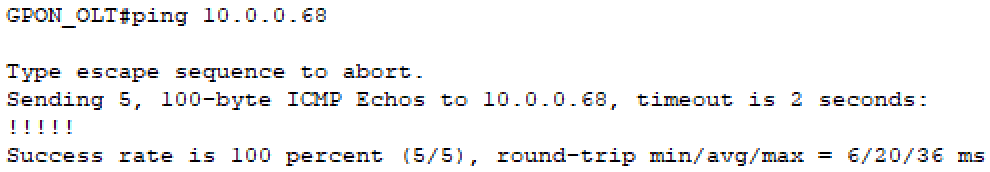
A PDU packet is sent from the GPON OLT to the target using the user interface (Figure 33). The result is successful.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	GPON OLT	Laptop36	ICMP	■	0.000	N	0

Figure 33 The result of testing the accessibility of first floor main line equipment in a graphical user interface

There is an alternative way to test the reachability of devices. The main network management unit allows testing to be carried out by specifying the target IP as *10.0.0.68* on the command line (Figure 34). The test result is again successful.



```
GPON_OLT#ping 10.0.0.68

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.68, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/20/36 ms
```

Figure 34 The result of testing the accessibility of first floor main line equipment in a command line interface

Simulation testing continues on the second floor scheme. The target is Laptop30 with IP address *10.0.1.57* (Figure 35). The packet flow in the scheme looks like this:

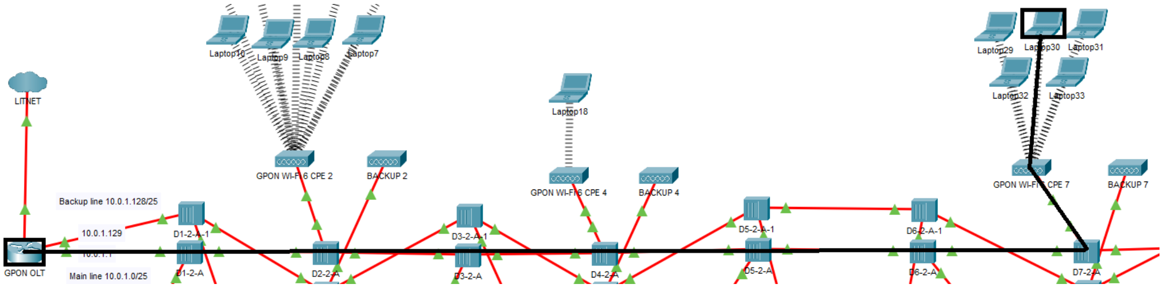
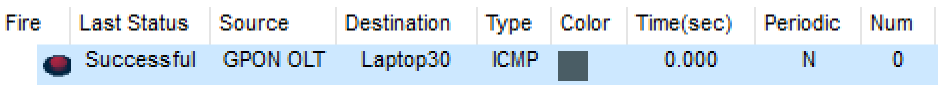


Figure 35 Testing the accessibility of second-floor main line equipment

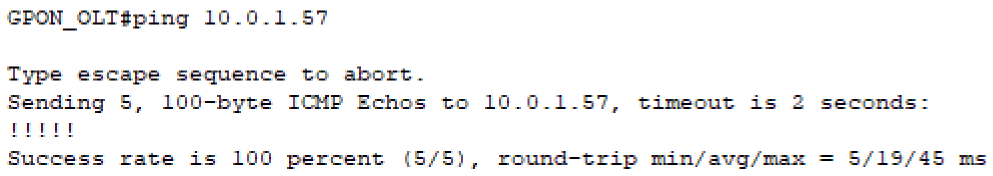
The result of PDU testing is successful (Figure 36):



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	GPON OLT	Laptop30	ICMP	■	0.000	N	0

Figure 36 The result of the accessibility testing of the second floor main line equipment in a graphical user interface

Testing via the network management station command line was also successful (Figure 37):



```
GPON_OLT#ping 10.0.1.57

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.57, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/19/45 ms
```

Figure 37 The result of testing the availability of second floor main line equipment in a command line interface

Floor schemes have backup optical signal and power lines that take over the movement of data through the network in the case of a failure of the main line. The end-user switches to the standby wireless router and is assigned network information on a different - standby - line subnet. The network access reservation for first floor end-users works as follows (Figure 38):

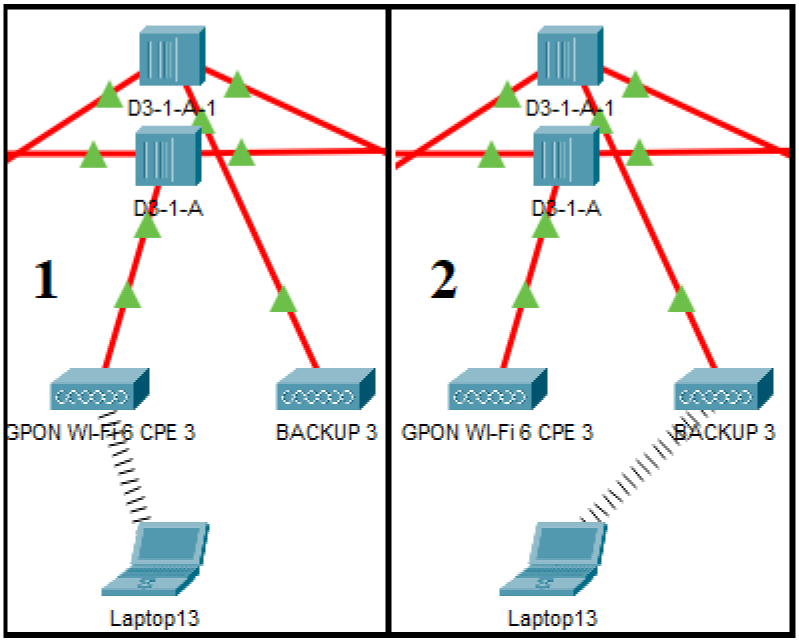


Figure 38 Reservation principle for end-user equipment on the first floor main line

The optical signal splitter D3-1-A (3 splitter on the first floor) on the main line, in situation one (1), sends a signal to the GPON Wi-Fi 6 CPE 3 router, which provides access to the end-user Laptop13. In case of failure of this line, the D3-1-A-1 optical signal splitter on the backup line takes over, so that a switch in the topology is seen, with the end-user access being provided by the BACKUP 3 router (2). In the case of different lines, different network information is assigned

(Figure 26, Figure 27). This reservation methodology is also used on other floors of the building.

5 CONCLUSIONS

The operation of copper cables and their technical characteristics were presented, which showed the need for the implementation of optical technologies in the study area. The lack of scalability and other characteristics of copper networks make it necessary to implement a fast, reliable and secure network solution based on optical technologies. GPON can be successfully implemented within in-building networks. The data rates provided by this technology are expected to be capable of handling the current demand.

Cyber security is becoming increasingly significant in today's world. The N-Stalker scan of an information system detected a range of threats with varying levels of vulnerability. It found 2 high-level vulnerabilities, 6 medium-level vulnerabilities, 1 low-level vulnerability and 8 information-related vulnerabilities. *ManageEngine* is the best performing software product for monitoring and analysis of cyber incidents. This product received the highest score (500) compared to *SolarWinds SEM* (494), *Zabbix* (494) and *Sumo Logic* (497).
A key feature of high-reliability optical networks is the availability of back-up network infrastructure. The lowest calculated reliability value for the interaction between the main and the back-up line is 0.97.

The chosen passive optical network design equipment is suitable for real-life deployment. Hardware for the passive optical network is shown on the floor plans. Wireless coverage diagrams are also included. Using *Cisco Packet Tracer* network simulation software, optical networks were designed, performance tests were carried out, and necessary improvements were described. The optical network diagrams for floors II, III and IV are identical.

The improvements needed for the PT schemes are based on the lack of customization of tasks/scenarios in the simulation tool, which is not able to work with optical technology solutions.
The version 8.1.0 in use does not have the optical splitter selection function, which results in the use of network *hubs*. However, they are not able to divide the optical signal proportionally according to the calculated splitting parameters. For

network routers or access-points, the hardware modules to be replaced do not follow the GPON G.984.3 standard, which makes it impossible to represent the relative flow rates, and the modules do not allow the simultaneous selection of optical and copper outputs. Laptop modules do not support Ethernet RJ-45 and Wi-Fi wireless connectivity at the same time.

For similar types of solutions, a different software product should be chosen (e.g. GNS3).

6 REFERENCES

Babani, S., Bature, A. A., Faruk, M. I., Dankadai, N. K. (2014). Comparative study between fiberoptic and copper in communication link. Available at: https://www.ijtra.com/view/comparative-study-between-fiber-optic-and-copper-in-communication-link.pdf?paper=comparative-study-between-fiber-optic-and-copper-in-communication-link.pdf [Accessed 02 Feb 2023]

Cogisoft. (n.d.). N-Stalker Web Application Security Scanner X. Available at: http://english.cogitosoft.com/html/product/item.aspx?id=860
[Accessed 05 Feb 2023]

CWDM Wavelength ITU Channels List: A Complete Guide. (2022). *OptCore.* Available at: https://www.optcore.net/article059/ [Accessed 07 Feb 2023]

Cyberspace Operations. (2013). Joint Publication 3-13 (R). Available at: https://web.archive.org/web/20180127164919/http:/www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf [Accessed 07 Feb 2023]

ExtremeCloud IQ. (n.d.). Project planner. Available at: https://extremecloudiq.com
[Accessed 06 Mar 2023]

Helmenstine, A. M. (2019). Table of Electrical Resistivity and Conductivity. Available at: https://www.thoughtco.com/table-of-electrical-resistivity-conductivity-608499 [Accessed 05 Feb 2023]

IEEE 802.11. (2023). Available at: https://en.wikipedia.org/wiki/IEEE_802.11
[Accessed 01 Feb 2023]

International Telecommunication Union [ITU]. (2016). G.652 Characteristics of a single-mode optical fibre and cable. (ITU-T, G.652). Available at: https://www.itu.int/ITUT/recommendations/rec.aspx?rec=13076&lang=en
[Accessed 02 Feb 2023]

Johnson, S. (2018). Copper Wire Advantages & Disadvantages. Available at: https://sciencing.com/copper-wire-advantages-disadvantages-8152803.html [Accessed 29 Jan 2023]

Mann, T. (2022). The Most Common Types of Network Devices. Available at: https://www.lepide.com/blog/the-most-common-types-of-network-devices/ [Accessed 30 Mar 2023]

McClelland, C. (2017). 8 Things You Didn't Know About Wifi. Available at: https://www.leverege.com/blogpost/how-does-wifi-work [Accessed 08 Feb 2023]

McVicker, D. (2014). 5 risks of copper cabling. Available at: https://www.fiberplex.com/blog/5-risks-of-copper-cabling.html [Accessed 11 Feb 2023]

N-Stalker. (2000). Web Application Security Scanner. Available at: https://www.nstalker.com [Accessed 13 Mar 2023]

Papiewski, J. (2017). Does Copper Explode? Available at: https://sciencing.com/copper-explode-16298.html [Accessed 06 Feb 2023]

Pascucci, M. (2013). Fiber optic networking: Assessing security risks. Available at: https://www.techtarget.com/searchsecurity/answer/Fiber-optic-networking-Assessing-security-risks [Accessed 07 Feb 2023]

Plėštys, R., Rimkus, D., Kavaliūnas, R., Lagzdinytė, I. and Sarafinienė, N. (2008). The security of computer networks. Available at: https://www.ebooks.ktu.lt/einfo/428/kompiuteriu-tinklu-sauga/ [Accessed 05 Feb 2023]

Science and Encyclopedia Publishing Centre. (n.d.). Cybersecurity. Available at: https://www.vle.lt/straipsnis/kibernetinis-saugumas/ [Accessed 10 Feb 2023]

Šakalys, R. (2022). Applying passive optical networking technologies in indoor building networks. In Grigonienė, G. Applying innovation in technology 2022. Kaunas, Kaunas University of Applied Sciences Advertising and Media Centre, 185-190. Available at: http://dspace.kaunokolegija.lt//handle/123456789/5757 [Accessed 06 Mar 2023]

Šimelis, R. (2015). Fibre optic - what is it? Available at: https://www.tinkluprojektavimas.lt/sviesolaidis-telekomunikacijos/ [Accessed 09 Feb 2023]

Venčkauskas, V. and Kazanavičius, E. (2011). The methods of information technologies security. Available at: http://www.esparama.lt/documents/10157/490675/Informaciniu_technologiju_saugos_metodai.pdf/046595c3-d8e8-4ddb-aebd-e5f69027a41e [Accessed 02 Feb 2023]

Vincent, M. (2020). Cyberattack risk detected in faulty unshielded Ethernet cables. Available at: https://www.cablinginstall.com/ip-security-av/article/14182112/cyberattack-risk-detected-in-faulty-unshielded-ethernet-cables [Accessed 10 Feb 2023]

What is a Firewall? (n.d.). Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html [Accessed 30 Mar 2023]

7 APPENDICES

Appendix 1

FORMULAS

$$P_x = P_{\mathrm{n}} * P_{Fn} * P_{L\mathrm{n}} * P_{D\mathrm{n}} \tag{1}$$

$$P_y = P_{P\mathrm{n}} * P_{E\mathrm{n}} * P_{G\mathrm{n}} * P_{W\mathrm{n}} \tag{2}$$

$$P_{x,y} = P_x * P_y \tag{3}$$

where	P_x	Probability of X	[-]
	P_{n}	Reliability of the OLT station	[-]
	P_{Fn}	Reliability of the SFP module	[-]
	$P_{L\mathrm{n}}$, $P_{P\mathrm{n}}$	Reliability of the splitter branch signal	[-]
	$P_{D\mathrm{n}}$	Reliability of the optical splitter	[-]
	P_y	Probability of Y	[-]
	$P_{E\mathrm{n}}$	Reliability of the power point	[-]
	$P_{G\mathrm{n}}$	Reliability of the ONU module	[-]
	$P_{W\mathrm{n}}$	Reliability of the WiFi-6 router	[-]
	$P_{x,y}$	Reliability of the X and Y link	[-]
	P_A	Reliability of the main/backup power supply	[-]