Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty of Computer Information System and Software Engineering
(full name of faculty)
Department of Computer Science
(full name of department)

QUALIFYING PAPER

For the degree of

Bachelor
(degree name)

topic: Analysis of means and methods of solving the "last mile" problem in computer networks

Submitted by: fourth year student _____ , group ICH-42
specialty 122 Computer science
(code and name of specialty)

	(signature)	Nikhil (surname and initials)
Supervisor	(signature)	Hotovych V.A. (surname and initials)
Standards verified by	(signature)	Matsiuk O.V. (surname and initials)
Head of Department	(signature)	Bodnarchuk I.O. (surname and initials)
Reviewer	(signature)	Stadnyk N.B. (surname and initials)

Ternopil
2023

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Faculty of Computer Information System and Software Engineering
(full name of faculty)

Department Department of Computer Science
(full name of department)

APPROVED BY
Head of Department
Bodnarchuk I.O.
(signature) (surname and initials)
« » 20___

ASSIGNMENT
for QUALIFYING PAPER

for the degree of Bachelor
(degree name)

specialty 122 Computer science
(code and name of the specialty)

student Nikhil
(surname, name, patronymic)

1. Paper topic Analysis of means and methods of solving the "last mile" problem in computer networks

Paper supervisor Hotovych V.A., PhD
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of «28» February 2023 № 4/7-233

2. Student's paper submission deadline 11.07.2023

3. Initial data for the paper Literature sources about architecture, principles of operation and development of computer networks.

4. Paper contents (list of issues to be developed)

Introduction, General Problem overview, operating modes, wireless networks.
Solving last mile for individual as well as corporative users of internet
Example of corporate computer network project, troubleshooting steps
Emergency safety & risk based approach
Occupational health & Hygienic classification of work
Overall conclusion

5. List of graphic material (with exact number of required drawings, slides)

6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
Occupational health	Okipnyy I.B.		
and emergency safety			

7. Date of receiving the assignment 28.02.2023

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	Analysis of the task for qualifying work. Selection	28.02.2023	*Completed*
	and work with literary sources.		
2	Writing chapter 1		*Completed*
3	Writing chapter 2		*Completed*
4	Writing chapter 3		*Completed*
5	Standartization control		*Completed*
6	Plagiarism check		*Completed*
7	Preliminary defense of qualifying paper		*Completed*
8	Defense of qualifying paper	11.07.2023	

Student ____________ Nikhil Chauhan
(signature) (surname and initials)

Paper supervisor ____________ Hotovych V.A.
(signature) (surname and initials)

ANNOTATION

Analysis of means and methods of solving the "last mile" problem in computer networks // Qualification work of the educational level "Bachelor" // Nikhil Chauhan // Ternopil' Ivan Puluj National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group ISN-42 // Ternopil, 2023 // P. 50, fig. – 11, tabl. – 6, chair. – , annexes – 2, references – 22.

Keywords: last mile problem, DOCSIS, xDSL, PON, wireless computer network, Wi-Fi, WiMAX.

The qualification work is dedicated to a full fledged study about last mile in telecommunications.

The goal of the work is to get familiar with every factor that is somehow connected with last mile.

The first section of the qualification paper considered the analysis of our task, some general definitions and introductions, some technologies related to last mile.

In the second section of the qualification work, it is considered to contain all the practical solutions which we described in first section with conclusions.

LIST OF ABBREVIATIONS AND TERMS

ADSL – Asymmetric Digital Subscriber Line;

BPL – Broadband Over Power Lines;

BSS – Basic Service Set;

IDF – Intermediate Distribution Facilities;

DCE – Data Channel Equipment;

DOCSIS – Data Over Cable Service Interface Specifications;

DCE – Data Channel Equipment;

DTE – Data Terminal Equipment;

LOM – Local Computing Network;

MAC – Media Access Control;

MDF – Main Distribution Facilities;

PON – PASSIVE OPTICAL NETWORK;

POP – Point of Presence;

Wi-Fi – Wireless Fidelity;

WiMAX – Worldwide Interoperability for Microwave Access.

CONTENTS

INTRODUCTION

The "last mile problem" in computer networks refers to the challenges associated with providing reliable and high-speed connectivity from the service provider's network to the end user's location. Resolving this problem often involves addressing issues related to infrastructure, technology, and service deployment. Here are a few approaches that can help solve the last mile problem [1-5]:

1. Fiber Optic Connectivity: Deploying fiber optic cables for the last mile connection can greatly enhance network performance and bandwidth. Fiber offers high-speed data transmission and can handle large volumes of data with low latency.

2. Wireless Technologies: Implementing wireless technologies such as Wi-Fi, fixed wireless, or cellular networks can be a viable solution, especially in areas where it's challenging to lay physical cables. Wireless connectivity can bridge the gap and provide access to remote or underserved areas.

3. Broadband Over Power Lines (BPL): BPL technology utilizes existing electrical power lines to deliver broadband internet access. This approach eliminates the need for extensive infrastructure deployment and can provide connectivity to areas already served by power grids.

4. Satellite Internet: Satellite internet services can provide connectivity to areas where terrestrial infrastructure is not available or cost-effective. Satellites in orbit transmit and receive data signals, allowing users to access the internet from almost anywhere on the planet.

5. Community Networks: Community-driven initiatives can play a significant role in resolving the last mile problem. These networks involve local communities or organizations building their own infrastructure and providing internet access to their members. This approach is particularly useful in areas where commercial providers have limited reach or interest.

6. Government Initiatives: Governments can implement policies and regulations that encourage investment in last mile infrastructure. Public-private partnerships or subsidies can incentivize service providers to extend their networks to underserved areas.

7. Mesh Networks: Mesh networks consist of interconnected nodes that cooperate to provide network access. Each node can communicate with multiple neighboring nodes, allowing data to hop from one node to another until it reaches its destination. This decentralized approach can improve connectivity in areas with limited infrastructure.

It's important to note that resolving the last mile problem requires a combination of approaches tailored to specific geographical, economic, and technological factors. The optimal solution for particular client may vary depending on the conditions and available resources.

The thesis's goal is to get a deep knowledge about last mile.

The following **problems are solved** in the work task to achieve this goal:

- Delivary problems
- Labour safety
- Risk to Individuals

The object of research is the process of developing a set of solutions to avoid last mile problems and individual safety.

The subject of research is the various factors affecting the last mile and also a threat to individual and labour safety.

CHAPTER 1. ANALYSIS OF THE PROBLEM, METHODS AND TECHNOLOGIES FOR ITS SOLUTION

1.1 General problem overview

The last mile is understood as the network segment from the user node or edge node of the local network to the first active node (Point of Presence, POP) of the telecommunications provider services [3 - 6].

The last mile describes the final stage of data transmission when it reaches network-connected devices in households or offices.

One of the main problems of the last mile is insufficient data transfer speed. Using older technologies, such as copper wires or wireless connections, can lead to limitations in data transfer speeds. This is especially true in large urban or congested areas where the number of users consuming large amounts of data may exceed the capacity of the infrastructure.

Another problem is the high cost of covering the last mile. Building new infrastructure, such as fiber optics or satellite connections, can be an expensive process. Especially in rural or remote areas where the population density is low, the costs of covering the last mile can be uneconomical for service providers.

The reliability of the connection is also a problem. Effects of adverse weather conditions, electrical interference, distance to broadcast towers or infrastructure damage can cause last-mile connectivity disruptions.

The last mile can also be a challenge for the development of new technologies. For example, the implementation of high-speed Internet, smart Internet of Things (IoT) networks or mobile applications requires powerful connections in the last mile.

Technologies of this class are used to solve the following tasks:

- connecting users or enterprise local networks to nodes telecommunications operators/providers to provide multi-service services: access to the Internet, cable (SATV) and IP (IPTV) television, video on demand (VoD), IP telephony (VoIP), etc.;

- connecting remote users or branches to the corporate network enterprises through intermediate data transmission networks;
- construction of corporate territorially distributed networks.

The following types of technology of this class can be distinguished.

- Modem connection:

a) modems for switched or dedicated telephone lines (speed transfers up to 64 Kb/s);

b) modems for physical lines (Short range modem), distance up to 18 km, transmission speed up to 738 Kb/s;

c) modems for connection to cable television networks (DOCSIS technology);

d) xDSL - modems (modems using technologies of digital subscriber line DSL).

- Passive optical networks (PON);
- Wireless technologies (Wi-Fi, Wi-MAX, satellite, microwave technologies).

The first two types of modem technologies are morally and physically obsolete and are no longer used nowadays. The most common last mile technologies are DOCSIS, xDSL and PON. Among wireless technologies, Wi-Fi technology is most often used to build general access networks.

1.2 Structure of the data transmission system

The data transmission system between nodes A and B has the following form (Fig. 1.1) [1, 7].

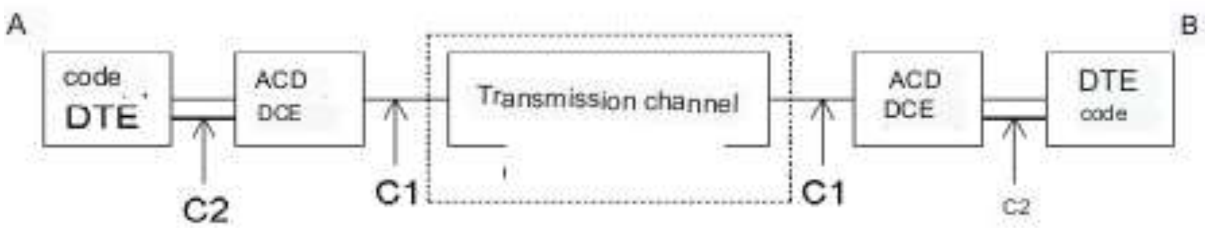

Figure 1.1 – The structure of the data transmission system

On the Fig. 1.1 we have: DTE – data terminal equipment; DCE data channel equipment; C1, 2 interface (joint); LOM – local computing network.

DTE – data terminal equipment – is the source or receiver of information. The DTE receives or transmits data over the transmission link using data link equipment (ACD or DCE). The main function of DCE is to provide the possibility of data transmission between two or more DTE devices on a channel of a certain type:

The interface between DCE and DTE devices is called the C2 interface. The interface between the DCE and the transmission channel is called the C1 junction. In the case of a local network, the RJ-45 connector acts as the C1 connector for connecting a network cable, the DCE device is a network adapter, the C2 connector is an RSI bus, and the DTE device is a personal computer. When connecting via modem technologies: CE device–modem, connector C1 – RJ-11(12) connector, connector C2 – port for connecting a modem (COM, USB).

In the case of connection to digital transmission channels, for example ISDN or E1 trunks, the DCE device is called a Data/Channel Service Unit (DSU/CSU).

The data service unit (DSU) performs physical encoding of signals received from the DTE, forms frames (for example, an E1 frame), performs synchronization functions.

The channel maintenance unit (CSU) is responsible for maintaining the necessary conditions for the transmission of electrical signals through the channel (channel testing procedures, restoration of the form of the electrical signal, presentation of the electrical signal in the entire band of the frequency channel). Typically, a DSU/CSU is implemented as a single hardware device.

Let's consider the technologies for solving the problem in more detail.

1.3 DOCSIS technology

Data Over Cable Service Interface Specifications (DOCSIS) specifies the medium access control (MAC) layer and the physical layer for high-speed data transmission over a hybrid optical-coaxial (Hybrid Fiber Coax - HFC) cable network used in cable television systems [8, 9]. In fig. 1.2 shows a typical network structure that uses DOCSIS technology.

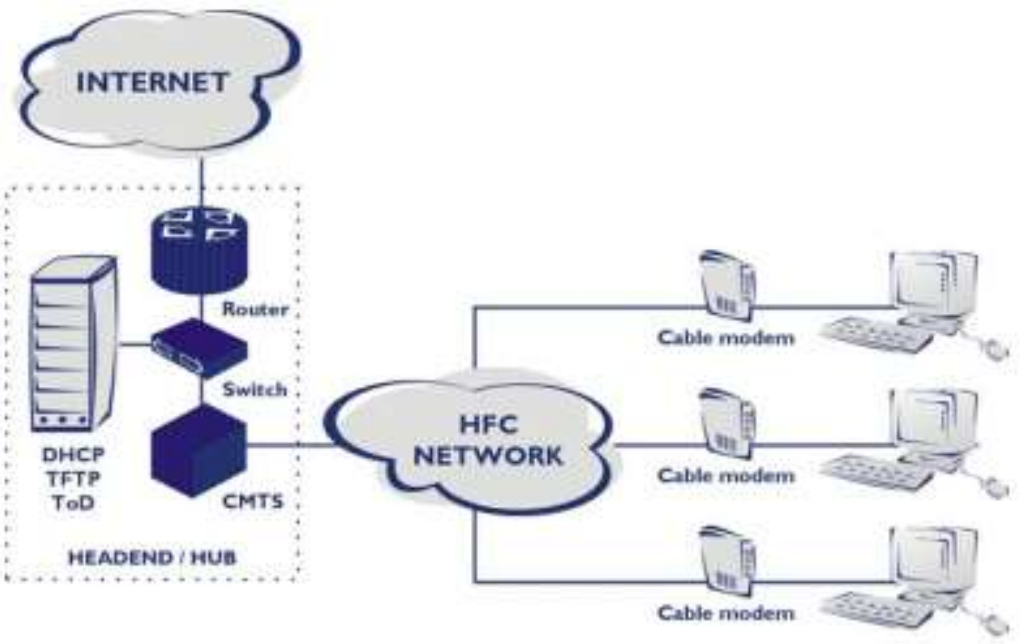

Figure 1.2 – The typical structure of DOCSIS network

The operator's main equipment, which is called a cable modem termination system (Cable Modem Termination System CMTS), is connected through a hybrid optical-coaxial (HFC) cable network with cable modems (cable modems CMs), the number of which can reach a hundred and even thousands of units. Taking into account the direction of data transmission, the channels are divided into a downward or direct data transmission channel (downstream – Down) from the operator to the user and an upward or reverse channel (upstream – UP) – from the user to the operator. For the organization of these channels using frequency distribution, certain frequency ranges are allocated.

Channel has a bandwidth 6MHz (8 MHz in Europe) and is used (shared) by all subscribers according to the one-to-many scheme (SMTS transmits frames intended for all end subscribers through this channel. Each modem has its own MAC address and can allocate from the general stream shots that are intended for him). As a result, it is available to the end bandwidth to the user depends on the number of end nodes and can vary widely.

Features of these methods will be discussed below. Table 1.1 shows the transfer rates of different versions of the DOCSIS protocol.

Table 1.1 – Transmission speeds of different versions of the protocol DOCSIS

Vesion	**DOCSIS**		**EuroDOCSIS**	
	Direct chanell (Down)	**Reverse chanell (Up)**	**Direct chanell (Down)**	**Reverse chanell (Up)**
1.x	42,88 Mb/s	10,24 Mb/s	55,62 Mb/s	10,24 Mb/s
2	42,88 Mb/s	30,72 Mb/s	55,62 Mb/s	30,72 Mb/s
3.0 4channel	171,52 Mb/s	122,88 Mb/s	222,48 Mb/s	122,88 Mb/s
3.0 8channel	343,04 Mb/s	122,88 Mb/s	444,96 Mb/s	122,88 Mb/s

The upstream or return channel (upstream-UP) can have a bandwidth from 0.2 to 6.4 MHz and to control access to the channel of end users, depending on the version of the technology, or the TDMA (time division multiple access) method is used, or the S-CDMA method (code division multiple access - supported in DOCSIS versions 2.0 and higher).

1.4 Set of digital subscriber line technologies xDSL

Digital subscriber line technology is used to organize network access according to the point-to-point topology. At the same time, existing copper cables can transmit an integrated stream, including computer data, video and voice data. The main field of application of this family is high-speed Internet access, dedicated channels for connecting branches, etc. The entire family of XDSL technology uses a portion of the bandwidth of a copper telephone cable and special modulation methods [10].

Access via ADSL requires telephone subscriber terminals and modems. Subscribers are connected to the global network through a digital subscriber line access multiplexer (DSLAM) (Fig. 1.3). It uses WAN ports (usually 1 GE) to connect to the IP network, and DSL ports to which the subscriber line is connected to connect clients.

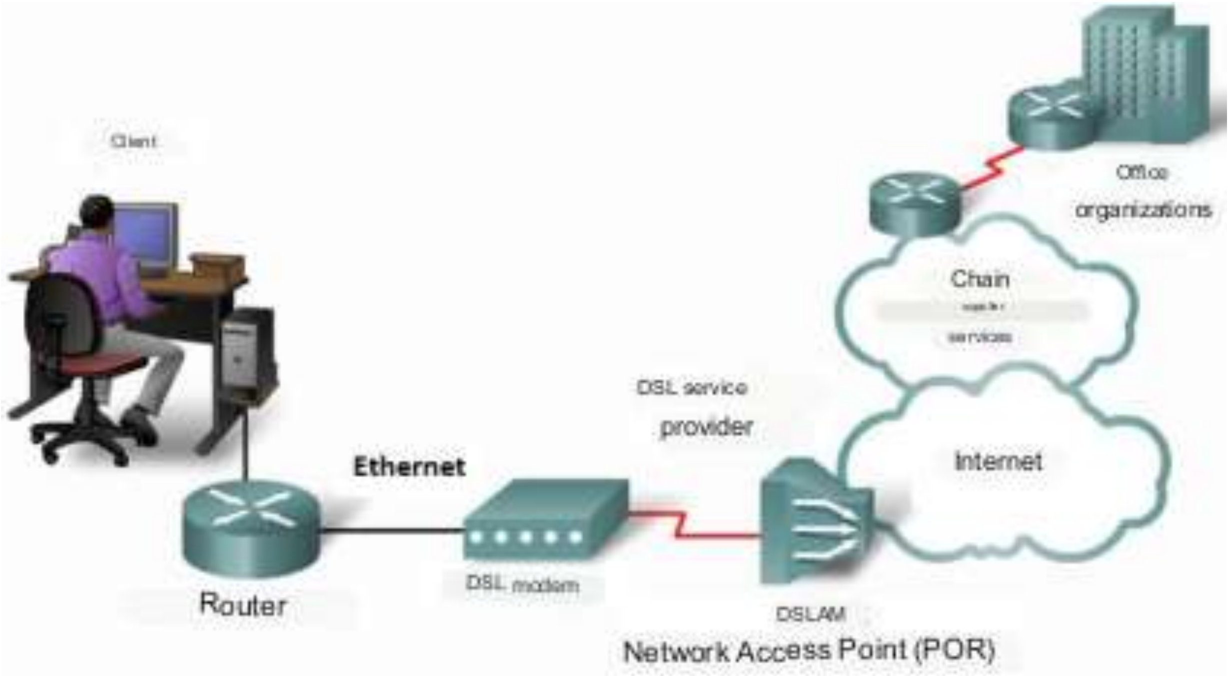

Figure 1.3 – Simplified structure of the network based on DSL technology

Letter "x" in the abbreviation defines different types of technologies. The most common are:

- ADSL – asymmetric digital subscriber line (full-speed or RADSL – speed-adaptive asymmetric digital subscriber line (dynamically adjustable transmission speed during connection establishment based on the quality and length of the physical channel);
- HDSL – high-speed digital subscriber line;
- SDSL – high-speed digital subscriber line for one pair;
- VDSL – ultra-high-speed digital subscriber line.

The main points that distinguish one technology from another are frequency ranges and ways of organizing frequency channels, differences traffic symmetry (incoming, outgoing), used modulation methods, supported line lengths and transmission speeds (table 1.2).

To ensure high speed in DSL technologies are used technique of digital signal processing with special modulation methods.

Table 1.2 – Tech logy comparative

Technology	**Speed**	**Distance**	**Application**
ADSL R-ADSL	1.5-8 Mb/s(Down) 16-1024 Kb/s	Up 6km (4km)	video and TV signal delivery
HDSL	2048Kb/s (full duplex 3 pairs)	Up to 4km	dedicated lines, telephone extension to connect to ATC
SDSL	2Mb/s (full duplex 1 Couple)	Up to 3km	dedicated lines, telephone extension to connect to ATC
VDSL	2-52Mb/s Down 1,5-16Mb/s(up)	300m-1.5 km	access, video transmission and TV signals are high clarity

Two modulation methods are used in ADSL: amplitude-phase is carrier suppression (SAR) and discrete multitone modulation (DMT) [11]. DMT modulation is adopted as a standard – more productive, less sensitive to obstacles. SAR- is used in R-ADSL.

To create several frequency channels (for reception and transmission), the frequency range is divided into sub-ranges. At the same time, frequency multiplexing (FDM) and the echo compensation method can be used. When using frequency multiplexing, one frequency range is allocated for the downlink and the second for the uplink channels. The range for the downstream stream is then divided into several frequency channels (up to 256), which, in principle, can have different widths. The upstream stream can also be frequency multiplexed (implemented in ADSL).

When applying the echo compensation method, the entire frequency range is used to organize the downlink and uplink channels. The bandwidth of the upstream channel will be equal to or slightly less than the bandwidth of the downstream channel (implemented in HDSL, SDSL, SHDSL, VDSL).

1.5 Technologies of passive optical networks (PON)

1.5.1 General characteristics of the technology

PON technology allows you to build branched networks on optical transmission channels according to the "tree" or "star" topology (point- to-multipoint connection) without intermediate active network equipment for connecting users to a common optical transmission channel [12]. PON technology makes it possible to build integrated multi-service access networks to provide subscribers with a set of services (voice, video, data) through the IP network, which have received the name Triple Play (triple service). The PON technology consists in the fact that a completely passive optical network is created on a single-mode cable between the central node, which is called OLT (Optical Line Terminal) and remote subscriber nodes - ONU (Optical Networking Unit - optical network device), which has tree topology.

Passive optical splitters are placed in the intermediate nodes of the tree (Fig. 1.4). The splitter consists of several fibres that are welded to each other in a special way in a section 2-5 millimetres long. Ratio of signal powers in output fibres (Distribution coefficient) is determined by the requirements for the network topology and can be selected by choosing the required type of splitter.

In the case where the signal power is divided equally, the attenuation, contributed by the divider itself, is about 3 dB, and about 1 dB is lost on connections - welded or switched. The attenuation coefficients in the forward and reverse channels match, and subscribers, due to the low level of the reflected signal, do not "see" each other and can communicate only through the main OLT device. To separate signals propagating in different directions, lasers with different wavelengths are used (for example, 1490 nm on a PON switch and 1310 nm on PON modems) and selective photodetectors tuned to the corresponding wavelengths (1310 nm on a PON switch and 1490 nm on PON modems).

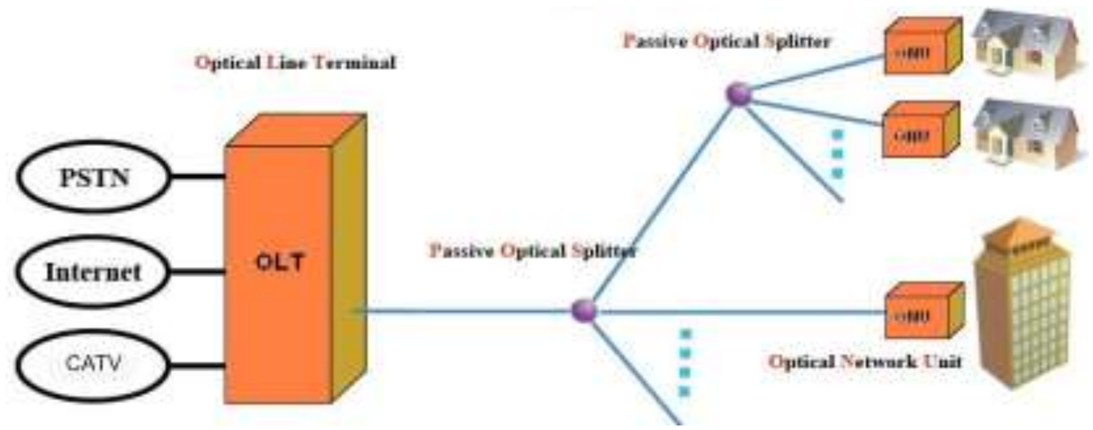

Figure 1.4 – Simplified network structure

The number of subscriber nodes connected to one OLT port is limited by the power budget (signal attenuation on splitters and optical lines) and the maximum transmission speed. The advantages of the PON architecture are: the absence of intermediate active nodes, the saving of fibers and optical interfaces on the equipment, the ease of connecting new subscribers, the ease of maintenance (Connection, disconnection or failure of one or more subscriber lines nodes does not affect the work of others).

P2MP (Point to multipoint) tree topology allows optimization placement of optical splitters based on the actual placement of subscribers, reduce costs for laying optical cable and operation cable network.

The following options for building a service access network (FTT - Fiber to The) (Fig. 1.5):

- FTTH (fibre delivery to a residential building/apartment),
- ETTV (bringing fibre to the building),
- FTTC (bringing the fibre to the place where the distribution box is placed),
- FTTC (bringing the fibre to the distribution cabinet).

On the subscriber's side, after the optical splitter, a WDM splitter is installed, which extracts radiation with a wavelength of 1550 nm and transmits it to a television signal amplifier, to which an analog or digital television receiver can be connected (Fig. 1.6).

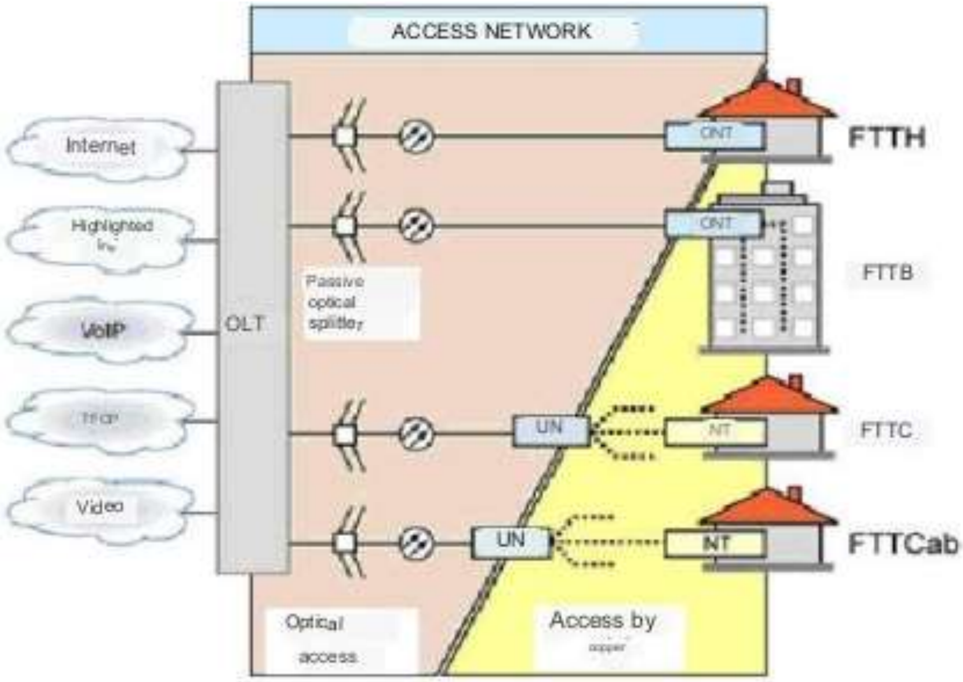

Figure 1.5 – Options for using PON technology

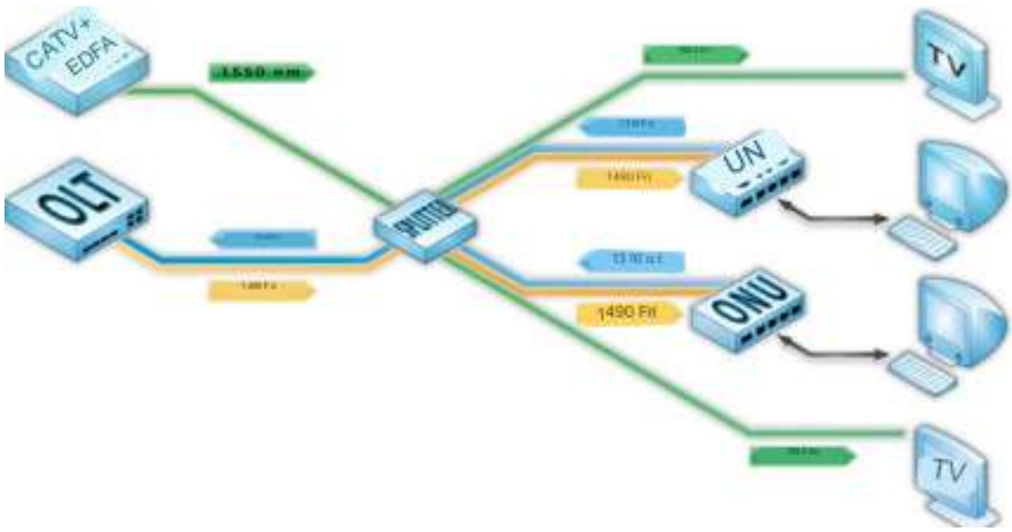

Figure 1.6 – Using of PON for transmission of SATV signals

Some operators consider it economically impractical to provide all services in the IP environment. The wavelength range of 1550 nm is reserved for the provision of regular cable television services in the direct channel. The signal generated by traditional cable television main stations is fed into the network in parallel with the IP stream through a device for spectral channel compression (WDM-wavelength compression).

1.5.2 Types of PON technology

Currently, there are the following PON technologies: APON (ATM PON), BPON (Broadband PON), GEPON (Gigabit Ethernet PON), GPON (Gigabit PON) [13]. Comparative characteristics of these technologies are given in table 1.3.

Table 1.3 – Comparative characteristics of PON technologies

Standards & Parameters	**ITU-TG.983 APON(BPON)**	**IEEE 802.3ah GEPON**	**ITU-T G.984 GPON**
1	**2**	**3**	**4**
Services	Triple Play + digital or analog TV	Triple Play + digital or analog TV	Triple Play + digital or analog TV
Frame type	ATM cells	Ethernet frames (up to which includes TDM header)	SDH frame
The maximum number of branches of the RON tree	32	32(64*)	64(128*)
Wavelength for descending (DS) and ascending (US) flows	DS: 1480-1500 US: 1260-1360	DS: 1480-1500 US: 1260-1360	DS: 1480-1500 US: 1260-1360
The maximum distance (depending on radiation power laser)	Class A (5-20 dB), 10 km Class B (1-25 dB), 20 km	Class A (5-20 dB), 10 km Class B (1-25 dB), 20 km	Class A (5-20 dB), 10 km Class B (1-25 dB), 20 km Class C (15-30 dB), 20 km

Continuation of Table 1.3

1	2	3	4
Data encryption	AES-128 encryption useful download ATM cells	AES-128 encryption useful download Ether frame	AES-128 encryption useful download SDH frame
Transmission speed	DS:155, 622 Mb/s US: 155,622 Mb/s	DS: 1 Gb/s US:1Tb/s (1.25 Gb/s Extended sequence)	DS: 1.2 Gb/s, 2.4 Gb/s US: 155 Mb/s, 1.2 Gb/s, 2.4 Gb/s
Basic protocol	ATM	Ethernet	SDH
Linear code	NRZ	8B/10B	NRZ
Equipment cost	average	average	High

The main difference between the technologies lies in the data transmission protocols and, accordingly, in the frame formats. For example, in GEPON, the frame length is 1518 bytes in accordance with IEEE 802.3. A

PON uses data transmission in frames of a fixed length of 53 bytes (ATM - cell: 48-byte data block and 5 bytes - header). The efficiency of APON when transmitting IP traffic is much lower, due to defragmentation of IP packets in ATM cells (additional time delay and equipment overload).

Let's discuss the WI-FI technology.

1.6 Technologies of wireless local networks (WI-FI) IEEE 802.11x standards

1.6.1 General characteristics of the standarts

The most common set of wireless network standards is the IEEE 802.11 set (also known as Wi-Fi). Technologies from this set of standards are intended for the organization of wireless data transmission networks (Wireless LAN) in a limited area with equal access of subscribers to the common transmission channel [6, 14].

Like all IEEE 802 standards, 802.11 operates on two lower layers ISO/OSI models: physical and channel.

Of all the existing IEEE 802.11 wireless data transmission standards, only four are most commonly used in practice: 802.11b, 802.11g, 802.11n, and 802.11ac. The basic characteristics of the 802.11x physical level standards are given in the table. 1.4.

The basic architecture, features, and services of IEEE 802.11b/g are defined in the original IEEE 802.11 standard. The IEEE 802.11b/g specifications cover only the physical layer, adding only higher access speeds.

Standards 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad belong to the physical layer of the transmission medium; 802.11d, 802.11e, and 802.11h - to the higher MAC level; 802.11c, 802.11f, 802.11i - to higher levels of the OSI model.

Table 1.4 – Basic characteristics of 802.11.x standards

Standard	**Frequency range (MHz)**	**Modulation methods**	**Width Stripes channel (MHz)**	**Transmission speed**
IEEE 802.11	2400-2483.5	DSSS FHSS	20	2Mb/s
IEEE 802.11a	5150-5350	OFDM	20	54Mb/s
IEEE 802.11b	5670-5850	DSSS	20	11Mb/s
IEEE 802.11g	2400.8-2483.5	DSSS OFDM	20	54Mb/s
IEEE 802.11n	2400.8-2483.5 5150-5350	OFDM	20, 40	600Mb/s
IEEE 802.11ac	5	SC, OFDM	40, 80, 160	6.93Gb/s
IEEE 802.11ad	60	OFDM	2160	6.7Gb/s

Let's discuss operating modes of the technology.

1.6.2 Operating modes

IEEE 802.11 defines two types of equipment. This is a client, which is usually a computer equipped with a wireless network interface card and an access point (Access point-AP), which acts as a bridge between wireless and wired networks. An access point usually includes a transceiver, a wired network interface (IEEE 802.3), and software that handles data processing

The IEEE 802.11 standard defines two modes of network operation - "Ad-hoc" mode (or temporary mode) and client/server (or infrastructure mode - infrastructure mode) (Fig. 1.7, 1.8) [6, 14].

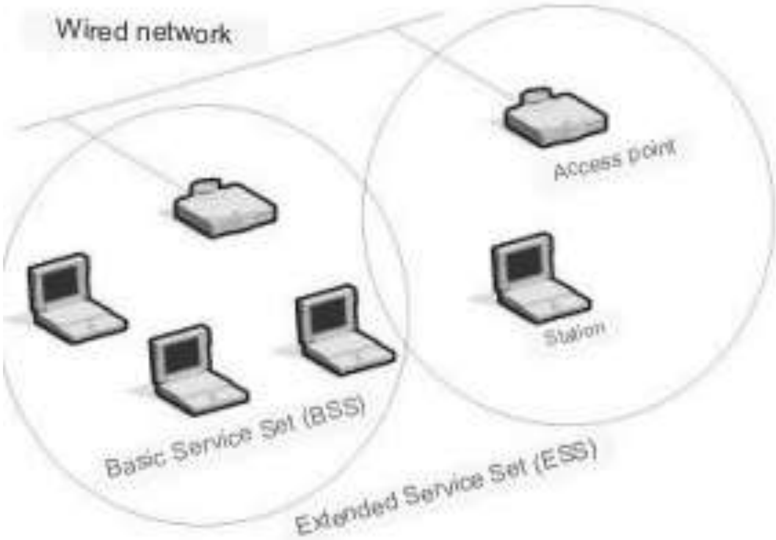

Figure 1.7 – Network architecture "client/server"

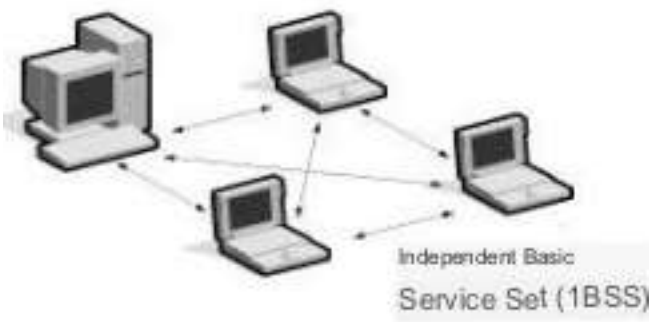

Figure 1.8 – "Ad-hoc" network architecture

In client/server mode, a wireless network consists of at least one access point connected to a wired network and some set of wireless end stations. Such a configuration is called a basic set of services (Basic Service Set, BSS). Two or more BSSs forming a single subnet form an extended service set (Extended Service Set, ESS). Since most wireless stations need to access file servers, printers, and the Internet available on a wired LAN, they will operate in client/server mode.

Ad-hoc" mode (another name is point-to-point or independent basic set of services – IBS) is a simple network in which communication between numerous stations is established directly, without the use of a special access point.

1.7 Wireless networks

Wireless technologies are intended for the organization of high-quality trunk communication channels and an effective "last mile" regardless of the presence of existing communication channels [15].

Compared to traditional wired networks, wireless technology has a number of advantages.

One of the main advantages is the ability to establish a connection at any time and from any point. The widespread use of wireless networks in public places, such as Internet cafes, allows you to connect to the Internet, download information, exchange e-mail and files.

Wireless technology is quite simple and inexpensive in terms of installation. The cost of home and commercial wireless devices continues to decrease. At the same time, despite the decrease in cost, the speed of data transfer increases, and the functionality of these devices becomes more perfect, which ensures higher speed and reliability of communication.

Wireless technology expands the boundaries of networks without the limitations inherent in cable connections. It allows you to quickly and conveniently install a network connecting an ever-growing number of users. Despite the flexibility and significant advantages of wireless networks, they too some limitations and risks are inherent.

First, wireless network technologies use unlicensed areas of the radio frequency spectrum. Since these areas of the range are not regulated, many different devices are used in them.

This leads to the overflow of spectrum areas and interference from various devices. In addition, these frequencies are used by many devices, such as microwave ovens and cordless phones, which can interfere with wireless local area networks.

Another problem with wireless communication is security. Access to wireless networks is open. Anyone can access the data transmitted in a broadcast session. At the same time, the level of data protection in the wireless network is also limited. Anyone can intercept data streams, even unintentionally. A number of methods, such as encryption and authentication, have been developed to ensure data security in wireless networks.

Wireless networks are divided into three main categories: wireless personal area networks (WPAN), wireless local area networks (WLAN), wireless metropolitan area networks (WMAN), and wireless global networks (Wireless Wide Area Network, WWAN) (Fig. 9.1).

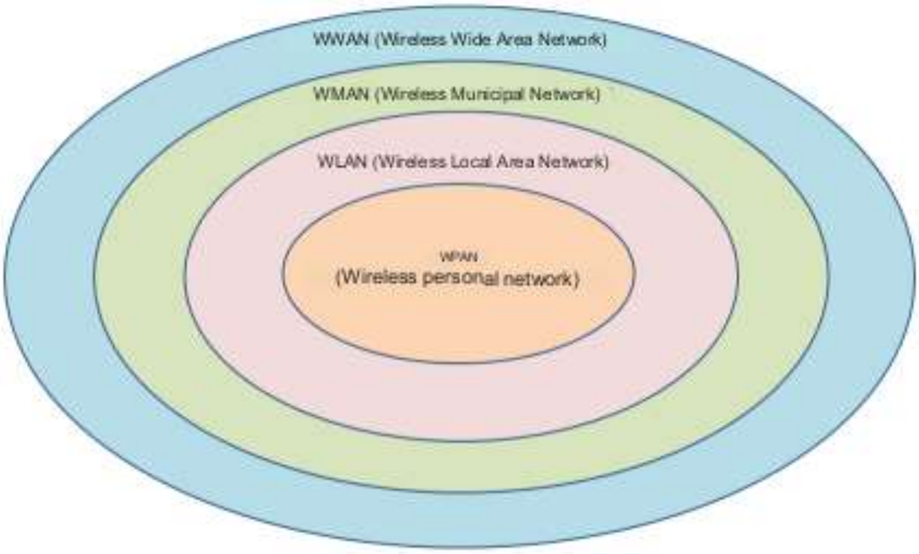

Figure 9.1 – Classification of wireless networks

Despite such clear categories, it is difficult to demarcate the scope of implementation of wireless technologies. This is due to the fact that, unlike cable networks, wireless networks do not need clearly defined boundaries. The range of data transmission in wireless networks can vary under the influence of various factors.

WPAN wireless networks are used to connect various peripheral devices, such as mice, keyboards, PDAs (Personal Digital Assistants), etc. to a computer and have the smallest operating range. All these devices are connected to one node using infrared or Bluetooth technologies.

WLANs extend the boundaries of wired local area networks (LANs). WLAN networks use radio frequency technology and meet the requirements of IEEE 802.11 (Wi-Fi) standards. In such networks, users can connect to a wired network using access points (Access Point, AR). An access point provides communication between wireless nodes and nodes in an Ethernet cable network.

WMAN networks provide broadband network access over a radio link within a city. WMAN networks comply with the IEEE 802.16 (WiMAX) standard, which describes the wireless MAN Air Interface. 802.16 is a so-called "last mile" technology that uses the frequency range from 10 to 66 GHz. The standard supports Point-to-Multipoint topology, Frequency Division Duplex (FDD) and Time-Division Duplex (TDD) technologies, with QoS support. Audio and video transmission is possible.

WWAN networks provide coverage of very large areas. The most obvious example of a WWAN network is a cellular network. These networks use technologies such as Code Division Multiple Access (CDMA) and Global System for Mobile Communication (GSM), and their operations are usually regulated by government organizations. Also examples of WWAN can be networks based on satellite and radio relay communication.

1.8 Wireless Municipal Area Networks (WMAN)

1.8.1 WiMAX technology

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications technology designed to provide universal wireless communication over long distances for a wide range of devices (from workstations and laptop computers to mobile phones). WiMAX is based on the IEEE 802.16 standard, also called Wireless MAN.

The name "WiMAX" was created by the WiMAX Forum - an organization that was founded in June 2001 to promote and develop WiMAX technology. The forum describes WiMAX as "a standards-based technology that provides high-speed wireless network access as an alternative to leased lines and DSL."

WiMAX is suitable for solving the following tasks:

- Connecting Wi-Fi access points to each other and to other Internet segments.
- Provision of wireless broadband access alternatives to dedicated lines and DSL.
- Provision of high-speed transmission services data telecommunication services.
- Creation of access points that are not tied to geographic position.

The main difference between technologies 802.160 (or fixed WiMAX) and 802.1be (or mobile WiMAX) is that fixed WiMAX allows serving only "static" subscribers, while mobile aimed at working with users moving at a speed of up to 120 km/h. Mobility means the availability of roaming functions and "seamless" switching between base stations when the subscriber moves (as in cellular networks). In some cases, mobile WiMAX can also be used to serve fixed users.

In general, WiMAX networks consist of the following main parts – base and subscriber stations, as well as equipment that connects base stations with each other and with the Internet service provider.

The high-frequency range of radio waves from 1.5 to 11 GHz is used to connect the base station with the subscriber station. Under ideal conditions, the data exchange rate can reach 70 Mbit/s, while it is not required to ensure a direct line of sight between the base station and the receiver.

1.8.2 Comparison of wireless communication standards

Comparison of wireless communication standards is shown in Table 1.5.

WiMAX and Wi-Fi technologies are often compared. Although these technologies equally use a wireless connection and are used to connect to the Internet (data exchange channel), despite this, they are aimed at solving completely different tasks.

Table 1.5 – Comparison of wireless communication standards

Technology	**Standard**	**Using**	**Pass ability**	**Range of action**	**Carriers**
Wi-Fi	802.11a	WLAN	Up to 54Mbit/s	Up to 300m	5.0 GHz
Wi-Fi	802.11b	WLAN	Up to 11Mbit/s	Up to 300m	2.4 GHz
Wi-Fi	802.11g	WLAN	Up to 54Mbit/s	Up to 300m	2.4 GHz
Wi-Fi	802.11n	WLAN	Up to 40Mbit/s	Up to 300m	2.4-2.5 or 5.0 GHz
WiMax	802.16d	WLAN	Up to 75Mbit/s	25-80Km	1.5-11 GHz
WiMax	802.16e	Mobile WLAN	Up to 40Mbit/s	1-5Km	2.3-13.6 GHz
WiMax2	802.16m	WLAN Mobile	Up to 1Gbit/s (WMAN), to 100Mbit/s (Mobile MAN)	Up to 100Km	10-66 GHz
WiMax3	802.16n	WLAN Mobile	Up to 10Gbit/s (WMAN), to 1Gbit/s (Mobile MAN)	N/A (Standard in developers)	N/A (Standard in developers)

WiMAX is a long-range system covering long distances (tens of kilometers) that typically uses licensed spectrum (although unlicensed frequencies are also possible) to provide an ISP with a point-to-point Internet connection to the end user. Different standards in the 802.16 family provide different types of access: mobile (similar to cell phone data) and fixed (an alternative to cable access where the user's wireless equipment is tied to a location).

Wi-Fi is a shorter-range system, typically covering hundreds of meters, that uses unlicensed frequency bands to provide network access. Typically, Wi-Fi is used by users to access their own local area network, which may not be connected to the Internet.

WiMAX and Wi-Fi have a completely different QoS (Quality of Service) mechanism. WiMAX uses a mechanism based on establishing a connection between a base station and a user device. Each connection uses a special scheduling algorithm that can guarantee it the same QoS parameter. Wi-Fi, in turn, uses a QoS mechanism similar to that used in Ethernet, in which packets receive different priority. This approach does not guarantee the same QOS for each connection.

1.9 Conclusion of the chapter 1

It's important to note that each solution has its own advantages, limitations, and applicability based on factors like geographical location, population density, and budget constraints. A combination of these methods and technologies, tailored to the specific requirements of a given region, can help overcome the challenges of the last mile problem and ensure universal and affordable broadband connectivity.

CHAPTER 2. PRACTICAL SOLUTION OF THE “LAST MILE” PROBLEM

2.1 A general list of troubleshooting steps

Based on the literature review, we identify and list the steps that should be included in a specific project to solve the "last mile" problem, which may include the following steps [1-7, 18-20]:

1. Needs Analysis. Start by identifying the needs of the individual user. Consider the speed of the Internet, the amount of data transfer, the types of applications and devices that will be used. This will help you understand which last-mile technologies may be most effective in meeting their needs.
2. Assess Available Options. Research available last mile technologies in your area. Consider different options such as copper wires, fiber optics, wireless connections (e.g., Wi-Fi, 5G) or satellite connections. Evaluate their advantages, disadvantages, data transfer speed, coverage and cost.
3. Choosing the optimal solution. Based on the analysis of needs and available options, choose the optimal solution for the individual user. It can be a combination of different technologies, for example, using copper wires for a stable connection to the workplace and a wireless connection for coverage in other parts of the house.
4. Installation and configuration. After choosing a solution, install and configure the necessary hardware. This may include connecting to a wired network, setting up a router, setting up a wireless access point, or installing a satellite dish.
5. Testing and Debugging. After installation, check system performance, test speed and quality of communication. Make adjustments or changes as needed to achieve optimal performance and meet user needs.
6. Migration and Training (for corporative users). Migrate to the new last mile system, ensuring a smooth transition for users. Provide the necessary training and support to employees so that they can effectively use the new network.

7. Support and Maintenance. Provide support and maintenance after system installation. This may include regular technical support, bug fixes and software updates.

8. Monitoring and Updating. Keep track of connection quality and system performance. If necessary, consider technology upgrades or system improvements to ensure the best results.

The design of the "last mile" solution must be tailored to the specific needs and conditions of the user. Of course, the best solution for choosing the optimal variant and its effective implementation will be the consultation of a specialist or an Internet provider.

2.2 Solving the problem of the “last mile” for individual users of the Internet service

When it comes to resolving the last mile problem for individual internet service consumers, the focus is on providing reliable and high-speed connectivity to residential areas. Here are some widely used approaches:

1. Digital Subscriber Line. DSL technology uses existing copper telephone lines to provide internet access. It offers faster speeds compared to traditional dial-up connections. DSL is widely available, especially in urban and suburban areas, and does not require significant infrastructure changes. However, the speed and quality of the connection may be influenced by the distance between the consumer's location and the nearest DSL provider's central office.

2. Cable Internet. Cable internet utilizes the existing coaxial cable infrastructure used for cable television. It offers higher speeds compared to DSL and is available in many residential areas. Cable networks generally have more bandwidth capacity, enabling faster and more reliable connections. However, the bandwidth may be shared among multiple users in the same neighborhood, leading to potential congestion during peak usage times.

3. Fiber-to-the-Home (FTTH). FTTH involves the deployment of fiber optic cables directly to individual homes, providing high-speed internet access. Fiber optic

connections offer exceptional speeds, low latency, and high bandwidth capacity, making it the fastest and most reliable option. On the other hand, FTTH deployment requires significant infrastructure investment and may not be widely available in all areas [16].

4. Fixed Wireless Internet. Fixed wireless internet uses radio signals to provide connectivity to individual households. A receiver is installed at the consumer's location, which communicates with a nearby base station. It is particularly useful in rural or remote areas where laying physical cables is challenging. But fixed wireless may be affected by signal interference, obstructions, or distance limitations, resulting in reduced speeds or reliability.

5. Internet via Satellite. Satellite internet is an option for consumers in areas where terrestrial options are not available. It uses satellite communication to establish an internet connection. It provides coverage in remote or underserved locations and offers global reach. But satellite internet can have higher latency due to the long-distance signals have to travel to and from satellites. It may also have limited bandwidth and be susceptible to signal degradation during adverse weather conditions.

The choice of resolving the last mile problem for individual consumers depends on factors such as location, availability of infrastructure, budget, and desired internet speeds. It's important to consider the trade-offs between speed, reliability, and cost when selecting the most suitable option.

2.3 Solving the problem of the "last mile" for corporative users of the Internet service

When addressing the last mile problem for corporate or enterprise internet service consumers, the focus is on providing reliable, high-speed, and scalable connectivity to support the needs of businesses. Here are some common approaches:

1. Dedicated Fiber Optic Connectivity. Deploying dedicated fiber optic connections directly to the corporate premises provides high-speed, low-latency, and scalable connectivity. Dedicated fiber offers dedicated bandwidth, ensuring

consistent performance and reliability. This solution requires collaboration with fiber optic service providers to establish a direct connection to the corporate network.

2. Metro Ethernet. Metro Ethernet is a high-bandwidth, fiber-based solution that extends the local area network (LAN) across a metropolitan area. It provides scalable and symmetrical connectivity, allowing for high-speed uploads and downloads. Metro Ethernet can be an effective solution for businesses with multiple branch locations requiring seamless connectivity.

3. Virtual Private Network (VPN). VPNs use encrypted tunnels over existing internet connections to provide secure and cost-effective connectivity. Businesses can establish VPNs to connect their branches, remote workers, or partners securely. VPNs can leverage various technologies, including IPsec, SSL/TLS, or MPLS, depending on the organization's specific requirements.

4. Dedicated Wireless Connections. In cases where physical cabling is challenging or not feasible, dedicated wireless connections such as point-to-point microwave or WiMAX can be deployed. These solutions offer high-speed connectivity with lower latency compared to shared wireless options like Wi-Fi. Dedicated wireless connections provide a reliable and secure option for businesses operating in areas with limited wired infrastructure.

5. Managed SD-WAN (Software-Defined Wide Area Network). SD-WAN is a technology that enables centralized management and control of multiple network connections. It combines multiple connection types (such as MPLS, broadband, or wireless) and dynamically routes traffic to optimize performance and reliability. SD-WAN allows businesses to leverage cost-effective connections while maintaining quality of service (QoS) for critical applications [17].

When resolving the last mile problem for corporate internet service consumers, it's essential to consider factors such as bandwidth requirements, scalability, security, reliability, and budget. Collaborating with internet service providers or managed service providers can help tailor the solution to meet the specific needs of the corporate environment.

2.4 Example of corporate computer network project

To demonstrate a practical solution to the problem of the last mile, a project of a corporate computer network placed in a two-story building was developed. The project provides access to the global network for all workstations, as well as efficient distribution of resources and the required level of security.

The option of segmentation of the projected network using the "Extended Star" topology was selected. The center of the star is the main communication room (Main Distribution Facilities, MDF), and the nodes of lower orders are auxiliary communication rooms (Intermediate Distribution Facilities, IDF). Network segments are arranged as follows: horizontal connections between the main (MDF) and auxiliary (IDF2) communication rooms on the first floor, and vertical connections between the auxiliary communication rooms and the main communication room (MDF).

Based on the requirements of the TIA/EIA 569 standard, the MDF room is located on the first floor of the building. This choice is explained by the following factors:

1. The selected room is located near the axis of symmetry of one of the two horizontal segments of the first floor, i.e. it is equidistant from the rooms in which workstations are planned to be installed;
2. The area of the premises is sufficient for the placement of all the necessary communication equipment and its maintenance and provides the possibility of expanding the network;
3. It is possible to connect an external optical fiber cable directly to the selected room, which connects the corporate network to the global network.

The door of the communication room opens outwards. Communication equipment is placed on racks in such a way that there is easy physical access to it.

All cables from MDF to IDF are laid through ventilation shafts, and outside them – inside special communication pipes.

UTP (Unshielded Twisted Pair) category 6 cable is chosen for the horizontal laying of a local network in the computer class – MDF (IDF) connection. The maximum length of the cable branch does not exceed 50 m. This type of cable allows you to ensure the speed of data transmission at the time of putting the network into operation 100 Mbit/s (Fast Ethernet), and in the future – 1 Gbit/s (Gigabit Ethernet). The cable is laid along the walls of the corridor above the level of the door in the communication pipes.

All servers of the corporate network are assigned static IP addresses.

In addition to the main DNS server in the MDF room, it is proposed to place additional caching DNS servers in the IDF rooms.

In order to centralize access to information resources in the MDF, it is also necessary to place e-mail, library and application servers.

An administrative server is installed in all communication rooms that segment the corporate network by subdivisions. Access to servers of this class should be granted only to maintenance personnel.

For addressing all hosts, servers and communication devices of the university's corporate computer network, the address range of the C class private network was selected: 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24.

All hosts located in administrative subnets are assigned static IP addresses, and workstations in computer classes are assigned dynamic IP addresses using DHCP servers.

Network management is carried out with the help of routers located in the main and auxiliary communication rooms.

The function of protecting the corporate network from the outside, namely, ensuring the initialization of external connections to DNS, e-mail, www services and banning any other connections, is performed by a router configured in NAT-firewall mode. Additional protection is based on the technology of access lists (ACLs).

Network expansion is possible in the following directions:

- territorial expansion of the network;
- connection of new workstations;
- increasing network bandwidth;
- increasing network manageability.

Free ranges of IP addresses are provided in each of the subnets for connecting new workstations, gateways or servers.

The physical environment of the designed network is a category 6 UTP cable, which allows data transmission at a speed of 1 Gbit/s using Gigabit Ethernet technology. Other network equipment, with the exception of switches, also supports this data rate. Thus, the designed network provides for a 10-fold increase in bandwidth by replacing the switches in use.

Appendix A shows the physical topology of the computer network. Appendix B shows the logical topology of the computer network.

2.5 Conclusion of the chapter 2

It's important to note that the practical solutions for the last mile problem vary depending on factors such as geographical location, population density, regulatory environment, and available resources. Therefore, a combination of approaches may be needed to ensure widespread and affordable connectivity, considering the unique requirements of each region or community.

3 OCCUPATIONAL HEALTH AND EMERGENCY SAFETY

3.1 Introduction

Occupational health and emergency safety in the last mile of telecommunications refers to the practices and protocols implemented to ensure the well-being and safety of workers involved in the installation, maintenance, and repair of telecommunication infrastructure in the final leg of the network.

3.2 Emergency safety

3.2.1 Risk-based approach to hazard analysis

In modern society, the mechanisms of interaction between man and nature, man and technology, individual and society are increasingly being disrupted, which leads to the appearance of many new dangers for normal life [21]. Society suffers significant losses in the form of human casualties, damages from accidents, catastrophes, natural disasters, etc. Provision of ecological, technogenic and social security and in case of emergencies becomes one of the main ones problems of any state. Under such conditions, the need to formation of knowledge on life safety as a condition of provision a comfortable and safe life. The main issue of the theory and practice of life safety is the question increasing the level of security. Security is a balanced state of a person, society, state, natural, anthropogenic systems, etc. Human safety is integral a component characteristic of the strategic direction of humanity, defined by the UN as "sustainable human development", which leads not only to economic, but also to social, cultural, spiritual growth, which contributes to the humanization of the mentality of citizens and the enrichment of positive universal human experience.

The order of priorities when developing any equipment or project requires that already at the first stages of product or system development the corresponding design has included elements that eliminate the danger.

It has been shown above that no system or operation guarantees absolute safety. Still, until we have 100% security, we try to get as close as possible to that goal. From time-to-time various activities and the methods used to solve the relevant problems are being improved, which increases our capabilities in the study of systems, determination hazards, exclusion or control of these hazards, risk reduction to acceptable level when working with these systems.

Management of the safety and stability of the functioning of the "human-living environment" system depends on the effectiveness of forecasting the socio-economic consequences of dangerous situations and timely planning and implementation a number of preventive and protective measures. Therefore, it is necessary to learn correctly assess the dangers. Obviously, danger is a stochastic, random concept that depends on many factors. Sometimes, to evaluate that whether another type of activity, we say that there is a great danger, and sometimes there is a small one. That is, we try to assess the danger quantitatively. For this purpose, it is introduced the concept of risk, which means the probability or frequency of realization danger

3.2.2 Concept of risk and its characteristics

All living and non-living things can be a source of danger. They are the carriers of danger natural processes and phenomena, man-made environment and human actions [21]. No danger have selective properties, during their occurrence they are negative act on the entire material environment that surrounds them. Dangers are realized in in the form of flows of matter, energy and information, they exist in space and in times

Despite the high technical level of production and science, annually in A large number of people are injured and killed in Ukraine and abroad.

Every year in the world accidents happen to more than 10 million people, and more than 600,000 people die.

In the USA, more than 55 people die and more than 8,500 people become disabled from accidents every year.

In Germany, there is an accident every 13 seconds, every 3 minutes one person becomes disabled, every 2.5 hours fatal accident. Today, about 120,000 people are injured at work in Ukraine every year, of which 2,500 die, more than 10,000 people receive professional disease.

The ability to predict the course of events is an integral feature of a person who improved in the process of practice throughout the entire history of human existence. Accumulation of observation results, facts that made it possible to predict natural phenomena, actions and actions of people made it possible to avoid typical dangers. The need to ensure the safety of life forced to consider the positive and negative consequences of actions, contributed to the development of the ability to model development events before their occurrence in reality. Forecasting the consequences of dangerous and of extreme situations includes: - probability assessment and analysis of the causes of extreme situations situations;

- expected force of influence (intensity) and mechanisms of danger development (damage);
- he characteristics and dimensions of the damage to the recipients (population, animal and plant life, air and geological environment, reservoirs, economic facilities);
- aggressiveness and depth of influence of danger factors (probability genetic changes in the biosphere, duration of periods of manifestation of negative consequences, multi-stage of such manifestation, etc.).
- frequency of occurrence of dangerous and extreme situations and their dynamics
- determination of the number of damages in case of implementation of dangerous and extreme situations.

All the above components are included in the concept of risk. According to ДСТУ 2293:2014 risk is the probability of causing harm, taking into account its severity.

Risk is inherent in any form of human activity that is associated with by many conditions and factors affecting the result accepted by people solutions Historical experience shows that, first of all, they began to study the risk based on the failure to obtain the intended results, which was especially evident when commodity-monetary relations, competition of economic turnover participants Research allows us to distinguish three main links of risk-dangerous behaviour; dangerous situation; trauma (Fig. 3.1).

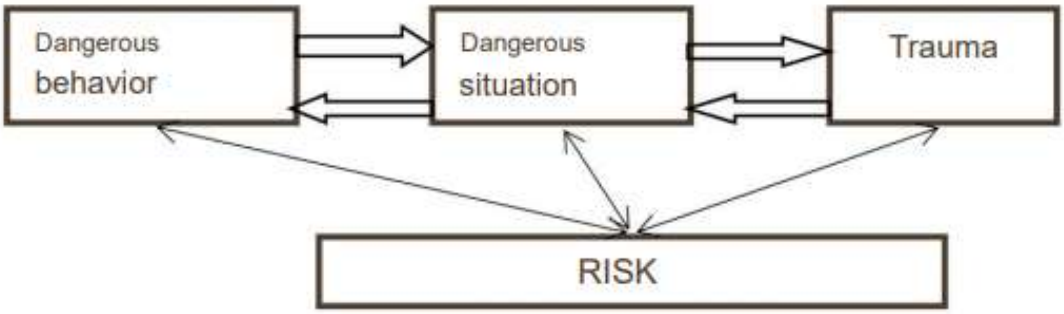

Figure 3.1 – Risk structure

The first link is one of the main reasons that cause injury or create a dangerous situation that can further lead to an accident in turn, dangerous behavior is a consequence psychological character of a person [21].

Risk is a quantitative measure of danger. Risk is a multi-component value and includes the following indicators:

- amount of damage caused by the hazard factor;
- the probability of occurrence of the danger factor;
- uncertainty of the amount of damage and probability.

Domestic experts believe that there is a risk of accidents for Ukraine directly depends on three groups of factors and is described by regression by the equation:

$$R=6,77-0,56\,x_1-0,43\,x_2-0,27\,x_3,$$

where: x_1 is the effectiveness of the environmental policy of local authorities; x_2 – capital investments in resource-saving and environmental protection equipment, x_3 – effectiveness of implementation of environmental state programs.

Risk can be defined as frequency (dimensionality inverse of time 1/s) or possibility (probability) of occurrence of an event (quantity without dimension, lies in 0 to 1), Risk can be assessed as a ratio of the number of these or others ranges from adverse consequences (n) to their probable number (N) for a certain period time:

$$R = \frac{n}{N},$$

where: R is the risk of adverse consequences, n-number of adverse events; N is the total number of probable events.

Quite conditionally, for the purpose of determining the degree of risk, the conditional is used scale regarding the probability of an undesirable result (Table 3.1).

Table 3.1 – Conventional scale of risk

The probability of an undesirable result (Amount of risk) 0.0–	**Gradation of risk**
0.1 -0.1	minimal risk
0.3 -0.3	little risk
0.4 -0.4	medium risk
0.6 -0.6	high risk
0.8-0.8	maximum risk
1.0	critical risk

There are two main types of risk, which are used to determine their methods assessment: individual and social.

Social risk is the dependence of the frequency of occurrence of undesirable events, consisting in the damage of at least a certain number of people exposed to actions danger from this number of people. In other words, this is the ratio between the number of people who can die in one accident, and the probability of such an accident Social risk characterizes the scale of catastrophic hazards.

Calculation methods of this type require complex mathematical methods calculations involved in actuarial mathematics-a branch of mathematics that studies issues related to risk assessment in various areas of human activity Insurance mathematics, financial mathematics, probability theory and mathematical statistics are also relevant to the study of risks.

Individual risk is the probability of undesirable actions arising from certain dangers at a specific point in space.

Quantitatively, the amount of risk is equal to the frequency of undesirable consequences during the action of a certain appearance. According to statistical data, the risk R for the time period f of existence of danger during the year with the total duration of observation T is determined taking into account the number of undesirable consequences n per period observations to their possible number:

$$R = \frac{n}{N} * \frac{t}{T} \cdot$$

The first coefficient reflects the probability of unwanted occurrence consequences for a year, and the second - the relative duration of the existence of the danger during year The unit of risk measurement is 1/year (it can be 1/hour, etc.).

There is also an acceptable level of risk-this is the probability of an event, the negative consequences of which can be neglected at this stage of development. There is a difference between the individual acceptable level of risk and the social acceptable level of risk. Individual acceptable level of risk should be 10-9-10-7- Permissible risk in the professional sphere is usually accepted as 10-6-10-4 and a risk of 10-3, 10-2 and more is considered unacceptable

The value of the probability of human death per year in production, which is within 10-6-10-4, is called the optimization area permissible occupational risk, in which the measure of protection against specific hazards should be undertaken taking into account economic rationale and feasibility.

Individual risk levels are also distinguished: background, acceptable, marginally acceptable. Background (natural) risk is a risk that exists in any system human interaction with technical means and the environment. Background risk can be: global, national, regional, local, object. The risk cannot be less than the background risk (see the axiom of potential danger).

Marginally acceptable risk is a risk that should not be exceeded regardless of the economic and social benefits received. The marginally acceptable level limits the aggregate risk for an individual from the whole activity as a whole (but not the risk caused by individual types of it activities).

An acceptable risk is a risk reduced to such a level that it industry, association of enterprises, enterprise, institution, organization can allow, taking into account its legal obligations and its own policy in the field occupational health and safety (according to ДСТУ 2293:2014). This is a risk that is acceptable for society (or regulatory body). As a rule, the risk is acceptable is within the limits of the background risk to the maximum permissible and should be as small as possible from economic, technical, social and other possibilities.

In some countries, the maximum permissible and acceptable risk are established in legislative procedure. For example, in the Netherlands there is a marginally acceptable risk of death in the technosphere is accepted as equal to 10-6, and acceptable - 10-8.

It is impossible to ensure absolute safety in ergatic systems, because a person is an unreliable system. The modern world has rejected the concept absolute safety and came to the concept of acceptable risk, the essence of which is striving for such a level of risk (security) as society can afford allow (at this stage of its development) and which would be economically justified (Fig 3.32). This is the principle in most countries of the world community known as ALARA (As Low as Reasonably Achievable) - as low as reasonably achievable. This graph shows that with increasing security costs technical systems in conditions of limited funds, the technical risk decreases, but the socio- economic risk increases, since the amount of funds that go into this sphere, decreases. Spending excessive money on security technical systems in the specified conditions, it is possible to cause damage to the social sphere, for example, to worsen medical care, to reduce assistance to the elderly, children, the disabled, etc. As can be seen from fig. 3.2, there is an optimal amount of funds that should be invested in the technical security system and at which it is ensured the minimum value of the individual risk factor. The plot indicated on graphics as "limits of acceptable risk", is optimal in terms of provision minimal risk. To the left and right of this area is the risk of activity person is growing. On the left is a high coefficient of individual risk conditioned by the imperfection of the technical system, and on the right-conditioned low level of social and economic security [21].

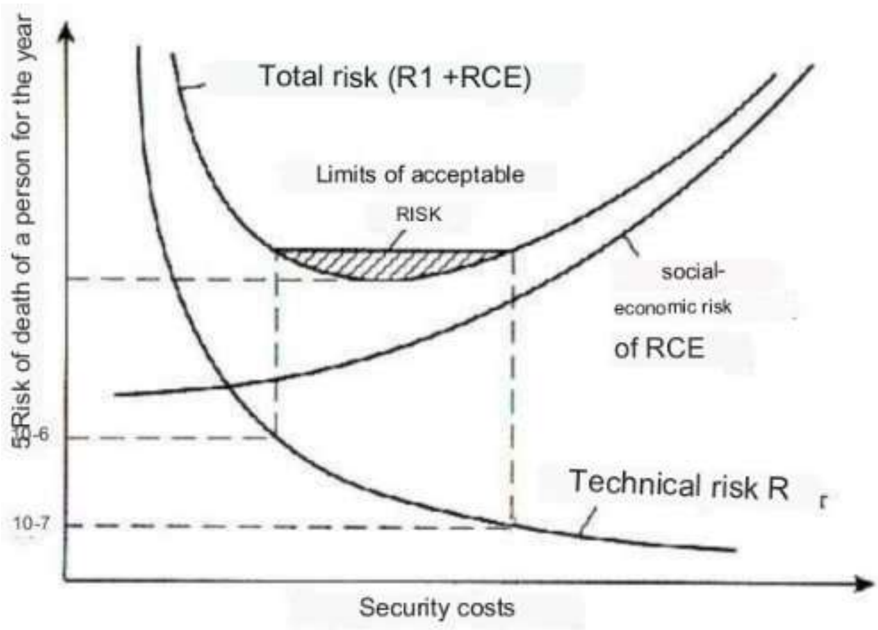

Figure 3.2 – Concept of acceptable risk

Currently in Ukraine, Resolution of the CMU dated December 27, 2017 No. 1043, which approved the criteria for assessing the degree of risk from carrying out economic activity and determining the periodicity of implementation of planned measures of state supervision (control) in the field of man-made and fire safety

3.3 Occupational health

3.3.1 Concept and definition of physiology, occupational hygiene and industrial sanitation

Labor physiology is a branch of physiology that studies changes in the state of the human body during various forms of work and develops the most favorable regimes of work and rest [22]. The concept of activity is inextricably linked with ideological phenomena (goal, plan, interest, etc) and labor movements. Physiological and biochemical processes occurring in the body, and primarily in the cerebral cortex, are the basis of human activity. The study of labor involves determining the physiological content of work (physical load, nervous and emational tension, rhythm/ pace and monotony of work volumes of information received and processed). These data make it possible to determine the load on the body during work and to develop rational regimes of work and rest, rational organization of the workplace, to carry out professional selection and thus ensure the optimal working capacity of a person over a long period of time.

In any tabor activity, two components are distinguished mechanical and mental. The mechanical component is determined by the work of the muscles. Complex labor processes consist of simple muscle movements that are regulated by the nervous system. During the work of the muscles, blood flows to them, which supplies nutrients and oxygen and removes the decay products of these substances. This is facilitated by the active work of the heart and lungs, which also require additional energy expenditure for intensive work.

The mental component is characterized by participation in the work processes of organs feelings, memory, thinking, emotions and willpower.

Hygiene is a branch of medicine that studies the impact of living conditions on human health and develops measures to prevent diseases, ensure optimal living conditions, preserve health and extend life Occupational hygiene is a subfield of general hygiene that studies the impact of the production environment on the functioning of the human body and its individual systems. The human body was formed in the conditions of a real natural environment. The main factors of this environment are microclimate, air composition, electromagnetic, radiation and acoustic background, light climate, etc.

Man-made human activity, depending on the conditions of implementation, the peculiarities of technological processes can be accompanied by a significant deviation of the parameters of the production environment from their natural value, which is desired to ensure the normal functioning of the human body. The result of the deviation of the factors of the production environment from the natural physiological norms for a person, depending on the degree of this deviation, may be different types of disturbances in the functioning of individual body systems or the body and the whole- partial or complete, temporary or permanent. The mechanism of influence of certain factors of the production environment on the human body and its possible consequences and the measures and means of protection of workers will be considered in the following topics of this section. It is practically impossible to avoid the unwanted influence of man's man-made activities on the state of the production. environment and the environment as a whole. Therefore, the goal of occupational hygiene is to establish such marginal deviations from natural physiological norms for humans, such permissible loads on the human body according to individual factors of the production environment, as well as permissible loads on the human body under the complex action of these factors, which will not cause negative changes in functioning of the human body and its individual systems, as well as genetic ones in future generations Constituent parts of legislation in the field of occupational hygiene are laws, resolutions, regulations, sanitary rules and regulations approved by the Ministry of Health of Ukraine, the Ministry of Environmental Protection and Nuclear Safety of Ukraine, the Ministry of Labor and Social Protection, the State Standard of Ukraine (for example, the laws "On protection of atmospheric air", "On labor protection", sanitary rules "Protection of atmospheric air in populated areas" "Sanitary norms of the microclimate of industrial premises" State Standard of Ukraine "Instructions for the implementation of environmental audit, etc.).

Sanitation is a set of practical measures aimed at improving the environment surrounding a person Industrial sanitation is a branch of sanitation aimed at implementing a complex of sanitary and health measures to create healthy and safe working conditions. According to ДСТУ 2293-99 (ciune 4.60), Industrial sanitation is a system of organizational, hygienic and sanitary-technical measures and means of preventing exposare of workers to harmful production factors. The scope of industrial sanitation is the prevention of occupational hazards (harmfulness) that can lead to occupational or occupationally caused diseases, including those that are fatal under the influence of such factors as the emission of electromagnetic fields, ionizing radiation, noise, vibrations, chemicals, low temperature, etc.

3.3.2 Hygienic classification of work

Hygienic classification of work is necessary to assess the specific conditions and nature of work at workplaces [22]. Based on this assessment, decisions are made aimed at preventing or maximally limiting the impact of adverse production factors. The assessment of working conditions is carned out on the basis of the "Hygienic classification of working conditions according to indicators of harmfulness and dangerous factors of the production environment, difficulty and tension of the labor process Based on the principles of Hygienic classification, working conditions are divided into 4 classes optimal working conditions, acceptable working conditions, harmful and dangerous working conditions.

The determination of the overall assessment of working conditions is based on a differentiated analysis of the definition of working conditions for individual factors of the production environment and labor process. Factors of the production environment include: microclimate indicators; the content of harmful substances in the air of the working area; radiation; level of noise, vibration, infrasound, illumination. The labor process is determined by indicators of difficulty and intensity of work. The term "hardness of work" refers to the degree of involvement of muscles and physiological costs due to physical exertion. Work intensity reflects the load on the central nervous system and is assessed by 16 indicators characterizing intellectual, sensory, emotional loads, monotony and work modes. Adequate assessment of specific conditions and the nature of work will contribute to the well-founded development and implementation of a set of measures and technical means for the prevention of industrial injuries and occupational diseases, in particular by improving the parameters of the industrial environment, reducing the difficulty and tension of the labor process.

3.4 Conclusion of the chapter 3

By implementing these measures, telecommunications companies can promote a safe and healthy working environment for their employees involved in the last mile of telecommunications. Prioritizing occupational health and emergency safety helps minimize the risk of accidents, injuries, and other adverse events, ultimately contributing to the overall well-being and productivity of the workforce.

CONCLUSION

The research allow us to know deeply about Last mile in Telecommunication.

Various methods of delivering information like one way or two way communication and many more.

Practical solutions like labour safety and safety of an individual.

Last mile telecommunication has seen significant progress in expanding connectivity and reducing the digital divide. The deployment of fiber-optic cables and advancements in wireless technologies have improved internet access and enabled the proliferation of new digital services. However, there is still work to be done to ensure universal and affordable last mile connectivity, particularly in undeserved areas. Continued investment, collaboration, and technological advancements will be key to achieving this goal and unlocking the full potential of the digital era.

REFERENCES

1. Computer networks. Principles, technologies, protocols: textbook for universities V.G. Olifer, N.A. Olifer. 5th ed. SPb.: Peter, 2016.992 p.: ill.

2. Stallings William. Computer Networking with Internet Protocols and Technology / William Stallings. — 2004. — 640 p.

3. Cherry, Steven (September 1, 2003). "The Wireless Last Mile". IEEE Spectrum. No. Special Report. IEEE. Retrieved 26 April 2019.

4. Last mile (telecommunications) https://en.wikipedia.org/wiki/Last_mile_(telecommunications).

5. Balcik, Burcu; Beamon, Benita M.; Smilowitz, Karen (30 April 2008). "Last Mile Distribution in Humanitarian Relief". Journal of Intelligent Transportation Systems. 12 (2): 51–63. doi:10.1080/15472450802023329. S2CID 6063514. Retrieved 12 February 2019.

6. Технології останньої милі: Текст лекцій з дисципліни «Комп’ютерні мережі та засоби телекомунікацій» [Електронний ресурс] : навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка», спеціалізації «Інформаційно-обчислювальні засоби радіоелектронних систем»/ П. В. Кучернюк. – Київ : КПІ ім. Ігоря Сікорського, 2019. – 124 с.

7. Кучернюк П. В. Текст лекцій з дисципліни «Комп’ютерні мережі та засоби телекомунікацій», розділ «Засоби телекомунікацій» для студентів спеціальності 7.05090201, 8.05090201 «Радіоелектронні апарати та засоби». – К.: НТУУ «КПІ», 2013 р. – 127 с.

8. Harry G. Perros. Connection-Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks. - John Wiley & Sons, 2005. – 356 p.

9. Mehmet Toy. Cable Networks, Services, and Management. - John Wiley & Sons, 2015. – 376 p.

10. Definitions of Managed Objects for Very High Speed Digital Subscriber Line 2 (VDSL2) https://www.rfc-editor.org/info/rfc5650

11. Definitions of Managed Objects for the ADSL Lines https://www.rfc-editor.org/info/rfc2662

12. RFC-4837. Managed Objects of Ethernet Passive Optical Networks (EPON). L.Khermosh. July 2007.

13. What is APON, BPON, EPON, GPON ? https://www.heyoptics.net/blogs/wiki/apon-network

14. 802.11n: Next-Generation Wireless LAN Technology https://web.archive.org/web/20060514160636/http://www.broadcom.com/docs/WLAN/802_11n-WP100-R.pdf

15. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

16. Fiber to the home (FTTH) https://www.techtarget.com/searchnetworking/definition/fiber-to-the-home

17. What is Managed SD WAN? (With Comparison App) https://www.netify.com/learning/what-is-managed-sd-wan

18. Stallings W. Data and Computer Communications 10th - Pearson, 2013. – 912 p.

19. Stallings William. Computer Networking with Internet Protocols and Technology / William Stallings. — 2004. — 640 p.

20. Thurwachter Jr. Data and telecommunication: systems and applications / Jr. Thurwachter, N. Charles. — 2000. — 630 p.

21. Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. – 336 с.

22. Безпека життєдіяльності та охорона праці. Навчальний посібник для здобувачів вищої освіти із галузі знань 08 «Право», спеціальність 081 «Право». Львів: Львівський державний університет внутрішніх справ, 2022. 219с.

ANNEXES

Appendix A

Physical network topology

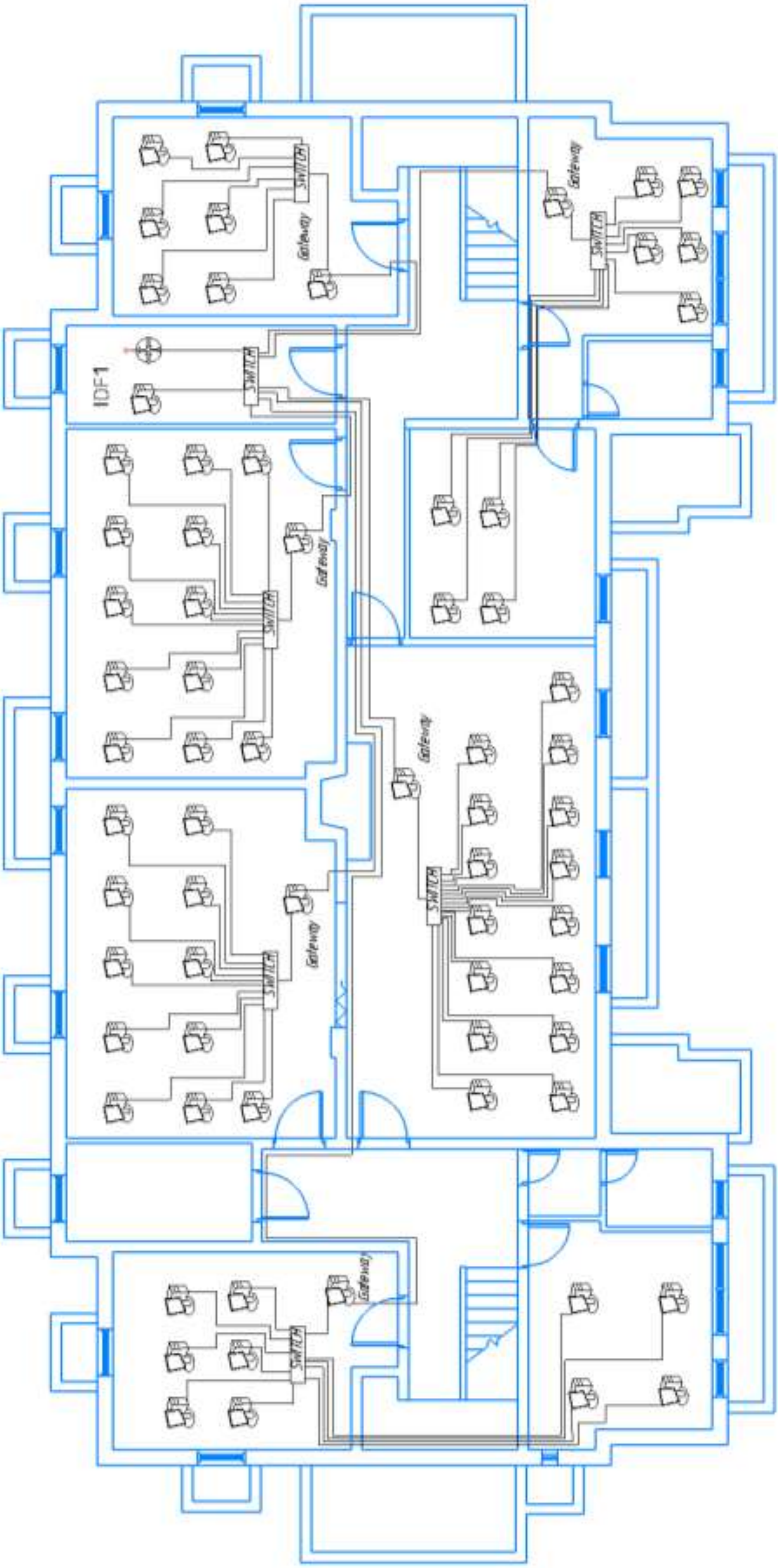

Figure A.1 – Ground Floor

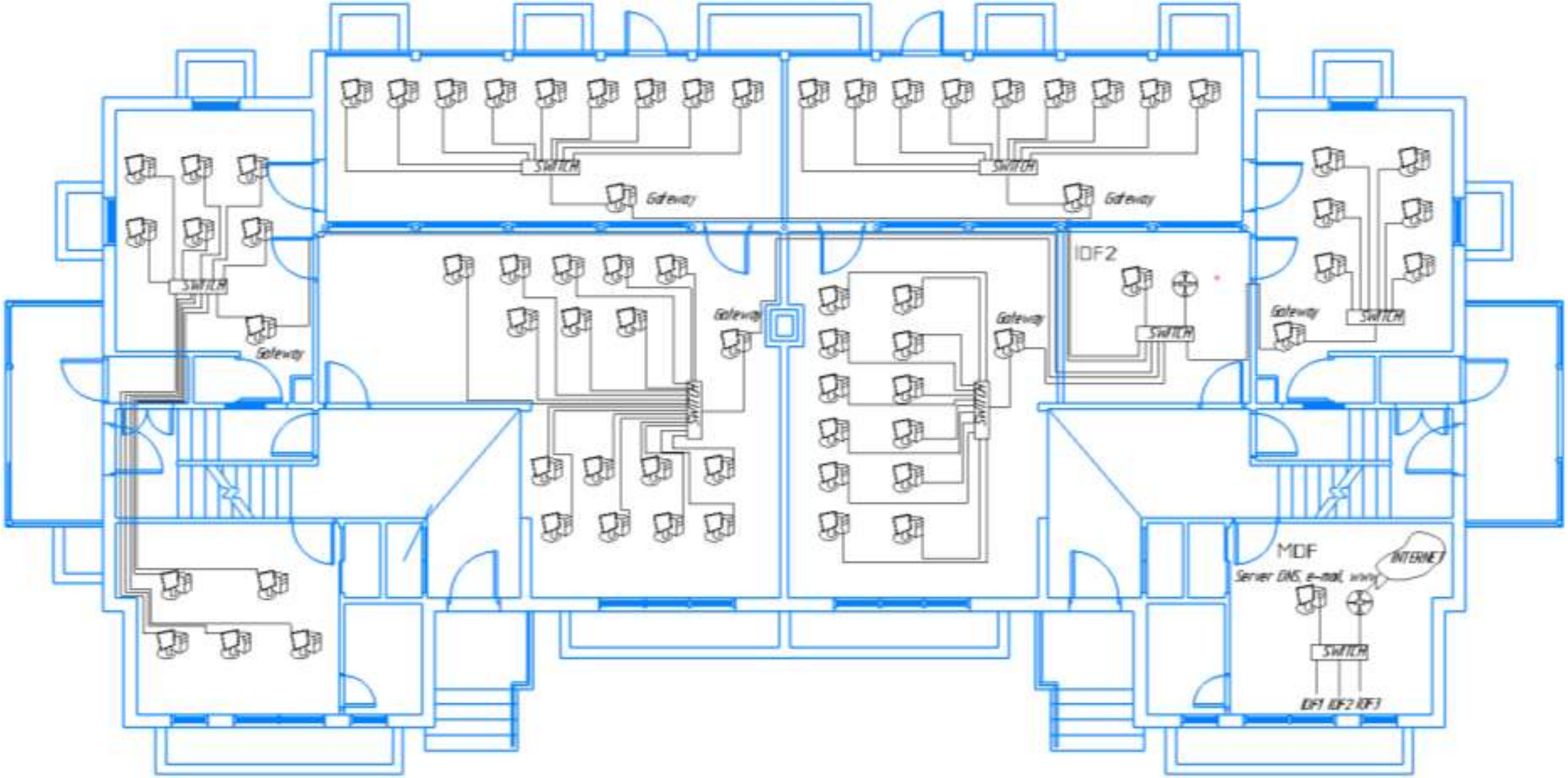

Figure A.2 – First Floor

Appendix B

Logical network topology