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: Development of a local computer network for the university library

Submitted by: fourth year student 4 , group ICH-42
specialty 122 Computer science
(code and name of specialty)

(signature) Kanjuru Kevin (surname and initials)

Supervisor (signature) Nykytyuk V.V. (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) (surname and initials)

Ternopil
2022

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 Kanjuru Kevin
(surname, name, patronymic)

1. Paper topic Development of a local computer network for the university library

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

Approved by university order as of 17.12.2021 № 4/7-1068.

2. Student's paper submission deadline 20.06.2022

3. Initial data for the paper task for work, structure of the university library, ways to organize a local computer network

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

Methods of local networks organization; General provisions; Ethernet LAN architecture
Two types of networks; Ways to organize wireless measures;
Designing a wired computer network for a university library; Overview of network cables and cable system components; Analysis and selection of network equipment;
Network design; Calculation of network bandwidth;
Designing a wireless network for a university library; Selection of network elements;
Hardware setup; Labor protection; Safety issues when laying networks;
The issue of lighting when working at a computer.

6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
LABOR PROTECTION	Lazaryuk V.V.		

7. Date of receiving the assignment _____

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
	Analysis of the task for qualifying work		
	Writing chapter 1		
	Writing chapter 2		
	Writing chapter 3		
	Writing chapter 4		
	Preliminary defense of work		
	Defense of work		

Student _____ Kanjuru Kevin
(signature) (surname and initials)

Paper supervisor _____ Nykytyuk V.V.
(signature) (surname and initials)

ANNOTATION

Information Technology: Development of a local computer network for a university library // Qualification work of the educational level "Bachelor" // Kanjuru Kevin // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information System and Software Engineering,

Department of Computer Science // Ternopil, 2022 // P. , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

In the qualifying work, the development of a computer network for the university library was carried out. The peculiarities of the implementation of wired and wireless networks were analyzed, and for the implementation of a local computer network it was decided to use the wired Ethernet network. The features of network cables and cable system components are also analyzed. To organize the local network of the university library, it is suggested to use a fiber optic cable. Methods of connecting computers to the hub and server were also analyzed. A drawing of the room plan was made and the location of computer network elements was indicated on it. Variants of network elements are offered, including computers, servers, hubs, etc. Calculations of the bandwidth of the projected network were carried out. The main elements of the Wi-Fi network are also analyzed. Specific types of these items are selected, including network adapter, wireless adapter, PCI adapter, and access points. Features and main stages of setting up such a network are considered.

CONTENTS

INTRODUCTION

A particularly powerful tool in the process of student education is the use of the university library. This includes access to literary sources, reference data, methodological support, lecture notes, but also the opportunity to individually perform the tasks received by students with the possibility of solitude and concentration of attention in the large and silent reading room of the library.

In order to effectively teach students and provide them with access to modern information resources, in particular the resources of the university library, it is proposed to organize computerized workplaces along with places for reading. This will be especially relevant for foreign students who often come to study at our university without having a netbook or computer with them, and buying them becomes problematic due to the high cost and difficulty of using them in a student dormitory.

The use of computers in the university library would significantly improve the situation and increase the opportunities of students in the process of learning, searching for materials, preparing essays, drawing up reports for laboratory and practical work, etc.

However, for this it is necessary to plan the placement of computers in the library reading room and to design a computer network for the efficient functioning of the computers. This is the purpose of the qualification work.

CHAPTER 1
METHODS OF LOCAL NETWORKS ORGANIZATION

1.1 General provisions

A computer network is a set of computers connected via communication channels and means of switching into a single system for messaging and user access to software, technical, informational and organizational resources of the network.

Wired technologies (data transmission via twisted pair cable or coaxial or fiber optic cable) are used as a medium for the data transmission over the network, and wireless technologies are used too, the principle of which will be used to build the network of this work.

There are different types and ways of building computer networks. The most “powerful” technical capabilities are, of course, provided by a wired network.

However, networks built using radio technologies are becoming more and more promising, allowing them to gain maximum mobility and independence.

Ease of creation and restructuring - this advantage of the wireless network is the main one. It means that in order to organize a workable and fast enough wireless network, it is enough to make a minimum of effort, and most importantly, it will require a minimum of costs.

Today, the indisputable advantage of wireless networks is universal mobility, which allows a person to do his job in any conditions, wherever he is.

Mobile phones, personal assistants, portable computers are representatives of the technology that brings this very mobility into human life.

With the advent of wireless networks and related computer technology, mobility has taken on a broader meaning. Now it allows you to connect with each other any devices capable of communication, of which there are so many in the modern world.

1.2 Ethernet LAN architecture

Ethernet is the most popular physical network architecture in use today. Created in the 1960s at the University of Hawaii as an ALOHA network, it was the first packet radio network.

In 1972, Robert Metcalfe and David Boffs implemented a network architecture with cabling and signaling at Xerox PARC, and in 1975 they released the first Ethernet product. This original network allowed more than 100 computers to be connected in a network with a data transfer rate of less than 3 Mbps at a distance of one kilometer.

Based on the original specification, Xerox, Intel and Digital have created an extended network specification that allows data transfer at 10 Mbps. This specification became the basis for the later IEEE 802.3 standard. In 1990, the IEEE 802.3 committee issued a specification for Ethernet running on twisted pair cable.

Ethernet has a bus or star topology that uses baseband signaling and CSMA/CD network access arbitration. The Ethernet transmission medium is passive, i.e. computers control the transmission of signals over the network.

Ethernet arbitrates network access using CSMA/CD. This means that only one workstation can use the network at a time. CSMA/CD functions similarly to the old telephone systems used in rural areas. If you needed to talk on the phone, you had to pick up the receiver and listen to see if anyone was using the line. If the line is already busy, then it was impossible to dial the number or talk. I had to just hang up and wait, and then listen again to see if the line was free. When two people dialed at the same time, a "conflict" would arise and they would have to hang up and try again. The first of them, who seized the free line, got access and could call.

In Ethernet, workstations send signals (packets) over the network. When a conflict occurs, they stop the transmission, wait for a random period of time, and then retry it. Using such rules, workstations must compete with each other for the

opportunity to transmit information over the network. For this reason, Ethernet is called a line grab contention system. Most Ethernet networks operate at 10 Mbps.

IEEE 802.3 standart.

The 802.3 committee has defined a standard basis for all Ethernet frame types. The minimum frame length is 24 octets, the maximum is limited to 1500 octets including payload and headers. Headers are used to identify the recipient and sender of each packet. The only restriction on identification is that each address must be unique and must be six octets long.

The first 12 octets of each packet are allocated to a 6-octet destination address (intended recipient address) and a source address (sender address). These addresses are hardware address codes and are often referred to as MAC addresses. The MAC address can be either a unique "universally configurable address" that is automatically assigned to all Ethernet network adapters at the time of manufacture, or a pre-configured address. The automatically assigned MAC address consists of six two-digit hexadecimal numbers separated by a colon, for example, 99:02:11:D1:8F:19. The first two pairs of numbers are the manufacturer's identification number. Each network adapter manufacturer must be licensed by the IEEE and given a unique identification number and MAC address range.

Custom addresses are known as "locally configurable". They are designed to identify a room, department, voice mail extension owner, and so on. The use of locally configured addresses can provide the network administrator with extremely valuable troubleshooting information. Unfortunately, assigning such addresses can be an extremely difficult and time-consuming task.

802-compliant frames may contain the address of a single computer or refer to a group of workstations with a common, definable characteristic. The transfer of data to a group of machines is called multicast.

Under normal operating conditions, Ethernet network cards only receive frames whose destination address matches the card's unique MAC address or satisfies the multicast criteria. However, most network adapters can function in the mode of receiving all network packets, which corresponds to the reception of

absolutely all packets on the local network, regardless of addresses. The use of this mode is associated with the risk of unauthorized access by another user of the local network, as well as the problem of reducing the performance of not only the network, but also the computer itself.

While most of the improvements to the 802.3 standard over previous versions of Ethernet have been in the native protocol, one significant improvement has been made to the 802.3 frame structure. The 802 Committee needed a self-contained standard independent of the good behavior of other protocols. Therefore, the Type field, which was two octets long in previous Ethernet protocols, has been replaced with a Length field of the same length.

With a given minimum and maximum field length determined by the worst-case message transmission time window, it was not necessary to define the frame size for the client protocol. Instead, the 802.3 working group changed the purpose of the two-octet field, which now explicitly specified the length of the frame's data field, and left the task of identifying the protocol to LLC.

Now consider the purpose of the frame control sequence (FCS). The computed value is assigned to this field by the computer sending the frame. The computer receiving the frame also knows how to calculate the value and thus checks the integrity of the packet. A packet can be corrupted during transmission due to a variety of reasons. Electromagnetic emissions, crosstalk, etc. may damage the package without affecting its delivery to the correct address.

Upon receipt of the packet, the FCS field is checked for integrity using a cyclic redundancy check (CRC) technique. The computer that received the packet performs the same calculation as the computer that sent the packet and compares the received value with the value read from the FCS field. If the values match, you can be sure that the correct data has arrived. Otherwise, a request is sent to retransmit the packet.

Ethernet 10 Mbps

Ethernet uses many types of cable. Different types of Ethernet use different signaling characteristics, but all use the same Ethernet frame specification, 10

Mbps rate, and CSMA/CD access arbitration. Here are the four most common types of 10 Mbps Ethernet cabling:

- thick Ethernet with thick coax cable
- thin Ethernet with thin coax cable
- 10 Base T where UTP cable is used
- 10 Base FL, which uses fiber optic cable

Ethernet 100 Mbps

For some applications, 10 Mbps is not enough. There are two competing standards to push traditional performance up to 100Mbps:

- 100 VG - AnyLAN
- Ethernet 100 Base T or Fast Ethernet

When designing a LAN for office workplaces based on the Ethernet protocol, the type of cable system 10 Base T will be used, which is the most optimal for small businesses.

1.3 Two types of networks

All networks have some common components:

- servers;
- clients;
- transmission medium - a way of connecting computers;
- shared data;
- shared peripherals;
- resources.

Despite the noted similarities, all networks may be divided into:

- peer-to-peer networks (PtP);
- networks, based on the server (Sb).

The differences between such networks are fundamental, as they predetermine the different capabilities of these networks. The choice of network type depends on many factors:

- the size of the enterprise;

- the required degree of safety;

- type of business;

- availability of administrative support;

- volume of traffic;

- the level of funding.

1.3.1 PtP networks

In the PtP network (Fig. 1.1), all computers are equal.

PtP networks often includes no more than 10 computers. Hence their other name is the working group, i.e. small group of users.

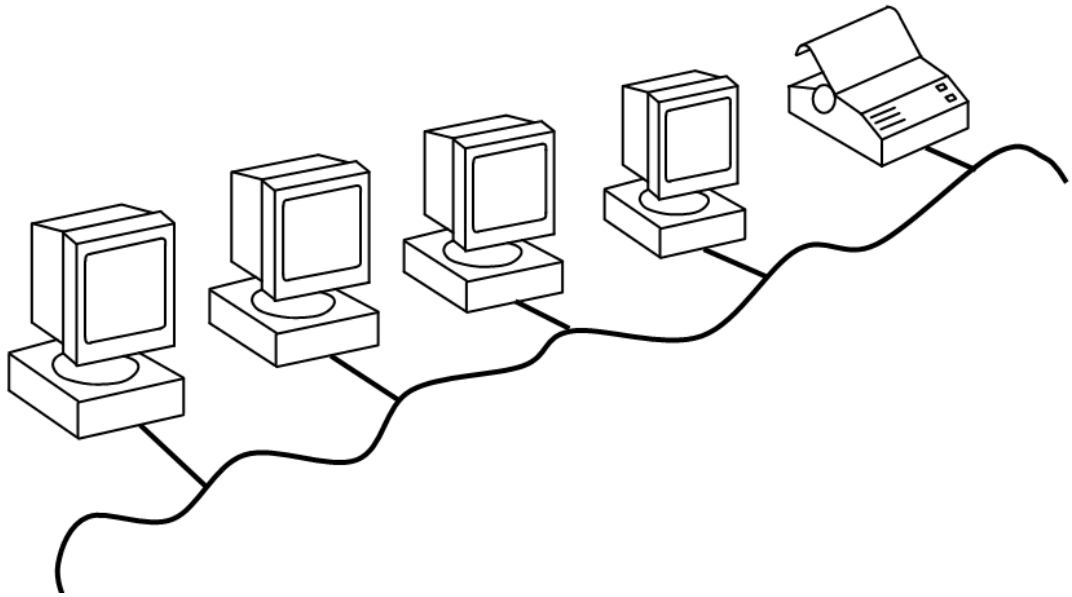


Figure 1.1. PtP network

PtP networks are very simple. This is usually the reason why PtP networks cost less Sb networks.

A PtP network is quite suitable where:

- the number of users does not exceed 10 people;

- users are located compactly;

- data protection issues are not critical;

- in the foreseeable future, a significant expansion of the company and, consequently, the network is not expected.

If these conditions are met, the PtP network structure will most likely be correct.

1.3.2 Server based networks

If more than 10 users are connected to a PtP network, it may not be able to cope with the volume of tasks assigned to it. Therefore, most networks have a different configuration - they work on the basis of a dedicated server (Fig. 1.2).

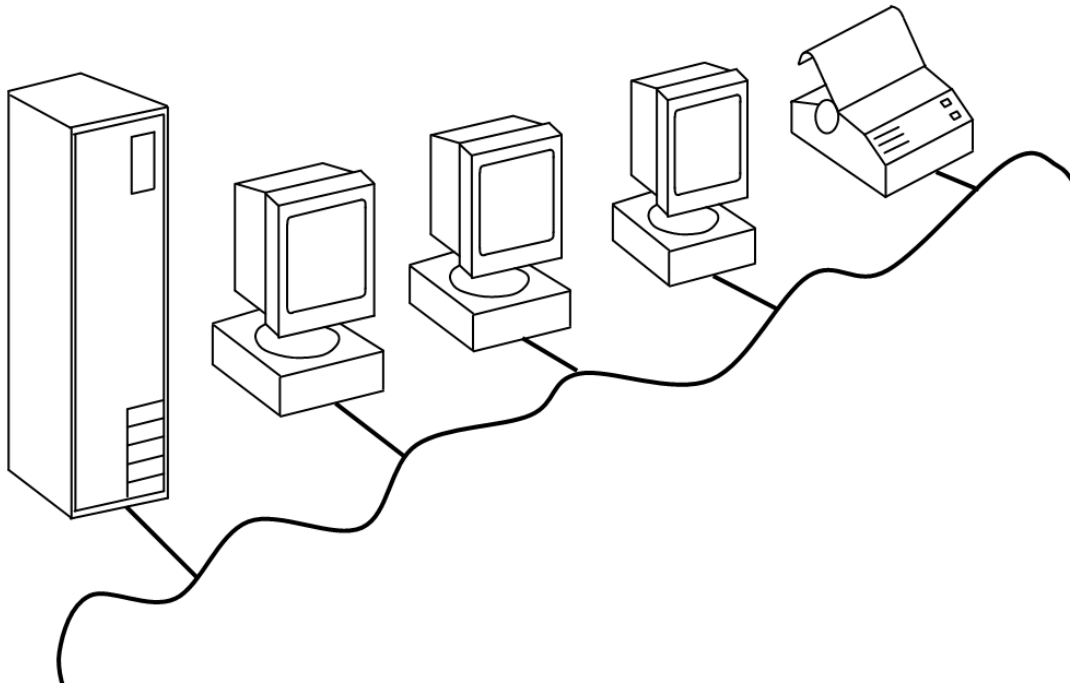


Figure 1.2. Sb network

With an increase in the size of the network and the volume of the network diagram, it is necessary to increase the number of servers.

The main argument that determines the choice of a server-based network is, as a rule, the reliability of data protection. In networks such as Windows NT, one administrator can deal with security issues: he forms a single security policy and applies it to each network user.

Server-based networks are capable of supporting thousands of users. Networks of this size, if they were peer-to-peer, would be impossible to manage.

1.4 Ways to organize wireless measures

At the dawn of the development of radio engineering, the term "wireless" (wireless) was used to refer to radio communications in the broad sense of the word, that is, literally in all cases when information was transmitted wirelessly. Later, this interpretation practically fell out of circulation, and "wireless" began to be used as an equivalent to the term "radio" (radio) or "radio frequency". Now both concepts are considered interchangeable when it comes to the frequency range (0.003-300) GHz. However, the term "radio" is more often used to describe technologies that have been around for a long time (broadcasting, satellite communications, radar, radiotelephony, etc.). And the term "wireless" today is usually attributed to new radio technologies, such as microcellular and cellular telephony, paging, subscriber access.

The most common wireless technologies are Wi-Fi and Bluetooth. Each type of technology has both advantages and disadvantages, which determine the areas of their application.

1.4.1 Bluetooth technology

Bluetooth technology became known to the general public in the spring of 1998, when Ericsson, IBM, Intel, Nokia and Toshiba announced the creation of a special working group for its joint development and further promotion. The new technology was developed with the aim of wirelessly exchanging information between various devices, such as a computer, cell phone, printers, digital cameras and other similar devices. The working group later included Compaq, Dell, Qualcomm, Motorola, Lucent Technologies, and currently the group has about 1,500 members.

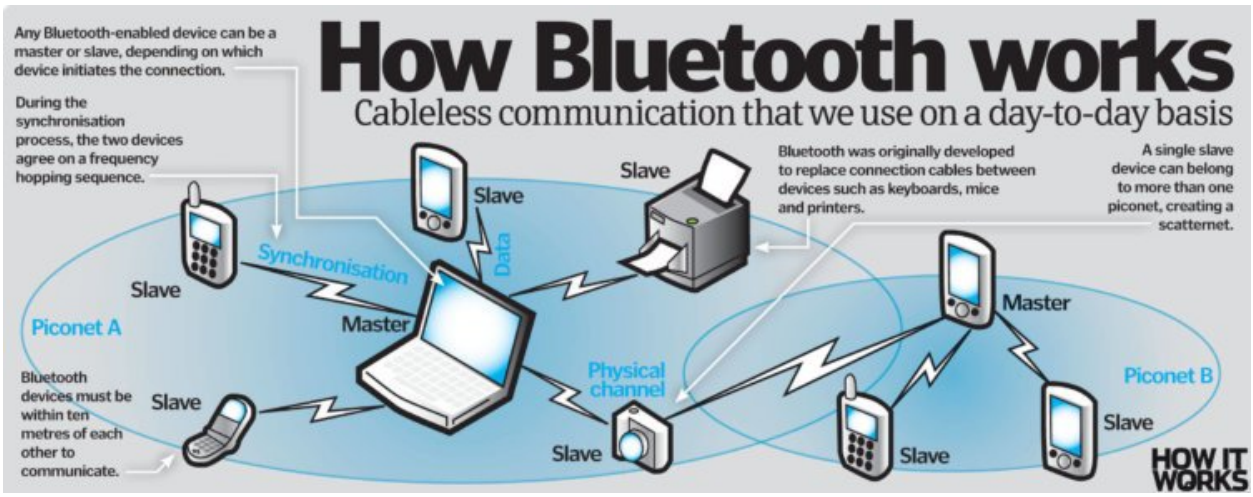


Figure 1.3. Bluetooth technology

Bluetooth is a low power radio technology. In Bluetooth technology, the so-called lower ISM band, 2.45 GHz, is used to transmit information. This range is widely used in civilian practice, for example for medical devices, so it is approved for operation in most countries of the world. Coupled with the fact that the technology is being developed with full openness of the standard and internal compatibility between devices from different manufacturers, it is practically doomed to success. The range of Bluetooth devices is 10-100 m (in the future it is planned to increase this distance to 300 m), while the presence of obstacles between the connected devices (walls, furniture, etc.) is allowed. At the moment, the data transfer rate is 721 Kbps, in addition, 3 voice signals can be transmitted. If the receiving device detects that the transmitter is closer than 10 meters, it will automatically reduce the transmission power. The device should also switch to low power mode as soon as the amount of traffic begins to decrease or stop altogether. Bluetooth devices are capable of linking together up to 256 devices, of which 8 are working at the same time (one in master mode and 7 in slave mode), and the rest are in standby mode.

Recently, there are more and more various devices using Bluetooth for data exchange. For example, recently, Anoto and Ericsson announced that they have developed a fountain pen that allows you to transfer notes made to her over mobile communications.

The technology uses small short-range transceivers, either directly built into the device or connected via a free port or PC card. Adapters work within a radius of 10 meters and, unlike IrDA, not necessarily in the line of sight, that is, there may be various obstacles or walls between the connected devices.

Bluetooth operates on the worldwide unlicensed frequency of 2.45 GHz (ISM band - Industry, Science, Medicine), which allows you to freely use Bluetooth devices around the world. The radio channel provides a speed of 721Kbps and transmission of 3 voice channels. The technology uses FHSS - frequency hopping (1600 hops/s) with spread spectrum. During operation, the transmitter switches from one operating frequency to another according to a pseudo-random algorithm. For full duplex transmission, time division duplex (TDD) is used. Isochronous and asynchronous data transfer is supported and easy integration with TCP/IP is provided. Time slots (Time Slots) are deployed for synchronous packets, each of which is transmitted on its own radio frequency.

The power consumption of Bluetooth devices should be within 0.1W. Each device has a unique 48-bit network address that complies with the IEEE 802 LAN standard format.

Some disadvantages of the technology.

The 2.4 GHz band is not licensed and can be freely used by everyone. Only the Federal Communications Commission (FCC) controls it, limiting the portion of the range that each device can use. The trouble is that these devices have become very numerous - ranging from wireless networks that support 802.11 and 802.11b standards and Bluetooth devices to microwave ovens! The commission is currently reviewing a request to increase the usable range for Home RF (a specification used in audio and video technology). This increase may affect other devices operating in this range, which are increasing in number. At the same time, the FCC stated that the use of an unlicensed frequency carries a definite risk and the possibility of interference and conflicts between devices is not excluded. Firms that support wireless networking technologies, including Bluetooth, are actively protesting against the increase in the range of Home RF, but what will happen is not yet

known.

Perspectives on Bluetooth.

Bluetooth technology is already confidently considered by many developers as a partner technology for universal radio communication for local area networks. Bluetooth is already active in the global market for new technologies as a catalyst for a number of other very important and promising networking initiatives. Bluetooth technology was nominated with Jini for the 1999 Best Technological Innovation Award (Discover magazine's annual awards).

In the next year, Bluetooth devices will be built into 80% of cell phones. Now there are transmitters connected via a PC card and USB. Ericsson has released a microphone and headphone kit that uses Bluetooth technology to communicate with a mobile phone, allowing you to talk on the phone without holding it in your hands. At the same CeBIT, Toshiba demonstrated a device that uses Bluetooth and the MPEG-4 video standard to conduct a video conference - the image from the camera was transmitted to a computer and then to another computer. NEC, followed by IBM, launched notebooks with built-in Bluetooth chips in mid-2000. Intel has already developed special software that will allow you to transfer computer files over Bluetooth radio networks. More and more companies are turning their attention to technology. Also, various peripheral devices have recently appeared, such as printers, keyboards, mice, working with the new technology.

In May 99, Ericsson began shipping the first Bluetooth toolkit for application developers. The kit costs about $450 (two motherboards, software modules, radio channel tests). The availability of Bluetooth specifications allows hundreds of developers to begin building prototype radio systems today.

1.4.2. WiFi technology

Wi-Fi technology is the most common wireless analogue of Ethernet.

Wi-Fi devices were designed for corporate users to replace traditional cable networks. The main benefit of such a replacement is that the cost of laying the network is greatly reduced by reducing the amount of manual work. A wired

network requires careful design of the network topology and manual laying of many hundreds of meters of cable. To organize a wireless network, you only need to install base stations at one or more points in the office (a central receiver-transmitter with an antenna connected to an external network or server) and insert a network card with an antenna into each computer. The main job of the installer is to ensure that there are no "dead" zones in the building or on the floor (reinforced concrete floors shield the signal, and then each floor needs its own station).

Devices using the 802.11b standard can transfer data at a maximum rate of 11 Mbps. (The 802.11a standard supports five times the speed - 55 Mbps.). In a word, the throughput of the 802.11 network is comparable to the throughput of a leased line of medium power (approximately class T1), and few organizations, not to mention individuals, can still afford such a communication channel.

However, initially the 802.11 standard was conceived as an alternative to Ethernet.

The 802.11b standard uses the 2.4 GHz frequency to transmit data.

The 802.11b standard was developed in the late 90s and finally approved in early 1999. In 2000, the first devices for data transmission based on it began to appear. It was far from the first wireless data transmission technology. Technically, the first means of digital wireless communication were still Popov-Marconi transmitters - these devices transmitted not an analog, but a discrete signal. The first wireless network devices appeared in 1990 and, although not widely used, were still widespread. The prototypes of such communication were text pagers and partly cell phones of GSM, CDMA and DAMPS standards. In Europe, text messages in the SMS format have become widespread, and two-way BlackBerry paging has been successfully used in the United States. In addition to transmitting data over the radio channel, other methods were also used - say, infrared devices.

In general, of all the prototypes of wireless transmission that had at least some prospect, 802.11b, aka Wi-Fi, was the most unpopular. Large companies and developed countries were experimenting with WAP and GPRS and were preparing to sell licenses for third generation cellular communications (in the UMTS

standard), which was designed to provide high-speed data transmission in cellular networks. The possibilities of the Bluetooth standard were widely discussed, with the help of which, as expected, personal devices and household appliances would be combined into a network. In a word, there were many alternatives to 802.11, the above list is far from complete. However, Wi-Fi still won.

The first consumers of the new technology were companies in Silicon Valley and other US technology centers. Demand for new devices grew, they were sold in ever-increasing quantities. The reason for the popularity is banal: the new standard was, probably by pure chance, optimal in terms of price-quality-convenience. Previous wireless technologies required users to install bulky devices that cost several hundred dollars each and complexly configured base stations. All such devices are small: a base station the size of a book, a laptop antenna board smaller than a credit card. A Wi-Fi base station was originally less than a thousand dollars, but now its price has dropped to three hundred, and antenna cards quickly began to sell for less than a hundred. Thus, it became possible to purchase the whole set for four hundred dollars, and, as the empirical experience of other markets shows, it is this price threshold that makes goods and services accessible to a wide range of consumers.

In recent years, everyone has become accustomed to the fact that real results turn out to be worse than forecasts. In the case of Wi-Fi, it was the opposite - demand forecasts for Wi-Fi devices were constantly revised upwards. In 2000, 6 million such devices were sold, in 2001 - 8 million, in 2004 - 28 million. In total: in four years, the new technology has gained about 40 million consumers, not counting the huge number of laptops that have appeared recently.

Now Wi-Fi is rapidly transforming from a high-tech novelty into an item without which everyday life is already unthinkable.

Devices for accessing the 802.11 network are also being created for other mobile devices: for example, all major manufacturers are developing dual-band (Wi-Fi and GSM) cell phones. Analysts are convinced that over time, everything that moves will be equipped with Wi-Fi access, moreover, we are talking about

completely new types of devices that will be created specifically for Wi-Fi capabilities.

1.4.3. Types of Wi-Fi connections.

There are two types of hardware in a wireless LAN: a client (usually a computer with a wireless network card, but it can be anything else) and an access point.

Connection "point-to-point".

All computers equipped with wireless cards are connecting to each other via a radio channel operating according to the 802.11b standard and providing an exchange rate of 11 Mbps, which is quite enough for normal operation.

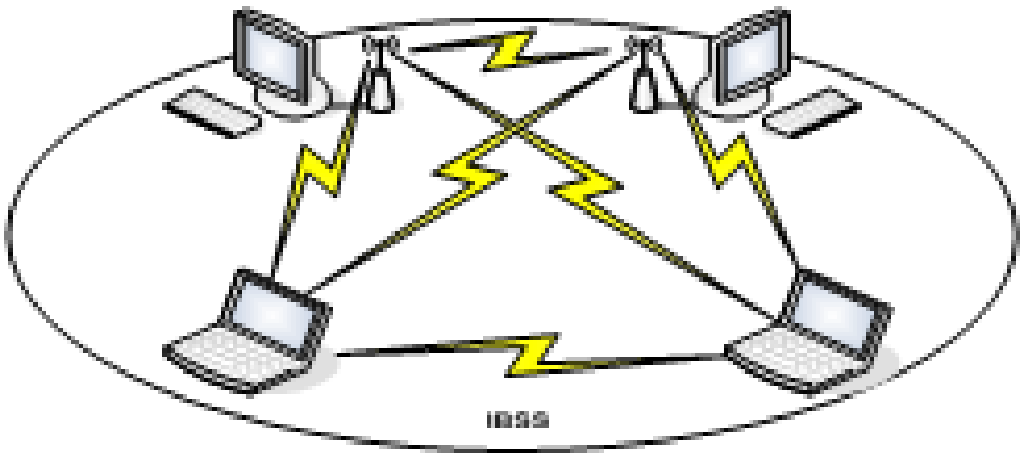


Figure 1.4. "Point-to-point"network

Access point-client connection.

All computers are equipped with wireless cards and connect to an access point. Which, in turn, has the ability to connect to a wired network.

This model is used when it is necessary to connect more than two computers. A server with an access point can act as a router and independently distribute the Internet channel.

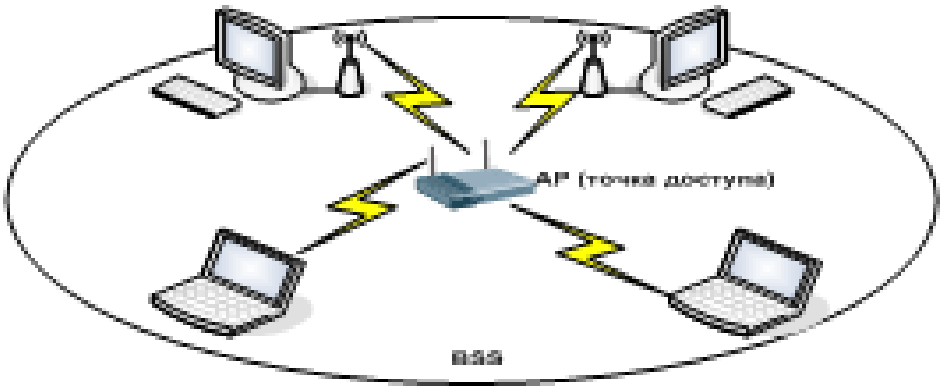


Figure 1.5. Infrastructure connection

Connection "Modem - router - access point - client". (Router-point).

The access point is included in the router, the router - in the modem (these devices can be combined into two or even into one, the so-called router). Now, on every computer in the Wi-Fi range that has a Wi-Fi adapter, the Internet will work.

Connection "Bridge" (bridge).

Computers are connected to a wired network. Access points are connected to each group of networks, which connect to each other via a radio channel. This mode is designed to combine two or more wired networks.

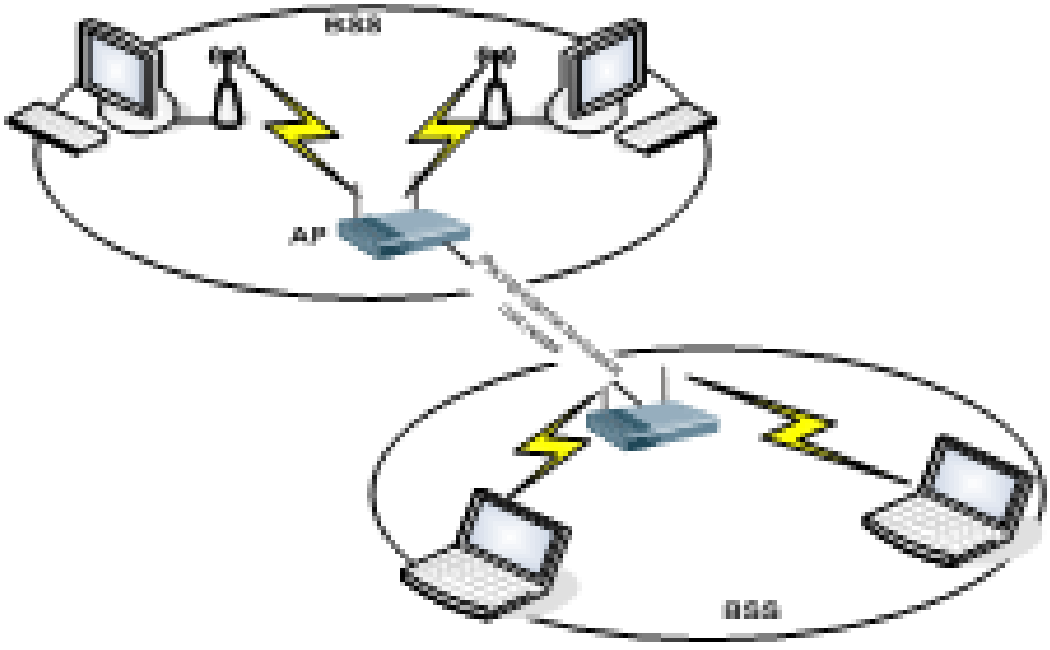


Figure 1.6. Connection bridge

Thus, I consider it most effective to use a wired Ethernet network for a local computer network, as well as to place wireless access points in the library premises. This will firstly enable students to prepare for studies and complete individual tasks on computers, while other students in the reading room itself will be able to search for information and work in Internet resources using their own smartphones or tablets.

1.5 Conclusion of the chapter 1

The chapter analyzes the peculiarities of the implementation of wired and wireless networks, and it was decided to use the wired Ethernet network for the implementation of a local computer network, as the most powerful in terms of data exchange, and also to place wireless access points in the notes of the library. This will firstly enable students to prepare for studies and complete individual tasks on computers, and other students in the reading room itself to search for information and work in Internet resources using their own smartphones or tablets.

CHAPTER 2
DESIGNING A WIRED COMPUTER NETWORK FOR A UNIVERSITY LIBRARY

2.1 Overview of network cables and cable system components

You can implement a wired local network either using twisted-pair cables, or using coaxial cables, or using fiber optic cables. Satellites, lasers, microwave radiation, etc. can also be used to transmit information, but such exoticism is beyond the scope of this course project.

2.1.1 Twisted-pair cables

Twisted pair is currently the most common transmission medium and is a pair of twisted wires. The cable, made of several twisted pairs, is usually covered with a hard plastic shell that protects it from the effects of the external environment and mechanical damage. The diagram of the twisted pair is presented in Fig. 2.1.

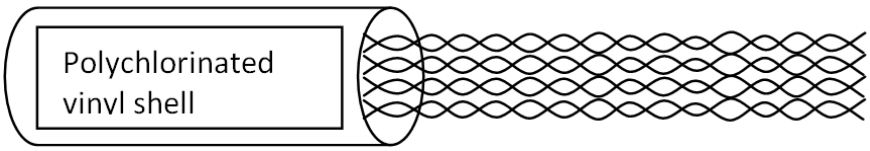


Figure 2.1. Twisted pair cable

Under normal conditions, twisted pair cable supports data transfer rates up to 100 Mbps. However, a number of factors can significantly reduce the data transfer rate, such as data loss, cross-connection, and the influence of electromagnetic radiation.

To reduce the influence of electric and magnetic fields, shielding is used (twisted pair cable is covered with foil or braid). But after shielding the twisted pair, the attenuation of the signal increases to a large extent. Signal attenuation refers to the weakening of the signal during transmission from one point of the

network to another. Shielding changes resistance, inductance, and capacitance in such a way that the line becomes prone to data loss. Such losses can make twisted pair an undesirable and unreliable transmission medium. Both cables are used to carry data over several hundred meters.

Five standard categories of twisted-pair cable are being introduced in accordance with the specifications of the Electronics and Telecommunications Industries Association. Only Unshielded Twisted Pair (UTP) is used in cable categorization.

- Category 1 cable is used for voice data transmission. Since the early 1980s, the CAT 1 cable has been used primarily for telephone line wiring. Category 1 cable is not certified for any type of data transfer and is generally not considered a medium for digital data transfer.

- The cable of the second category is used to transfer information at a speed of no more than 4 Mbps. This type of wiring is typical for networks with legacy network topologies that use a token passing protocol. The cable is clocked at 1 MHz.

- Category 3 cable is mainly used in legacy Ethernet 10base-T LANs and is certified for data transfer rates up to 16Mbps. The cable is clocked at 16 MHz.

- Category 4 cable is used as a medium for connecting networks with ring architecture or 10base-T/100base-T architecture. The CAT 4 cable is certified for data transmission at speeds up to 16Mbps and consists of four twisted pairs. Clocked at 20 MHz.

- Category 5 cable is the most commonly used for Ethernet. The cable supports data transfer rates up to 100Mbps and is used in networks with 100base-T and 10base-T architecture. The cable is clocked at 100 MHz.

2.1.2 Coaxial cable

Such cable is a widespread and fairly convenient data transmission medium. The name of the cable was due to the fact that it consists of two conductors. One conductor (solid or twisted core) is shielded by the second, which can also be solid

or twisted. Conductors are usually separated by a layer of dielectric material. The cable itself is covered with a plastic sheath. Coaxial cable is better protected from interference and allows you to increase the length of the network segment. 10base-2 networks using coaxial cable - approximately 180 m. 2.2 and 2.3 shows a coaxial cable in section.

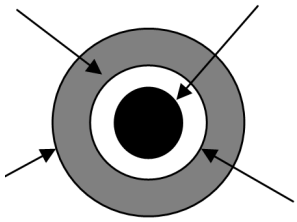


Figure 2.2. Cross section of a coaxial cable.

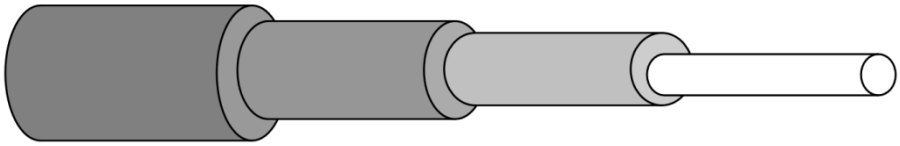


Figure 2.3. Longitudinal section of a coaxial cable.

With an increase in the diameter of the coaxial cable, the throughput increases. However, at the same time, the cost of wiring from such a cable increases, since special tools must be used. Characteristic properties of coaxial cable:

- It is less affected by noise.

- It consists of two concentric conductors separated by a layer of dielectric material.

- The coaxial cable impedance can be 75 ohms (½ inch thick cable) or 50 ohms (3/8 inch thick cable).

2.1.3 Fiber optic cable

It is a thin and flexible medium that allows data to be transmitted in the form of light waves over a glass "conductor" or cable. Fiber-optic communication lines are used at distances over one kilometer. Their characteristic feature is high

security against unauthorized connection (which is not surprising, since no electrical signals are used for data transmission). There are two types of cable: singlemode and multimode.

Fiber optic cable device

Coaxial and fiber optic cable are almost the same. The core of the latter consists of a weave of thin glass fibers and is enclosed in a plastic shell that reflects light back to the core. The cladding is covered with a concentric protective plastic layer. On fig. 2.4 shows the structure of a fiber optic cable.

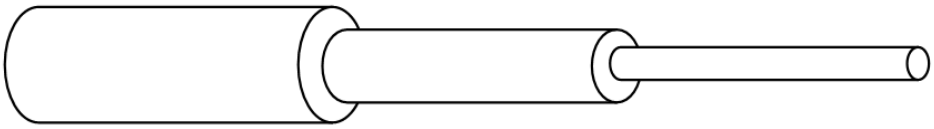


Figure 2.4. Fiber optic cable

Singlemode and multimode cable

In a relatively thin fiber optic channel, light will propagate along the longitudinal axis of the channel. In physics textbooks, this effect is mentioned in the following formulation - "light pulses propagate in the axial (axial) direction." This is exactly what happens in a single-mode cable (see Figure 2.6).

However, the benefits of this type of transmission are limited. In order to eliminate such restrictions, a similar cable began to be produced. But here another problem arose - the rays of light tend to enter the channel at different angles, the waves travel different distances and arrive at the recipient at different times. This effect, illustrated in Fig. 2.7 is called modal dispersion.

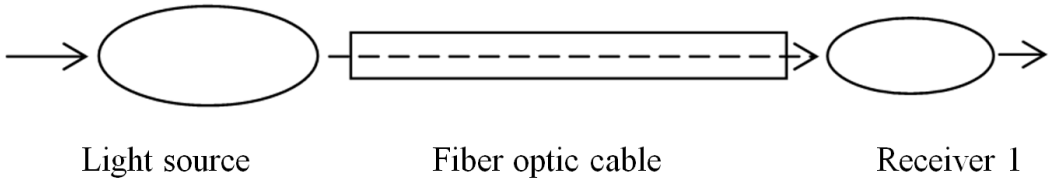


Figure 2.5. The principle of operation of a fiber optic cable.

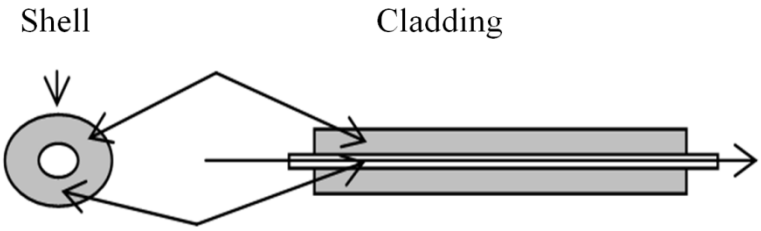


Figure 2.6. In a thin cable, light travels along a single-mode path.

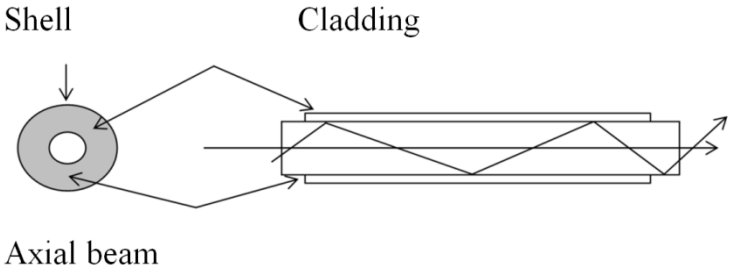


Figure 2.7. In a thick cable, non-axial beams are subject to modal dispersion

The greater the number of light modes in a channel, the narrower the bandwidth. In addition to the fact that different pulses reach the receiver at almost the same time, the increase in dispersion leads to pulse overlap and the introduction of the receiver into a "delusion". As a result, the overall throughput is reduced. A single-mode cable transmits only one mode of light pulses. The data transfer speed reaches tens of gigabits per second. A single-mode cable is able to support several gigabit channels simultaneously, using light waves of different lengths for this. Therefore, the throughput of multimode fiber optic cable is lower than that of single mode.

The simplest way to reduce dispersion is to level the fiber optic cable. As a result, the light beams are synchronized in such a way that the dispersion on the receiver side is reduced. Dispersion can also be reduced by limiting the number of light wavelengths. Both methods reduce dispersion to some extent.

In the US, “62.5/125” multimode cable is widely used. The designation "62.5" corresponds to the diameter of the core, and the designation "125" corresponds to the diameter of the cladding (all values are given in microns). Of the single-mode cables, the cables marked 5-10 / 125 are common. Bandwidth is

usually given in MHz/km. A rubber band is a good model for the relationship between bandwidth and transmission distance—bandwidth narrows as distance increases (and vice versa). In the case of data transmission over a distance of 100 meters, the bandwidth of the multimode cable is 1600 MHz at a wavelength of 850 nm. The analogous characteristic of a single-mode cable is approximately 888 GHz.

The main characteristics of fiber optic cable:

- Absolute immunity to electromagnetic radiation.

- Data transmission up to 10 km is possible.

- In laboratory conditions, it is realistic to achieve transfer rates of up to 4 Gbps.

- Light emitting diode or laser can be used as light source.

2.1.4 Overview of cabling and Ethernet layout

There are four main cabling schemes used in an Ethernet environment: Thick Ethernet, Thin Ethernet, Twisted Pair Ethernet, and Fiber Ethernet. Differences in their specification, layout, and number of nodes result in differences in the performance of specific Ethernet systems.

The transfer rate for all types of Ethernet is the same and is 10 Mbps. The connection diagram for each type can be either a bus or star configuration.

Thick Ethernet - 10Base5

- data transmission - 10 Mbps, single-band;

- connection diagram - in the form of a bus;

- the type of cable used in a thick Ethernet environment - typically wide coaxial (4" diameter);

- maximum segment length - 500 m;

- thick Ethernet cable segments must be terminated with 50 ohms;

- repeaters and other devices can be used to extend the segment, as well as cable hubs;

- workstations and network devices are connected to the network through external transceivers, or MAUs;

- to connect the transceiver to the cable medium, a vampire tap connector is used;

- up to 100 workstations or LAN devices can be connected to a thick Ethernet segment;

- thick Ethernet cable connection system provides more reliable protection against electrical interference.

Thin Ethernet

- data transmission - 10 Mbps, single-band;

- connection diagram - in the form of a bus;

- maximum segment length - 185 m;

- thin Ethernet cable segments must be terminated with 50 ohms;

- repeaters and other devices can be used to extend the segment, as well as cable hubs;

- workstations and network devices are connected to the network through external transceivers, or MAUs. They can be external or internal to network cards;

- to connect the transceiver to the cable medium, a BNC-T type adapter is used;

- no more than 30 workstations or network devices can be connected to one thin Ethernet segment by means of transceivers.

Ethernet over twisted pair - 10Base-T

- data transmission - 10 Mbps, single-band;

- connection scheme - in the form of a star;

- the cable type, used in this environment is unshielded twisted pair, levels 3, 4 and 5;

- central cable hubs are used to connect individual cables - 10Base-T taps to workstations and LAN devices;

- maximum segment length per UTP Ethernet drop cable - 100 m. This value may vary depending on the manufacturer of a particular cable hub and network adapter;

- UTP-based Ethernet cards usually come with internal UTP transceivers. In the absence of internal UTP transceivers, an appropriate external device can be selected, with which standard boards for thick and thin Ethernet can work in the UTP scheme;

- as a network card connector, a RJ45 modular jack is usually used with positive and negative receive and transmit pairs based on 8-pin connections;

- UTP cable connections are easy to install and maintain, their relative cost is low. They are susceptible to electrical interference and must be installed in accordance with the specification.

Fiber Optic Ethernet 10Base-F

- data transmission - 10 Mbps, single-band;

- connection scheme - in the form of a star;

- typically 50 or 100 micron fiber optic cable is used;

- to connect individual 10Base-F drop cables to workstations and LAN devices, central fiber-optic cable hubs or multiport repeaters are used;

- maximum segment length per fiber optic Ethernet drop cable - up to 2100 m;

- fiber optic cable provides maximum protection against interference from power sources.

Ethernet cable connectors.

Depending on the type of Ethernet, different types of cable connectors are used to connect to network cards, transceivers, repeaters, and hubs.

All thick Ethernet devices are equipped with a 15-pin AUI or DIX connector. A workstation or other device is connected to the Ethernet transceiver using a device interface cable that connects the DIX connector on the Ethernet network card to the DIX connector on the transceiver. The transceiver, in turn, is connected to the coaxial Ethernet cable either using connectors or using a vampire tap that bites directly into the cable. A variety of coaxial cable connectors are used to connect two coaxial cables.

To connect Ethernet cables directly to a jack on a workstation or other device in a thin Ethernet environment, use the BNC T-connector. It should be noted that the connector is often the source of various problems with a particular cable segment in a thin Ethernet environment. To avoid them, you need to check if it is properly connected to the coaxial cable.

Ethernet 10 Base-T is used for connections between 10Base-T NICs and smart cable hubs based on UTP Ethernet, standard phone type RJ45 connector.

On a conventional cable hub, quite often there are various Ethernet-type connectors for organizing connections between different types of networks. For example, on the back panel of a conventional 10 Base-T cable hub, you can very often see a DIX connector for connecting AUI thick Ethernet, as well as a BNC connector for connecting standard thick Ethernet. This allows you to integrate systems of various types of Ethernet in order to organize their joint work. It is very common to have BNC, RJ45, and AUI connectors on the same Ethernet board.

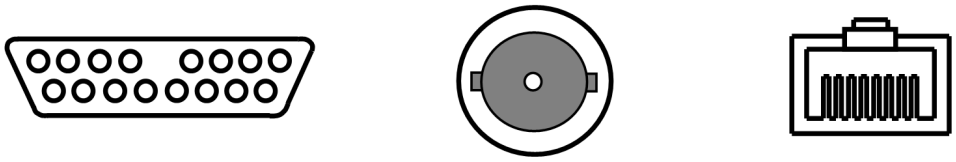


Figure 2.8. Main Connectors for Various Ethernet Environments

On fig. Figure 2.8 shows the main types of connectors found in various types of Ethernet systems, including DIX thick Ethernet connector, thin Ethernet connector, and RJ45 10Base-T connector for UTP.

2.2 Analysis and selection of network equipment

When designing an Ethernet local area network, the following equipment will be used:

- network adapter boards;
- active concentrators;
- server;

- uninterrupted power supply unit;
- bridge.

2.2.1 Network adapter cards

They are like a physical interface between PC and the transmission medium.

Network adapter cards are designed for:

- preparation of data coming from a PC for transmission over a network cable;
- data transfer to other PCs;
- data flow control between PC and cable.

Before data can be sent to the network, the network adapter card must convert it from a form that the PC can understand to a form that can be transferred over the network cable.

The NIC accepts parallel data and organizes it for serial, bit-by-bit transmission. This process is completed by the conversion of digital data into the form of electrical or optical signals.

The main elements of network adapters are:

- transceiver (transceiver);
- Network Controller;
- microprogram memory;
- RAM.

There are two types of Ethernet network adapters: 10 Mbps and 100 Mbps. They are known for their high reliability, and cable and adapter problems are easy to diagnose.

2.2.2 Network servers

The server processes and stores the basic information located in the computer network. Due to the variety of information used and the types of its processing, there are various types of servers, the most common of which is the file server. The last is a computer connected to a network used to store data files accessed by workstations. From the user's point of view, the file server is viewed

as a central archive that stores information common to all workstations. Centralized storage of data allows more efficient control over data, as well as access to them by users.

In more complex computer networks, in addition to the file server, there may be other types of servers, for example: a print server, a database server, a Web server, a mail server, etc.

In terms of equipment composition, servers are not much different from workstations, however, higher requirements are imposed on the equipment itself. This is due to the fact that the file server must quickly process many requests from all workstations. With the increase in the number of workstations and the complexity of the tasks being solved, the requirements for the server in terms of performance, memory size, and reliability increase significantly.

The server must be equipped with an uninterruptible power supply (UPS) to ensure normal network operation and to prevent information loss during a sudden power outage. The UPS uses the battery to keep the server running long enough to save data and shut down normally.

Network servers must be able to grow their resources. In this regard, servers are designed taking into account the possibility of installing more powerful or additional processors, RAM and hard drives.

2.2.4 Hubs

Nowadays, the hub is becoming one of the standard components of networks. And in networks with a star topology, it serves as a central node (Fig. 2.9).

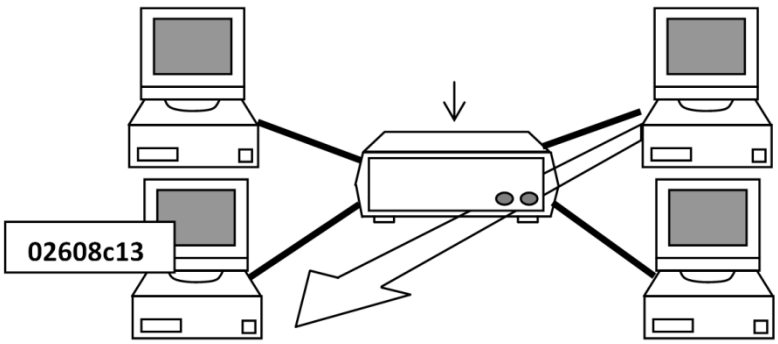


Figure 2.9. Hub - the central node in a network with a star topology

There are active and passive hubs.

Some types of hubs are passive, such as mounting panels or switch boxes.

Hybrid hubs are hubs that can be connected to different types of cables (Figure 2.10).

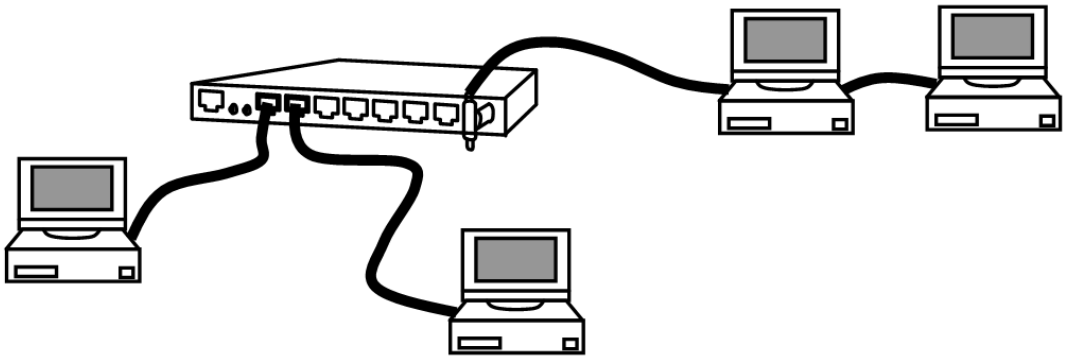


Figure 2.10. Hybrid hub

A bridge consists of the hardware and software required to link two separate LANs, or subnets, located in the same location into one Internetwork. The simplest type of bridge parses the 48-bit destination address field of a packet and compares that address to a table that lists the addresses of all workstations on that network segment. If the address does not match any of those specified in the table, the bridge forwards the packet to the next segment. These simple bridges continue to forward packets, hop by hop, until they reach the network segment containing the computer with the specified destination address. Bridges involved in this process of parsing address tables and forwarding packets are called transparent bridges. This method is used in all Ethernet bridges and in some bridges in Token Ring networks. The principle of operation of this type of bridge is shown in Fig. 2.11.

Some bridges create their own network address tables. Such bridges verify the source and destination addresses of each packet sent to the LANs to which they are connected. Then they build tables of addresses that list the addresses of the senders of packets on their network that have a number corresponding to this network. After that, the bridges check the addresses of the recipients of the packets with the addresses of the senders. Having found a match, the bridge filters the packet and sends it further along the network; the destination station recognizes its

address and copies this packet into its memory. If there is no match, the packet is advanced, i.e. it is allowed to travel across the bridge to the next network segment. Broadcast and multicast packets are always forwarded because their destination address fields are never used as source addresses.

Bridges "do not understand" higher level protocols and are not associated with them. They operate at the MAC sublayer of the OSI data link layer and are far removed from upper layer protocols such as XNS and TCP/IP. If both networks conform to the IEEE 802.2 logical channel control standards, then the bridge can link them regardless of differences in media and access methods. As will become clear from the discussion below, this means that businesses can bridge their Ethernet, Token Ring, and 802.3 LAN networks using 100BaseX Ethernet over data class twisted pair, 100BaseT Ethernet over unshielded twisted pair, or thin coaxial cable.

2.3. Network design

The analysis of the plan of the reading room of the university library was carried out. This room is open and spacious, but only has tables for working with books, magazines or computers. However, the existing Wi-Fi network access points do not cover the entire hall and it is difficult to work from a netbook or smartphone, the connection is often lost. Also, the hall is used most often for various gatherings or cultural events. Students rarely work in the reading room. Especially foreign students, who often simply do not have their own netbooks.

Images of the reading room are shown in fig. 2.11.

Figure 2.11. Image of the university library reading room

In the work, it is proposed to arrange 14 computers in two rows near the windows, and one separately near the back wall of the hall with a printer and a scanner.

To create a computer network, we need good computers. For the connection, I chose Ethernet technology, namely 1000BASE-LH - a development that uses optical fiber for data transmission at a speed of 1000 Mb/s.

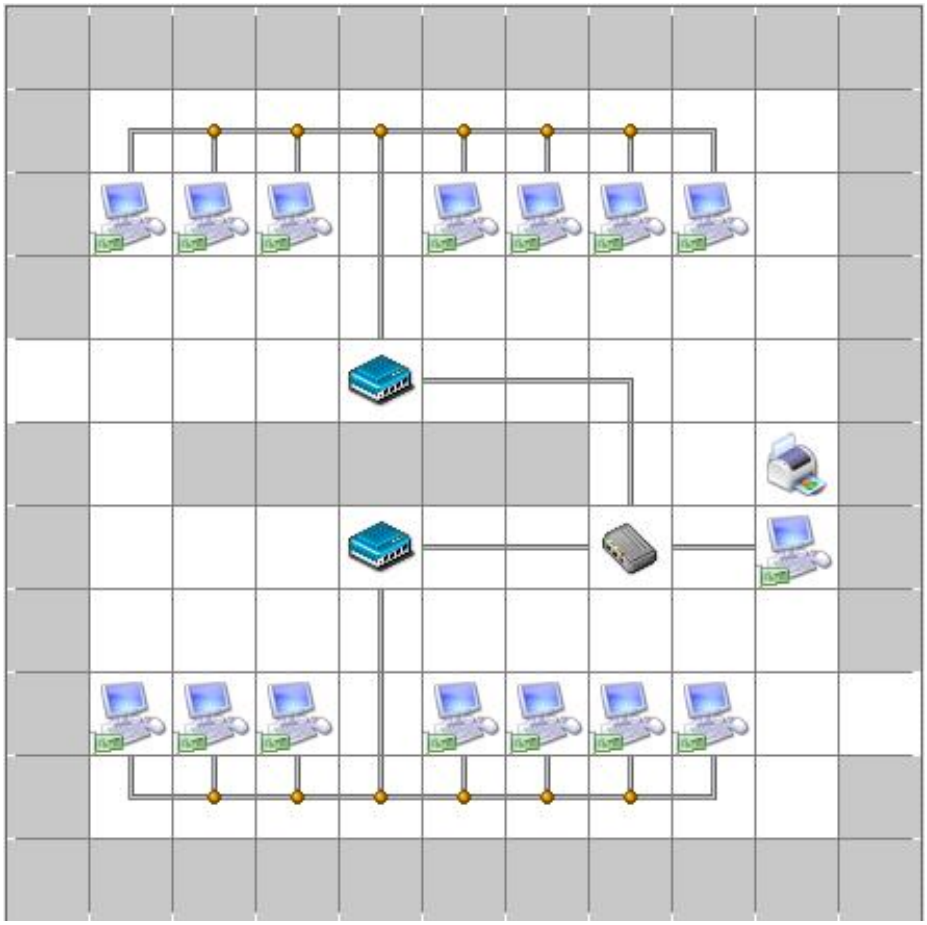


Figure 2.12. Room plan

On fig. 2.12 shows:

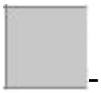
 - Computer with installed software, also built-in network card;

 - Switch;

 - Hub (he is also a repeater, a branch, a concentrator);

 - Fiber optic cable;

 - Printer (Scanner);

 - Wall.

Required equipment

For the server computer I took:

- System unit HP Pavilion p6-2227er
- RAM, 4GB
- Processor type Core i7-3770
- The clock frequency of the processor is 3.4 GHz
- 1 TB hard drive
- Video card GeForce GT630 2GB
- Drive type 1 DVD+-RW/DL
- Network card (D-link)

Client computers

- System unit Lenovo IdeaCentre H430
- Windows 7 operating system
- Processor type Celeron G530
- The clock frequency of the processor is 2.4 GHz
- RAM 4 GB

Hard disk (HDD) 500 GB

Graphics controller GeForce GT620

- Video memory 1 GB
- Drive type 1 DVD+-RW/DL
- network card (D-link)

The following cables were used to connect the computer to the network:

- Fiber optic cable.

Additional equipment is required:

Hubs/switches, I suggest one of the following

- Asus GX-D1081, 8 ports.
- Asus GX-D1081 8 ports.
- Hub Gembird 4-Port Video Splitter GVS-124

Gembird 4-Port Video Splitter GVS-124.

2.4 Calculation of network bandwidth

We will accept the following initial data for calculation:

1. total network length S = 87 m,
2. modulation speed B = 100 Mbit/s,
3. number of stations M = 15
4. the speed of signal propagation along the communication cable $V = 3 \cdot 10^5$ km/s,
5. the maximum number of repeaters between two stations np=1,
6. maximum delay of one repeater in bits Lp = 15 bits.
7. the type of protocol from which the average length of the information part of the frame is set Ly = 1520 bits (Ethernet),
8. the average length of the service part of the frame protocol Lc = 320 bits,
9. the law of distribution of the lengths of the service part of the frame is deterministic,
10. the law of distribution of the lengths of the information part of the frame is exponential),
11. the average value of the intensity of messages received in total from all stations $\lambda = 560$ 1/s.

Based on the specified initial data, we will calculate the delay time in the network and determine its bandwidth.

1. Signal propagation time by cable between two stations, the distance between which is the greatest:

$$\tau p = S/V = 87/(3 \cdot 10^8) = 29 \text{ us}$$

2. Maximum signal delay time in repeaters

$$\tau pт = Np \text{ x } (Lp/B) = 1 \text{ x } 15/(10^8) = 1{,}5 \text{ x } 10^{-7} \text{ c} = 0{,}15 \text{ us}$$

3. Full signal propagation time over the network (maximum)

$$\tau = \tau p\tau + \tau p = 29 + 0{,}15 = 29.1 \text{ us}$$

4. The duration of the information part of the frame

$$\tau u = Lu/B = 1520/(100 \times 10^6) = 152 \cdot 10^{-7} c = 15{,}2 \text{ us}$$

5. The duration of the service part of the frame

$$\tau c = Lc/B = 320/(100 \times 10^6) = 32 \times 10^{-7} \text{ c} = 3{,}2 \text{ us}$$

6. Total Frame Duration

$$\tau cp = \tau u + \tau c = 15{,}2 + 3{,}2 = 18{,}4 \text{ us}$$

7. Coefficient of variation in message frame transmission time

$$\nu cp = \sigma cp/\tau cp = \sqrt{\sigma_u^{\,2} + \sigma_c^{\,2}/\tau_{cp}^{\,2}} = \sigma u/\tau cp = 15{,}2/18{,}4 = 0{,}826$$

8. Average intensity of messages received from each station

$$\lambda cp = \lambda/M = 560/14 = 40 \text{ s}^{-1}$$

9. Total network load factor

$$R = \lambda \times \tau cp = 560 s^{-1} \times 18{,}4 \times 10^{-6} \text{ s} = 0{,}01$$

10. Long-range coefficient taking into account the delay time in repeaters

$$\alpha = \tau/\tau cp = 0,36/18,4 = 0,02$$

11. Relative message delivery delay time Wn

$$Wn = \frac{tn}{\tau cp} = R(1 + V^2 cp)\frac{1 + \alpha(1 + 2e)}{2[1 - R(1 + \alpha(1 + 2e))]} + 1 + \frac{\alpha}{2}$$

$$Wn = 0,01(1 + 0,826^2)\frac{1 + 0,02 \cdot 6,44}{2[1 - 0,01(1 + 0,02 \cdot 6,44)]} + 1 + \frac{0,02}{2} = 1,0196$$

12. Message delivery time

$$tn = W \text{ x } \tau cp = 1,0196 \text{ x } 18,4 = 18,8 \text{ us}$$

13. Network bandwidth

$$C = \frac{1}{1 + 6,442} = \frac{1}{1 + 6,44 \cdot 0,059} = 0,72$$

14. The maximum allowable value of the total intensity at which the load is equal to the channel bandwidth

$$\lambda max = \frac{C}{\tau cp} = \frac{0,72}{18,4 \cdot 10^{-6} c} = 49130\ s^{-1}$$

15. Minimum delivery delay time (when R=0)

$$t_{n\ min} = (1 + \frac{\alpha}{2}) \cdot \tau cp = (1 + \frac{0,02}{2}) \cdot 18,4 = 18,58 \text{ us}$$

2.5 Conclusion of the chapter 2

The chapter analyzes the features of network cables and components of the cable system. It is proposed to use optical fiber cable to organize the local network of the university library. Methods of connecting computers to the hub and server were also analyzed. A drawing of the room plan was made and the location of the computer network elements on it was indicated. Variants of network elements are offered, including computers, servers, hubs, etc. Calculations of the bandwidth of the projected network were carried out.

CHAPTER 3
DESIGNING A WIRELESS NETWORK FOR A UNIVERSITY LIBRARY

3.1 Selection of network elements

To create a wireless network, you will need to select an access point and network adapter.

In order to connect the computer to the network, a network adapter is required. There are many types of network adapters. They differ from each other by the manufacturer, technical features and type of interface. Adapters with PCI and USB interfaces manufactured by D-Link, ASUSTek, 3Com, SureCom, Trednet, etc. are most widely used. In addition, you can often find adapters with additional devices, such as a flash or HDD drive.

Network adapterof type: “D-Link Air Xpert DWL-AG650” (Fig. 3.1) is designed for laptops and portable computers equipped with the appropriate connector (32-bit CardBus slot).

Figure 3.1. B-Link DWA-AG650 adapter

The peculiarity of this adapter is that it is a universal device capable of operating in wireless networks IEEE 802.11 a, and lg standards. This means that by connecting it to a laptop, you can not worry about the incompatibility of any standards.

On the basis of such a wireless adapter, transfer speeds of up to 54 Mbit/s can be achieved in the case of application of IEEE 802.1 la and IEEE 802.1 lg standards and 11 Mbps on IEEE 802.1 lb networks.

In terms of security, this adapter supports the WPA security protocol using TKIP protocol and authentication using a RADIUS server. It also supports the older WAP (Wareless Access Protocol) security protocol.

The D-Link DWL-G122 wireless network adapter (Fig. 5) is designed to work in computers equipped with a USB interface.

Figure 3.2. D-Link DWL-G122 Wireless Adapter

Such an adapter can operate in IEEE 802.1 lg and IEEE 802.11b networks, while providing data transfer rates up to 54 and 11 Mbps, respectively.

To connect the device, a high-speed USB 2.0 port is used, which is present in almost any computer. This means that by connecting a device to the port, you can immediately start working on the network.

The adapter supports the WPA security protocol using the TKIP protocol and authentication using a RADIUS server. In addition, the device supports the older WAP security protocol.

Shown in fig. 3.3 Wireless PCI Adapter 3Com l l a / b / g (3CRDAG675) is designed for installation in the PCI slot of a personal computer.

Figure 3.3. Wireless PCI Adapter 3Com l l a / b / g

A feature of this adapter is the ability to work in networks of standards IEEE 802.1 la, IEEE 802.1 lb and IEEE 802.1 lg, which makes it absolutely universal in use.

This adapter comes with a host of additional security and authentication features, making it one of the most secure wireless adapters on the market. In particular, it supports WPA, AES (128-bit key) and WEP (40/64-, 128- and 152-bit key) encryption protocols, MD5, 802.1x and EAP authentication mechanisms.

Separately, we can note the fact that the adapter has autonomous load balancing mechanisms (Autonomous Load Balancing), which allows you to achieve the maximum data transfer rate and a dynamic rate shifting mechanism (Dynamic Rate Shifting), which allows you to select the connection speed depending on the current traffic in the network and conditions environment.

Access points used for designing wireless networks can be divided according to the connection method: via a USB port and an Ethernet connection port - RJ45. Access points connected via the RJ45 port are the most successful, as they are the easiest to set up and manage, and also have a higher transfer rate to the local network.

The access point made on D-Link DWL-2100AP (Fig. 3.4) is a common device that combines not only the properties of an access point, but also a wireless bridge, client, and repeater. This fact makes this device universal for organizing the operation of a wireless network.

Fig 3.4. Access point DWA-2100

This device supports WPE and WPA security protocols. User authentication occurs using a RADIUS server. In addition, if some network clients do not support authentication using a RADIUS server, then the D-Link DWL-2100AP is ready to provide a WPA Pre-Shared Key mechanism that allows such users to receive a temporary encryption key every time they connect to an access point.

It should be noted that there is a built-in DHCP mechanism that allows you to assign IP addresses to computers connected to a wireless network.

Access points can be indoor (in door) and all-weather (out door) execution. To create a wireless network indoors, use the indoor version of the device. It has a lower cost and, as a rule, a greater aesthetic appearance. Such access points work within one or more rooms. In open areas (line of sight), operation at a distance of up to 300 meters is possible using standard omnidirectional antennas.

All-weather access points are designed to create a radio network between buildings. Depending on the types of antennas, such devices are capable of organizing communication channels at a distance of about 3-5 km. The maximum range of the wireless communication channel increases markedly when using amplifiers. In this case, the length of the radio channel reaches 8-10 km.

To design a wireless network for this computer class, the best option would be to use a room access point operating on Wi-Fi technology, an “Access Point-Client” connection, connected in turn to a wired Ethernet network that has Internet access and works according to one of the wireless standards. IEEE 802.11g,b,n

communications.

3.2 Hardware setup

To create a network, the first step is to install and configure an access point and network adapters.

To create a network, a D-link DAP-1353 access point and D-link DWA-140 wireless adapters were selected. This equipment fully complies with the desired characteristics and has a low cost, meets modern standards.

To connect the access point to the network, follow these steps:

• Plug the power adapter into the power connector on the back of the DAP-1353 and then plug the other end of the power adapter into a wall outlet or surge protector. The Power indicator will light up.

• Connect Ethernet cable to the LAN port and to the Computer. The LAN indicator will light up indicating a valid Ethernet connection.

To configure on the computer to which the access point is connected, you need to download a web browser and enter the ip address of the device by default, the address http://192.168.0.50. (The address given to the access point when connecting it to an existing wired network http://192.168.1.18).

If the authorization page does not open, you need to set the IP address in the range from http://192.168.0.1 to http://192.168 .0.49; use mask 255.255.255.0

After configuration, a window will open: the access point authorization page where you must enter the username and password to log in to the system (by default, the username is admin, there is no password).

After entering data for authorization, a window will open that contains information about the model, software version, system timer, operating time, operating mode, MAC address and IP address.

To switch to the setup mode, select the item Basic Settings - Wireless in the side menu. And do the following:

• In the wireless settings window that opens, you need to select the operating

mode (“Mode” item), in our case, Access Point - Access Point.

• Set the network name (Network Name item (any name can be set, set “wi-fi network class 233)”.

• Select the width of the adapter's channel ("Channel Width") - select "20 mhz" since the access point is located close to the computers.

• Set a user authorization password when connecting to a Wi-Fi network (“WPA Mode” item) - select WPA2 only and set the password 123456789. Click the Save button.

The resulting settings should match the figure below.

• To apply the settings, you need to restart the access point, for this you need to go to the Configuration menu, select the Save and Activate item.

After that, the access point takes 59 seconds to apply the settings.

As a result of the performed operations, the device is completely ready for operation.

After setting up the access point, you need to start configuring the computers that will be on the network.

To connect the adapter, do the following:

• Connect the adapter to the USB port.

• Insert the CD (included with the device) into the CD-ROM drive. The installation wizard will start automatically.

For correct operation, you need to install the driver, for this you need to select the Install Driver item.

After selection, the license agreement window will open, in which you need to click on the “AGREE” button to confirm.

Next, you need to follow the steps of the wizard:

Step 1. Select the installation language. Click "Next".

Step 2. When the welcome window appears, click “Next”.

Step 3. Use the driver installation folder. (default). Click "Next".

Step 4. Enter the name of the folder where the driver will be located. Click "Next".

Step 5. Wait for the installation wizard to complete. Click "Next".

Step 6. Select the type of connection that will be established between the adapter and the access point. Select the SSID (enter the key manually). Click "Next".

Step 7. Enter the name of the wireless network: "Class 233 Network". We press "Next".

Step 8. Select a wireless network from the list of available networks. We press "Next".

Step 9. Enter the encryption key that was specified in the access point. (123456789). We press "Next".

Step 10. We complete the adapter installation wizard. Click "Finish"

Upon successful installation, the wireless network icon will appear on the taskbar by clicking on which the D-Link Connection Manager program will open, in which you can make sure you are connected to the network, see the signal strength, or connect to another network.

3.3 Conclusion of the chapter 3

The chapter analyzes the main elements for a Wi-Fi network. Specific types of these elements are selected, including network adapter, wireless adapter, PCI adapter, and access points. Features and main stages of setting up such a network are considered. This network should be effective for working in the library hall.

CHAPTER 4
LIFE SAFETY, BASICS OF LABOR PROTECTION

4.1 Safety issues when laying networks

Before starting work, you should make sure that the wiring, switches, sockets, with which the equipment is connected to the network, are in good condition, that the computer is grounded, that it is working,

In order to avoid damage to the insulation of wires and the occurrence of short circuits, it is not allowed to: hang anything on wires, paint over and whitewash cords and wires, lay wires and cords behind gas and water pipes, behind heating system batteries, pull out the plug from the socket by the cord, force must be attached to the plug body.

To avoid electric shock, it is forbidden: to frequently turn on and off the computer without the need, to touch the screen and to the back of the computer blocks, to work on computer equipment and peripheral equipment with wet hands, to work on computer equipment and peripheral equipment that have violations of the integrity of the case, violations of wire insulation, faulty indication of power on, with signs of electrical voltage on the case, put foreign objects on computer equipment and peripheral equipment.

It is forbidden to clean the electrical equipment from dust and dirt while energized.

It is forbidden to check the operability of electrical equipment in premises unsuitable for operation with conductive floors, damp, which do not allow accessible metal parts to be grounded.

It is unacceptable to carry out repairs of computer equipment and peripheral equipment under voltage. Repair of electrical equipment is carried out only by specialist technicians in compliance with the necessary technical requirements.

To avoid electric shock, when using electrical appliances, do not touch any pipelines, radiators, metal structures connected to the ground at the same time.

Take special care when using electricity in damp rooms.

Safety requirements in emergency situations

If a malfunction is detected, immediately turn off the power to the electrical equipment, notify the administration. Continuation of work is possible only after the malfunction has been eliminated.

If a broken wire is found, it is necessary to immediately inform the administration about this, take measures to exclude people from contact with it. Touching the wire is life-threatening.

In all cases of electric shock to a person, a doctor is immediately called. Before the arrival of the doctor, it is necessary, without wasting time, to start providing first aid to the victim.

It is necessary to immediately start artificial respiration, the most effective of which is the mouth-to-mouth or mouth-to-nose method, as well as external heart massage.

Artificial respiration to the person affected by electric current is performed until the arrival of a doctor.

It is forbidden to have flammable substances in the workplace.

In the premises it is prohibited:

a) light a fire

b) turn on electrical equipment if the room smells of gas;

c) smoke;

d) dry something on heaters;

e) close the ventilation openings in electrical equipment

Sources of ignition are:

a) a spark when discharging static electricity

b) sparks from electrical equipment

c) sparks from impact and friction

d) open flame

In the event of a fire hazard or fire, the personnel must immediately take the necessary measures to eliminate it, at the same time notify the administration about the fire.

Safety requirements at the end of work

After finishing work, it is necessary to de-energize all computer equipment and peripheral equipment. In the case of a continuous production process, it is necessary to leave only the necessary equipment switched on.

4.2 The issue of lighting when working at a computer

Among the factors of the external environment that affect the human body during work, light occupies one of the first places. After all, it is known that almost 90% of all information about the environment a person receives through the organs of vision. During the implementation of any work, eye fatigue mainly depends on the intensity of the processes accompanying visual perception. Such processes include adaptation, accommodation and convergence.

Adaptation – adjustment of the eye to changing lighting conditions (illumination level).

Accommodation is the adaptation of the eye to clear vision of objects that are at different distances from it due to changes in the curvature of the lens.

Convergence is the ability of the eye to take a position when viewing close objects, in which the visual axes of both eyes intersect on the object.

Light affects not only the function of the organs of vision, but also the activity of the body as a whole. With poor lighting, a person gets tired quickly, works less productively, and the potential danger of wrong actions and accidents increases. According to statistics, up to 5% of injuries can be explained by insufficient or irrational lighting, and in 20% it contributed to the occurrence of injuries. After all, poor lighting can lead to occupational diseases.

To create optimal conditions for visual work at the computer, not only the amount and quality of lighting, but also the color environment should be taken into

account. Thus, with light painting of the interior, due to the increase in the amount of reflected light, the level of illumination increases by 20-40% (with the same power of light sources), the sharpness of shadows decreases, and the uniformity of lighting improves.

Artificial lighting is provided in all industrial and domestic premises where there is not enough natural light, as well as for lighting premises in the dark period of the day. When organizing artificial lighting, it is necessary to ensure favorable hygienic conditions for visual work and at the same time take into account economic indicators.

In order to create favorable conditions for visual work at the computer, which would exclude rapid eye fatigue, the occurrence of occupational diseases, accidents and contribute to increasing labor productivity, lighting should meet the following requirements:

- should not have a blinding effect both from the light sources themselves and from other objects in the field of vision;

- ensure sufficient uniformity and constancy of the level of illumination in the rooms in order to avoid frequent re-adaptation of the visual organs;

- do not create sharp and deep shadows (especially moving ones) on the work surface;

- the contrast of illuminated surfaces must be sufficient to distinguish details;

- do not create dangerous and harmful production factors (noise, thermal radiation, dangerous electric shock, fire and explosion hazard of lamps).

CONCLUSION

In the qualifying work, the development of a computer network for the university library was carried out.

The relevance of the selected topic was shown and the peculiarities of the implementation of wired and wireless networks were analyzed, and for the implementation of a local computer network it was decided to use the wired Ethernet network, as the most powerful in terms of data exchange, and also to place wireless access points in the library hall. First of all, this will allow students to prepare for studies and complete individual tasks on computers, and other students in the reading room itself - to search for information and work in Internet resources using their own smartphones or tablets.

The features of network cables and cable system components are also analyzed. To organize the local network of the university library, it is suggested to use a fiber optic cable. Methods of connecting computers to the hub and server were also analyzed. A drawing of the room plan was made and the location of computer network elements was indicated on it. Variants of network elements are offered, including computers, servers, hubs, etc. Calculations of the bandwidth of the projected network were carried out.

The main elements of the Wi-Fi network are also analyzed. Specific types of these items are selected, including network adapter, wireless adapter, PCI adapter, and access points. Features and main stages of setting up such a network are considered. This network should be effective for working in the library hall.

LIST OF SOURCES USED

1. https://en.wikipedia.org/wiki/Computer_network

2. Gillies, James M.; Gillies, James; Gillies, James and Cailliau Robert; Cailliau, R. (2000). How the Web was Born: The Story of the World Wide Web. Oxford University Press. pp. 13

3. Roberts, Lawrence G. (November 1978). "The evolution of packet switching" (PDF). Proceedings of the IEEE. 66 (11): 1307–13.

4. https://www.techtarget.com/searchnetworking/definition/network

5. https://www.javatpoint.com/computer-network-tutorial

6. https://www.javatpoint.com/types-of-computer-network

7. https://www.geeksforgeeks.org/basics-computer-networking/

8. https://www.britannica.com/technology/computer-network

9. https://www.sierraexperts.com/7-types-of-computer-networks-explained

10. https://www.techtarget.com/searchnetworking/feature/7-types-of-networks-and-their-use-cases

11. https://en.wikipedia.org/wiki/Optical_fiber

12. https://en.wikipedia.org/wiki/Coaxial_cable

13. https://www.geeksforgeeks.org/what-is-coaxial-cable/

14. https://www.techtarget.com/searchdatacenter/definition/Categories-of-twisted-pair-cabling-systems