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 the university educational laboratory computer network

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

	(signature)	Oluwadare Oluwasegun Jesse (surname and initials)
Supervisor	(signature)	Dozorskyi V.G. (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
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 Oluwadare Oluwasegun Jesse
(surname, name, patronymic)

1. Paper topic Development of the university educational laboratory computer network

Paper supervisor Dozorskyi V.G., PhD, Associate Profesior
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of 28.02.2023 № 4/7-233.

2. Student's paper submission deadline 01.07.2023

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

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

Principles of organizing computer networks; classification of a local computer network; selection of network type and topology; stages of network design; necessary criteria of a local computing network; OSI system interaction model; network technology IEEE802.3 Ethernet; Wi-Fi technology standards; protection of information in local computing networks. Development of the computer network of the teaching laboratory of the university; choosing a network topology; description of standards; twisted pair; fiber optic cable; coaxial cables; transmission standards; typical equipment, materials and tools for organizing a computer network. Results of network design; configuration of server computers; configuration of workstation technology; network equipment.

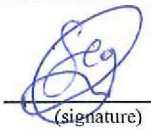
6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
LABOR PROTECTION	Okipnyy I.B.		

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  Oluwadare Oluwasegun Jesse
(signature) (surname and initials)

Paper supervisor _____ Dozorskyi V.G.
(signature) (surname and initials)

ANNOTATION

Theme of qualification work: Development of the university educational laboratory computer network // Qualification work of the educational level "Bachelor" // Oluwadare Oluwasegun Jesse // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information System and Software Engineering,

Department of Computer Science // Ternopil, 2023 // P. , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

In the qualifying work, the development of computer network of the university educational laboratory was carried out. The concept of a local computer network, its purpose and principles of operation were analyzed. An analysis of the type and topology of networks was carried out. The existing network topologies, analyzes the standards used for the organization of computer networks, considers typical equipment, materials and tools for the organization of a computer network were analyzed.The seven-level OSI model was analyzed. The selection of computers that will play the role of servers and workstations was carried out. Their configuration and number are given. The selection of network equipment was also carried out.

CONTENTS

INTRODUCTION 7

CHAPTER 1. PRINCIPLES OF ORGANIZING COMPUTER NETWORKS..9

1.1 Classification of a local computer network……9

1.2 Selection of network type and topology……..10

1.3 Stages of network design ……11

1.4 Necessary criteria of a local computing network ……11

1.5 OSI system interaction model ……12

1.6 Network technology IEEE802.3 Ethernet ……..14

1.7 Wi-Fi technology standards ……17

1.8 Protection of information in local computing networks ……18

1.9 Conclusions to chapter 1 ……20

CHAPTER 2. DEVELOPMENT OF THE COMPUTER NETWORK OF THE TEACHING LABORATORY OF THE UNIVERSITY ……21

2.1 Choosing a network topology ……21

2.2 Description of standards ……24

2.3 Twisted pair ……24

2.4 Fiber optic cable ……..26

2.5 Coaxial cables ……27

2.6 Transmission standards ……...28

2.7 Typical equipment, materials and tools for organizing a computer network ……29

2.8 Conclusions to chapter 2 ……33

CHAPTER 3. RESULTS OF NETWORK DESIGN ……..34

3.1 Configuration of server computers ……34

3.2 Configuration of workstation technology ……..36

3.3 Network equipment ……37
3.4 Conclusions to chapter 3 ……38
CHAPTER 4. LIFE SAFETY, BASICS OF LABOR PROTECTION……..39
4.1 Electric current as a factor of danger……..….39
4.2. Fire safety requirements for extinguishing electrical installations…….…41
CONCLUSIONS……44
LIST OF SOURCES USED……...…45

INTRODUCTION

In our time, in the context of the rapid development of information and computing technology, information acts as one of the most important goods. The success of commercial and entrepreneurial activities is associated with banking, municipal, banking information systems, the operation of which is based on local area networks.

The past decade has been characterized by the rapid development of network systems. Networks provide the most cost-effective way to use computer technology - collectively. By connecting existing servers, computers, printers, modems due to relatively low costs with cables, you get the opportunity to reduce the downtime of expensive equipment to a minimum, saving significant amounts on its purchase and maintenance.

In its original form, LANs were nothing more than a coaxial cable connecting servers to desktop terminals, whose users worked exclusively with textual information displayed on a low-resolution monochrome monitor.

In the mid-1990s, Ethernet network reached its peak of development. And also Token Ring network. However, unlike the first generation of LANs, the performance crisis was not due to insufficient bandwidth. In Ethernet networks in particular, throughput is not an issue at all. On the contrary, the decrease in the efficiency of functioning was due to other reasons:

- fierce competition for access to the local network;
- saturation of the available bandwidth with optional overhead messages.

Fundamentally new types of software have also contributed to the disclosure of the shortcomings of existing networks. The network performance requirements of the software differed from those that the networks were able to provide.

LANs have now evolved into local area networks with sufficient bandwidth and performance for traditional forms of data processing (e.g., email) and even for processor- and network-demanding client-applications such as real-time interactive voice and video conferencing.

Today, network technologies cover all issues related to the sharing of data, software and computer peripherals, including printers, modems, multifunction copiers and fax machines, CD drives, tape drives, hard drives and other data storage equipment, Internet access.

In the qualification work, the development of the computer system of the primary laboratory of the university is carried out.

The relevance of such a development is due to the fact that today a significant amount of applied software for the simulation of electronic circuits, design of printed circuit boards and nodes, video and audio processing, processing and modeling of complex signals and processes, etc. is used in student education, which requires significant computing resources . This, in turn, determines the need to modernize educational laboratories and ensure the opportunity for each student of the relevant specialty to work on a personal computer and perform assigned tasks in accordance with the educational process.

CHAPTER 1
PRINCIPLES OF ORGANIZING COMPUTER NETWORKS

1.1 Classification of a local computer network

A set of nodes (computers, terminals, peripheral devices) that have the possibility of information interaction with each other by special communication equipment and software is called a computer network. A local computer network connects a number of computers in an area limited by the boundaries of one room, building or enterprise.

Serious attention is paid to the issues of LOM classification due to the fact that modern computer networks can cover large areas, be used to solve tasks of different complexity and purpose, use different environments and data transfer protocols. Thus, when designing a local computer network, the customer and the contractor face the question of the ambiguity of the terminology used.

Below is a classification of local networks according to some features.

The classification of LOMs according to the management method distinguishes them into networks with dedicated servers, peer-to-peer networks (all network nodes are equal) and terminal networks (networks using the so-called network-centric construction concept, in which the end-user equipment provides only input-output functions, and all requests to processing and receiving information is performed by the network core).

According to the coverage of the geographical territory, local public transport systems are divided into local (limited to a building or a group of buildings), territorial or regional (operating within a limited territory, covering a significant geographical space - a city, region, country) and global (connecting nodes located in different regions and points). world).

Wired, fiber optic and wireless networks are distinguished by physical environment.

There is a classification of LOM according to the method of access of workstations to the data transmission medium (deterministic and random). The most famous are multiple access method with carrier control and conflict detection (CSMA/CD), which is regulated by IEEE802.3 standard, and the token transmission method - the IEEE802.5 standard. CSMA/CD refers to decentralized random (more precisely, quasi-random) methods. It is used in both ordinary Ethernet-type networks and high-speed networks.

The characteristics and areas of application of these networks, which are popular in practice, are related to the specifics of the access method used.

1.2 Selection of network type and topology

For my project, I chose the Ethernet network type.

Ethernet is a family of packet data transfer technologies for computer networks.

Ethernet standards define wired connections and electrical signals at the physical level, frame format and media access control protocols at the channel level of the OSI model. Ethernet is mainly described by the IEEE standards of the 802.3 group. Ethernet became the most widespread LAN technology in the mid-1990s, replacing such outdated technologies as Arcnet and Token ring.

The name "Ethernet" (literally "ether network") reflects the initial principle of this technology: everything transmitted by one node is simultaneously received by all others (that is, there is some similarity with radio broadcasting). Currently, the connection is almost always made through switches, so that the frames sent by one node reach only the addressee (the exception is transmissions to a broadcast address) — this increases the speed of work and the security of the network.

1.3 Stages of network design

Construction begins with the design of a local computing network (LAN), which takes into account its main tasks, the required bandwidth, the method of transmitting information flows, as well as their nature and the number of network participants. Then the installation of the LAN is carried out, consisting of the laying of cable routes, installation and wiring of the network. The final stage can be called work on its adjustment and testing of the LAN.

The construction of the LAN is carried out with the aim of uniting all workplaces of the company's employees into a single information network. This is necessary for the rapid exchange of information between employees.

The construction itself consists of the following main stages:

Preliminary inspection of the object, where the network section is broken, or its laying is required;

Network design;

Local network installation. This includes installation of cable routes, installation of twisted pair at workplaces.

Local network testing;

Start-up work (checking and, if necessary, setting up the equipment);

Follow-up maintenance and (if necessary) repair of the local network.

1.4 Necessary criteria of a local computing network

Resilience

Backup lines provide protection against failure and allow you to connect network equipment in various ways. If one of the connections fails, the traffic is instantly transferred over the backup lines.

Protection

Each network needs one or another form of protection. Simple password protection offered by operating systems is rarely sufficient. You should look for network solutions that offer additional security options at the hub, switch, router, and remote access server level

Manageability

With the growth of the network, the ability to monitor and manage traffic flows, predict various problems and diagnose malfunctions becomes increasingly important.

Reliability

As your dependence on the network grows, its downtime becomes more and more expensive. It is necessary to look for solutions that provide increased reliability, the necessary warranty and service strategies. Such critical factors as fault tolerance should be taken into account

Flexibility

Since the requirements for the network change very quickly, the configuration should be designed to adapt to new needs without major modifications.

1.5 OSI system interaction model

The OSI model (Open System Interconnect Reference Model) is a universal standard for the interaction of two systems (computers) through a computer network.

This model describes the functions of seven hierarchical levels and the interaction interfaces between the levels. Each level is defined by the service it provides to the higher level, and by the protocol - a set of rules and data formats for the interaction of objects of the same level running on different computers.

The idea is that the entire complex procedure of network interaction can be broken down into a certain number of primitives, which are sequentially executed by objects correlated with the levels of the model. The task of objects is to provide a

certain higher-level service through a standardized interface, using, if necessary, a service that provides this object with a lower level.

For example, a process sends data over a network to a process on another computer. Through a standardized interface, the sender process transmits data to the lower level, which provides the process with a data forwarding service, and the receiving process, through the same standardized interface, receives this data from the lower level. At the same time, none of the processes knows and does not need to know exactly how the lower-level protocol transfers data, how many layers are below it, what is the physical environment of data transfer and which way they move.

These processes, on the other hand, may not be at the top level of the model. Let's assume that they interact with higher-level applications through a standard interface and their task (service) is data transformation, namely fragmentation and assembly of large blocks of data that higher applications send to each other. At the same time, the essence of these data and their interpretation are not important at all for the analyzed processes.

Interchangeability of objects of the same level is also possible (for example, when changing the method of service implementation) in such a way that the object of a higher level will not notice the replacement.

Let's go back to the example: applications do not know that the data is transformed precisely by fragmentation/assembly, they need to know that the lower layer provides them with some "correct" data transformation service. If, on the other hand, some other network requires not fragmenting/assembling packets, but, say, permuting the even and odd bits, then the processes of the layer in question will be replaced, but the programs will not notice anything, because their lower-level interfaces are standardized and specific actions of lower levels are hidden from them.

Objects performing the functions of levels can be implemented in software, software-hardware or hardware form. As a rule, the lower the level, the greater the share of hardware in its implementation.

The organization of network interaction of computers, built taking into account hierarchical levels, as described above, is often called a protocol stack.

Listed below (from top to bottom) are the layers of the OSI model and their general functions.

The application level (Application) is an interface with application processes.

The level of presentation (Presentation) - coordination of the presentation (formats, encodings) of application process data.

Session level (Session) - establishing, maintaining and closing a logical communication session between remote processes.

Transport layer – ensuring error-free end-to-end exchange of data streams between processes during a session.

Network layer (Network) - fragmentation and compilation of data transmitted by the transport layer, routing and forwarding them over the network.

Channel level (Data Link) - control of the transmission channel, control of access to the transmission medium, transmission of data through the channel, detection of errors in the channel and its correction.

Physical level (Physical) - a physical interface with a transmission channel, data presentation as physical signals and its coding (modulation).

1.6 Network technology IEEE802.3 Ethernet

There are many varieties of Ethernet, denoted by rather complex abbreviations, such as 10BASE-T, 10BASE-2, 100BASE-T, 1000BASE-LX, and 10GBASE-T. These and many other Ethernet technologies have been standardized over the years by IEEE802.3· CSMA/CD (Ethernet) working group. At first glance, reductions may seem terrible, but in fact there is a certain order to them. The first part of the abbreviation indicates the speed used in the standard. BASE stands for unmodulated Ethernet – that is, the physical medium carries only Ethernet traffic; almost all 802.3

standards are specific to unmodulated Ethernet. The last part of the abbreviation defines the physical medium itself. There are both channel and physical layer specifications for Ethernet, and data is transmitted over a variety of physical media, including coaxial cable, copper cable, and fiber optic. In general, the letter T means twisted pair.

Historically, Ethernet technology was designed to transmit information over a coaxial cable. Early standards 10BASE-2 and 10BASE-5 describe Ethernet transmission on 10Mbit/s speed over 2 types of coaxial cable, in both cases the length of the cable should not exceed 500 m. Transmission of longer distances is carried out using a repeater. This is a physical level device that receives a signal at the input and reproduces it at the output. All frames transmitted by an interface are received on all other interfaces, and the CDMA/CD Ethernet protocol does a good job of solving the multiplicity problem.

Ethernet technology has undergone a number of evolutionary changes over the years, and today's Ethernet is very different from the original bus topology that used coaxial cable. In most configurations today, nodes are connected to the switch using two-point segments made of twisted-pair optic fiber access.

In the mid-90s, the Ethernet standard appeared with 100Mbit/s transfer rate - that is, ten times faster than 10 Mbit/c. It retained the original Ethernet MAC protocol, but described higher-speed physical layers for copper cable (100BASE-T) and for fiber optic. Figure 1.1 shows the various standards, as well as a common Ethernet MAC protocol and frame format.

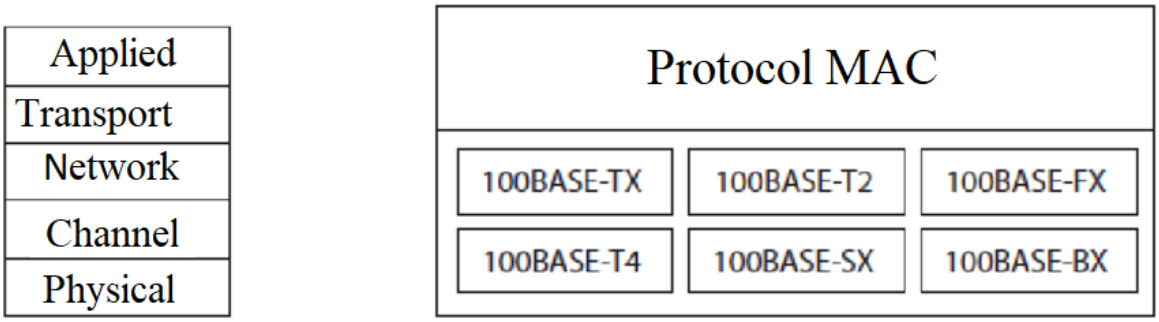


Figure 1.1 Ethernet standards

For 100Mbit/s Ethernet maximum cable length is 100 meters for twisted pair transmission and up to several kilometers if fiber is used. In this way, it is possible to connect Ethernet switches in different houses.

Gigabit Ethernet is an improvement over the highly successful 10Mbit/s - 100Mbit/s standards. It provides a maximum physical data transfer rate of 1000 Mbps, as well as full compatibility with the entire vast base of Ethernet equipment already installed. According to the document, Gigabit Ethernet standard implements the following functionality:

– Uses standard Ethernet frame format, provides backward compatibility with 10BASE-T and 100BASE-T technologies. In this way, the convenient integration of Gigabit Ethernet into the already deployed technical base of Ethernet equipment is ensured.

– Allows the use of point-to-point channels as well as split broadcast channels. When working with two-point channels, switches are used, and when working with broadcast hubs, as described above. In Gigabit Ethernet terminology, a hub is called a buffered hub.

– Uses CSMA/CD protocol when working with broadcast channels. In order to ensure acceptable work efficiency, the maximum distance between nodes is strictly limited.

- Provides full-duplex operation of point-to-point channels at a speed of 1000 Mbit/s in both directions.

Gigabit Ethernet originally operated over fiber optic cable, but now also supports category 5 UTP cable. 10 Gbit/c Ethernet technology was standardized in 2007, after which Ethernet LANs became even more powerful.

In the days of bus topologies and star topologies with the use of a hub in Ethernet, of course, broadcast communication was used. When this mechanism of communication between frames was used, collisions could occur if the nodes transmitted data simultaneously. In order to deal with collisions, the Ethernet standard provided for the use of the CSMA/CD protocol, which is indeed very effective when laying cable LANs in small areas. But currently, Ethernet networks are dominated by star topologies using switches, where packet switching with intermediate storage and transmission is implemented. a switch coordinates its data operations and never transmits more than one frame on a given interface at a given time. Moreover, modern switches are full-duplex, that is, they provide frame transmission in both directions without interference. In other words, there are no collisions in switched Ethernet local networks, which means that we can conclude that the MAC protocol is not needed.

1.7 Wi-Fi technology standards

Wireless LANs, firmly entrenched in workplaces, our homes, educational institutions, cafes, airports and street intersections, have become one of the most important technologies for accessing the Internet.

There are several 802.11 wireless LAN standards. All that standards can be used in both "infrastructure" and "decentralized peer-to-peer" modes.

The 802.11b standard has a data rate of 11 Mbps and operates in the unlicensed frequency range of 2400.0-2483.5 MHz, sharing it with 2.4 GHz telephones and microwave ovens.

Depending on the type of signal modulation, the 802.11n standard allows data transfer rates of up to several hundred megabits per second.

1.8 Protection of information in local computing networks

Data protection in computer networks is becoming one of the most acute problems in the modern information environment. Today, there are the following basic principles of information protection construction:

1. Ensuring the integrity of information, which includes protection against failures, such as loss of data during transmission, and even illegal creation and destruction of data;

2. Confidentiality of information – prevention of data disclosure;

3. Set access levels for users.

There is a classification of access rights violations, as well as failures during data exchange, which can lead to the destruction or restructuring of information:

- equipment failures

1) violation of the cable system;

2) Power outages;

3) Failures of disk systems;

4) Violation of servers, network cards, etc.

5) Errors in the operation of disk systems.

- Software malfunctions:

1) Loss of data in case of malfunction of software tools;

2) Infection of the workstation with computer viruses.

- Unauthorized access to information:

1) Illegal copying, destruction and modification of information;

2) Dissemination of the enterprise's commercial secret by unauthorized disclosure.

- inefficient information storage system.

- The human factor when working with important information:

1) Accidental destruction or modification of data;

2) Inefficient use of software, which caused the destruction or modification of important information.

The types of network violations listed above have influenced the creation of protection tools, such as:

1. Means of physical protection (protection of the cable system, power supply, archiving);

2. Means of software protection (antivirus programs, demarcation of access rights);

3. Administrative means of information security (control of access to premises, development of enterprise strategy).

One of the main means of protecting information on the network is user authentication - the need for an identity card.

Thus, when contacting the server with the information storage, control is transferred to the authentication server, and only after its positive response, the user is granted access to the requested information.

Also, due to the recently developed trend of using the Internet for data transfer, a competent approach to network protection is necessary. For this, network engineers use firewalls - a system of dividing the network into several blocks and describing the rules for their further passage. The firewall passes all traffic through itself and for each packet transmitted through the network, a decision is made to pass it or not. At the same time, the use of a firewall can be implemented both by hardware, i.e. by installing the appropriate hardware, and by installing software.

There is also a method of converting text into a random set of characters called cryptography or encryption. Cryptography is based on concepts such as an algorithm - a method of encoding a signal, resulting in an encoded message, and a key - a means

of interpreting an encoded message. Using a key allows you to use the same algorithm with different keys to send messages to different recipients. At the same time, if the integrity of the key is violated, it can be replaced without making changes to the encryption algorithm.

However, it is still possible to modify or replace the original message during encoding. To ensure information security, users are provided with a brief representation of the message being transmitted, called a message digest. Algorithms for creating a digest are developed in a single form for each message. However, there are problems when transferring the message digest, so a system for transferring it to an electronic signature was developed. This tool is created by encoding the digest and additional information with the sender's private key, which allows the sender to be identified as the originator of the message.

1.9 Conclusions to chapter 1

The chapter analyzes the concept of a local computer network, its purpose and principles of operation. An analysis of the networks type was carried out. For the project itself, I chose the Ethernet network type. The stages of network design are also analyzed and the necessary criteria that the designed network must satisfy are highlighted.

CHAPTER 2
DEVELOPMENT OF THE COMPUTER NETWORK OF THE TEACHING LABORATORY OF THE UNIVERSITY

2.1 Choosing a network topology

Computers and other components of a local network may be connected in various ways. The topology of a network is defined by a geometric figure formed by communication lines between computers, or by the physical location in relation to each other of connected computers. In addition, the cost of acquiring and installing network equipment is of great importance, which is an important issue for an educational institution, the price range here is also quite large.

There are many ways to connect network devices.

Star connection means the connection of computers to a central node (Fig. 2.1)

Networking: When the source sends signals to the network environment, the data is sent to the central network device (hub), then the hub forwards it to the device according to the address contained in the data.

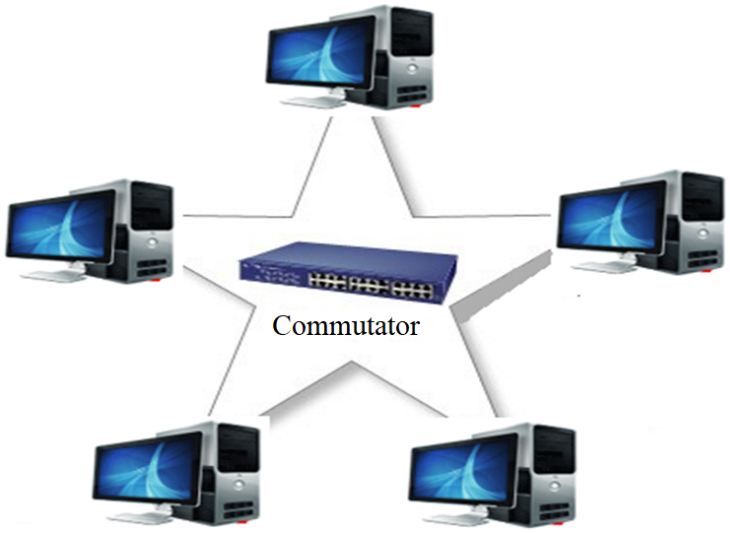


Figure 2.1. Star topology

Ring cjnnection means connection of the computers in series (Fig. 2.2).

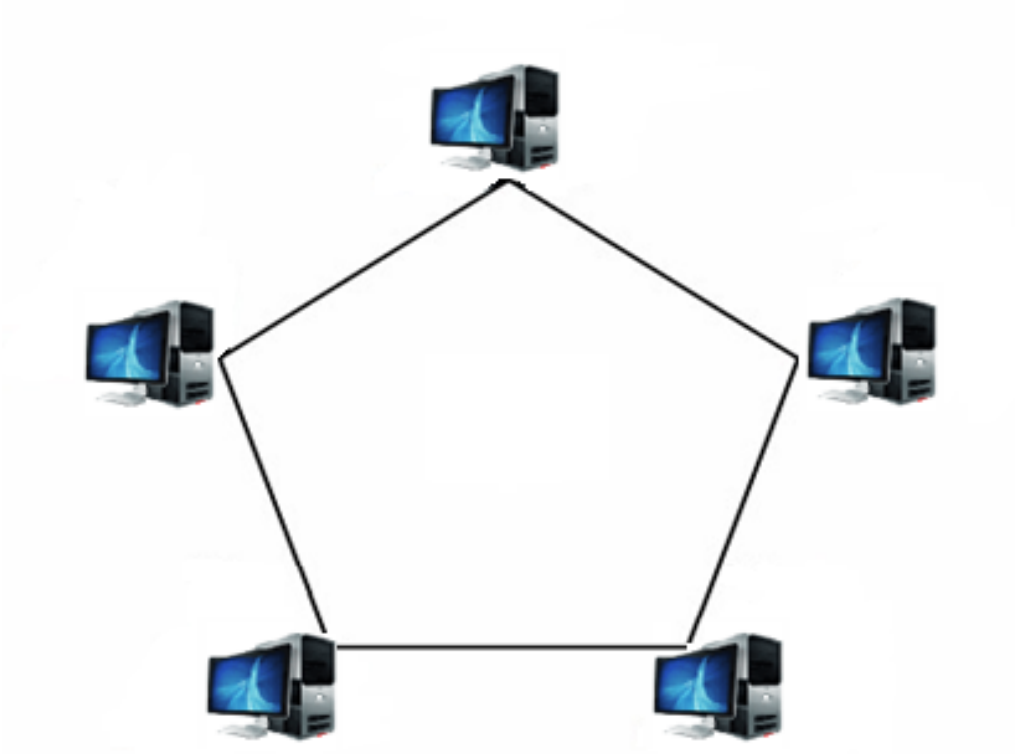


Figure 2.2. Topology "ring"

Figure 2.3. shows the bus connection

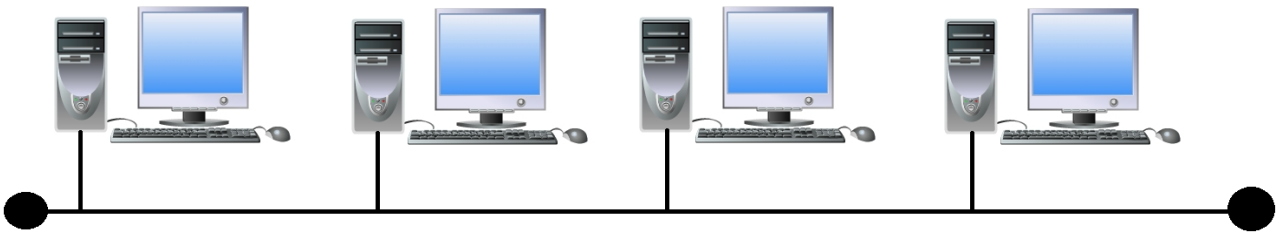


Figure 2.3. Bus topology

The figure also shows terminators. Such devices are installed at the ends of the network and limit the propagation of the signal by closing the network segment. If a cable break occurs somewhere or a terminator is not installed at least at one end of the network, the signal will begin to be reflected from the break point and the corresponding end of the network, which will lead to a communication failure.

The advantages of using networks with a "common bus" topology are as follows:

• significant cable savings;

• ease of creation and management.

• Main disadvantages:

• the probability of collisions with an increase in the number of computers in the network;

• a cable break will shut down many computers;

low level of protection of transmitted information. Any computer can receive data that is transmitted over the network.

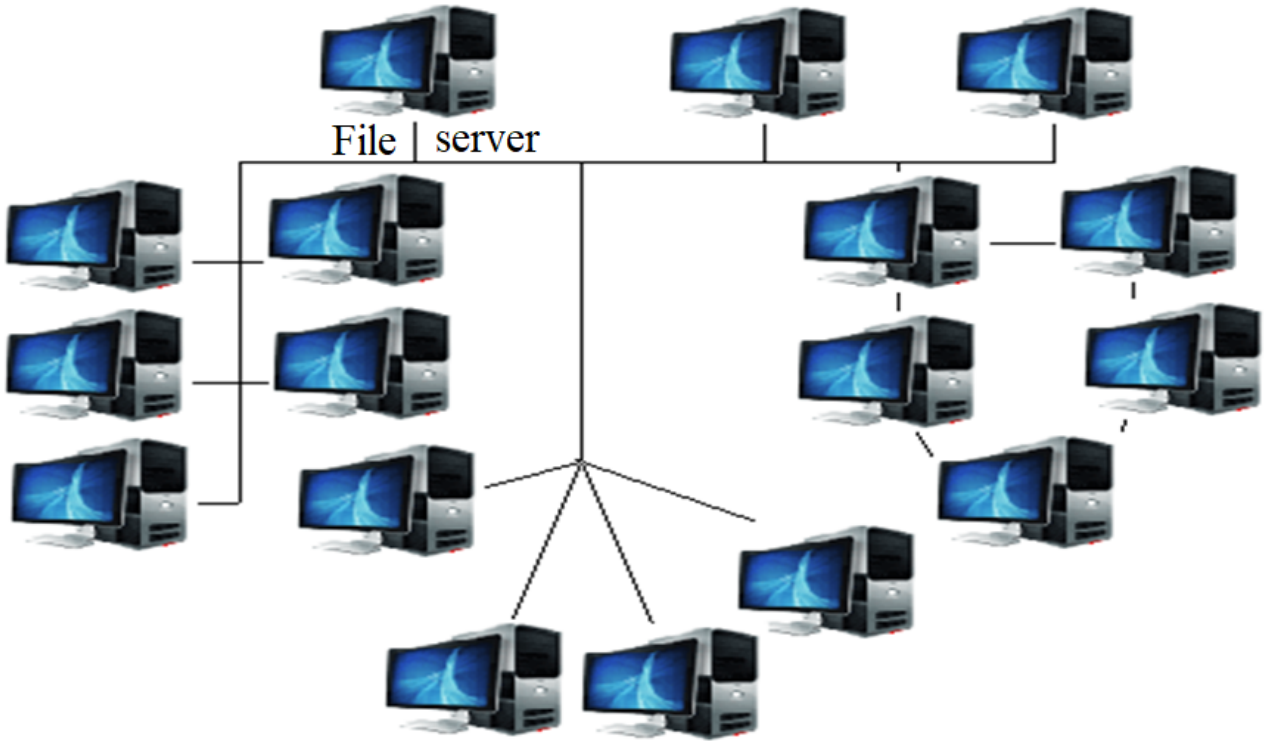


Figure 2.4. "Tree" topology

2.2 Description of standards

Fast Ethernet (100BASE-T) - a set of standards for data transmission in computer networks to 100 Mbps.

In 1995, a number of network equipment manufacturers (such as 3Com, SynOptics, etc.) formed the Fast Ethernet Alliance, intended to create a new specification that would unite individual developments of various companies in the field of data cable transmission.

At the same time, work has begun at the IEEE to standardize the new technology. A research group set up to do this, from late 1992 to late 1993, studied many 100-megabit solutions offered by various manufacturers, as well as high-speed technology offered by Hewlett-Packard and AT&T.

2.3 Twisted pair

Line of "twisted pair" type can be at least two conductors that are separated by dielectric materials and have uniform gaps throughout the transmission. A balanced voltage equal in amplitude and opposite in phase is applied to these two conductors.

The flowing currents create a concentric magnetic field that surrounds each of the existing conductors. The magnetic field voltage always increases in the section between the conductors and disappears in the space where the concentric field is outside the two conductors. Any change in current will generate a voltage across each of the conductors with a resultant electric field.

As a result, characteristic impedance is considered a function of the frequencies of the transmitted signals and depends on the length of the line. At very high frequency, the characteristic impedance without resistance tends to some resistive resistance.

Signal attenuation characteristic is the ratio, measured in decibels (dB), of the strength (power) of the input signal to the strength of the output signal according to the impedance of the sources and loads of the characteristic impedance of the cable. You can determine the input power by measuring the power when the load is directly connected to the source, while there should be no signals passing through the cable. In other cases, when at the termination point the impedances do not perfectly correspond to each other, the ratio of input to output power is called such a definition as loss or attenuation.

Transient attenuation occurring at the near end is a parameter that characterizes the attenuation of an interference signal that can be induced by a signal passing from one pair of conductors to another that is nearby. It is measured in decibels. The larger the value, the better the interference isolation between the two pairs of conductors.

Reflection losses (return losses) – occur when the impedance of the cable and the load do not match, so the signal propagated by the cable can partially be reflected in the software interface or when measuring the cable load.

The power of the reflected signal is called the return loss. The greater the impedance match, the lower the power of the reflected signals and, accordingly, the lower the return loss.

One of the characteristics of cable networks is the time delay (timing) of signal propagation. The signal that propagates from the input point to the output point arrives with some time delay, the value of this delay is the ratio of the length of the cable to the speed of propagation of signals among data transmission.

Also, for example, in an ideal transmission line consisting of two conductors in a vacuum environment, the speed of signal propagation will be equal to the speed of light propagation.

In real conditions, the speed of signal propagation in the cable will depend on the properties of the dielectric material surrounding the conductors.

Signal-to-noise is the difference or ratio between the received signal level and the received noise and signal level must be significantly higher of noise level to ensure sufficiently acceptable transmission conditions.

Ratio of extinctions to transient extinctions. The signal/noise ratio can be expressed as the attenuation to transient attenuation ratio - ACR. ACR is the difference between the attenuated output signals and the harmful input signals (noise). The section of the "twisted pair" is presented in Figure 5.

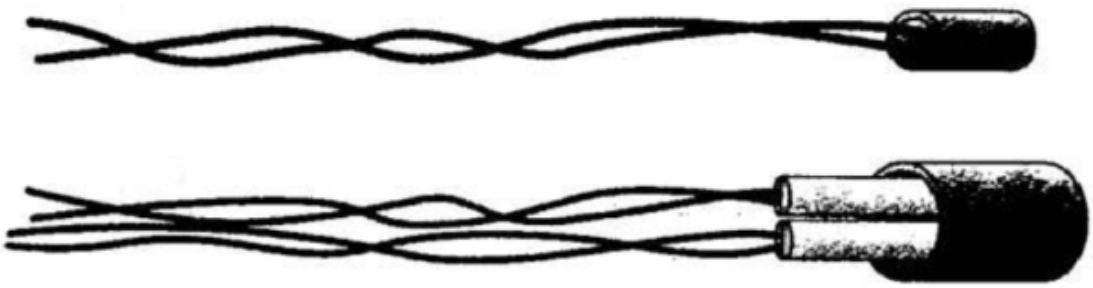


Figure 2.5 Unshielded and shielded twisted pairs

2.4 Fiber optic cable

Such communications have a number of advantages over cable systems that use a metal-based transmission medium. In optical cable systems, the transmitted signal is not distorted by any type of external interference - electronic, magnetic, and radio frequency. That is, the effect of interference caused by lightning or high voltage sources is completely excluded on optical cable networks. In addition, optical fibers do not emit radiation, which makes it ideal for meeting the requirements of the modern standard for computer applications. Based on the fact that the optical signal does not require the presence of a grounding system, it turns out that the transmitter and receiver are isolated (dielectric) from each other, and there are no problems associated with the occurrence of a parasitic current loop. With no or insufficient potential shift in the grounding system between the two terminals, which excludes sparks and various electrical discharges, fiber optic cabling is still the best choice for

many applications where safety in explosive or flammable environments is one of the main requirements.

The latest digital, computer systems, ip-telephony and video-language systems increase requests to create new directions for improving the quality of transmission characteristics. A significant range width of optical cables means an increase in channel capacity. Moreover, fewer repeaters are required for long cable runs because fiber optic networks have very low attenuation.

These properties are ideal for broadcast and telecommunication systems.

Compared to conventional coaxial cable with the same bandwidth, the smaller diameter and weight of optical cable means relatively easier installation, especially in existing routes.

The electronic method of wiretapping cable systems is based on electromagnetic monitoring. Optical cable systems are completely immune to such techniques. To take readings or data, you need to physically connect to the cable, which will reduce the signal level and increase the error rate - but such phenomena are easily and quickly recognized.

2.5 Coaxial cables

Coaxial cable consists of two copper conductors, only these conductors are not parallel, but concentric (or coaxial). With the help of this design, as well as thanks to special insulation and shielding, the coaxial cable allows you to achieve high data transfer rates. It is often used in cable television systems. Cable television systems combined with cable modems can provide subscribers with Internet access at speeds of tens of megabits per second. In cable television and cable access networks, a transmitter carries a digital signal into a specific frequency band, and then the resulting analog signal is sent from the transmitter to one or more receivers. Coaxial cable uses as a conductive separation medium. Multiple end systems can be directly

connected to the cable, and each can receive data. Figure 9 shows the cross-section of coaxial cable.

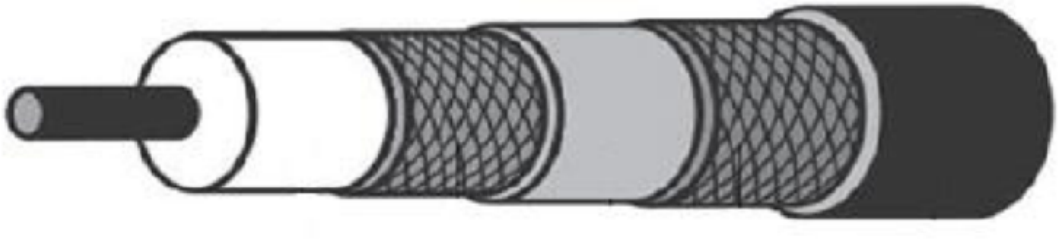


Figure 2.6 Coaxial cable

2.6 Transmission standards

The structure of network protocols - the hardware and software implementing these protocols - is organized using layers. Each protocol belongs to a certain one layer. Let's consider the functions that a layer provides to the layers above - the so-called model of layer maintenance. Each level provides its services. For example, layer n services may include reliable delivery of messages from one end of the network to the other. This can be implemented using layer n - 1 unreliable end-to-end message delivery with the addition of layer n detection and lost message forwarding functionality.

2.7 Typical equipment, materials and tools for organizing a computer network

A computer (workstation) connected to a network is the most versatile node. The application use of the computer on the network is determined by the software and the installed accessories. For long-distance communications, a modem is used, internal or external. From a network point of view, the "face" of a computer is its network adapter. The type of network adapter must match the purpose of the computer and its network activity.

The server is also a computer, but with more resources. This implies its higher network activity and relevance. Servers should preferably be connected to a dedicated switch port. When installing two or more network interfaces (including a modem connection) and the corresponding software, the server can play the role of a router or bridge. Servers are generally required to have a high performance operating system.

The RJ abbreviation means Registered Jack. Although there are a great many of them, the most popular connector types are RJ11, RJ12, and RJ45. The first two types of connectors are mainly for telephone wires, and the main difference in RJ11 - RJ12 is the number of pins. These two types of interface have 6 pin positions, but these positions can be occupied by 2, 4 and 6 pins - RJ11 has up to 4 pins, and RJ12 has all 6 positions occupied.

RJ45 connectors (Fig. 5) are used for Category·5·twisted·pair, one of the most common cables today. In it, all 8 positions come with contacts, and such a cable is actively used to build local networks. There is no pin compatibility problem between the RJ11, RJ12 and RJ45 interfaces. But here we should not forget the principle of "weak link" - the principle of assessing the characteristics of the smallest indicator. For example, it is possible to connect an RJ12 to an RJ45 socket, if only 6 pins are used, there is no problem if two RJ45 pins are not active.

Crimping schemes

There are two options for crimping the connector on the cable:

• The TIA/EIA-568Bstandard is used to create a direct cable - to connect the network card port to a switch or hub (Fig.6)

• The TIA/EIA-568Bstandard is used to create a crossover (using crossed MDI, MDI-X) cable with an inverted pinout of the connector for connecting directly two network cards installed in computers, as well as for connecting some old models of hubs or switches (uplink port) (Fig.2.7)

If you need an MDI cable with external crossover, the so-called "straight" cable for connecting a computer to a hub / switch, the following schemes are used:

According to one of these schemes, connectors are crimped on both sides.

Crossover cable

Used to connect equipment of the same type (for example, computer-to-computer). However, most network devices are able to automatically detect the cable crimp method and adapt to it (Auto-MDI/MDI-X).

Option for 100 Mbps

If you need an MDI-X cable with internal crossover, a "crossover" cable for connection, for example, "computer-to-computer" (at speeds up to 100 Mb / s), then on one side of the cable the EIA / TIA-568B scheme is used, on the other EIA / TIA-568A

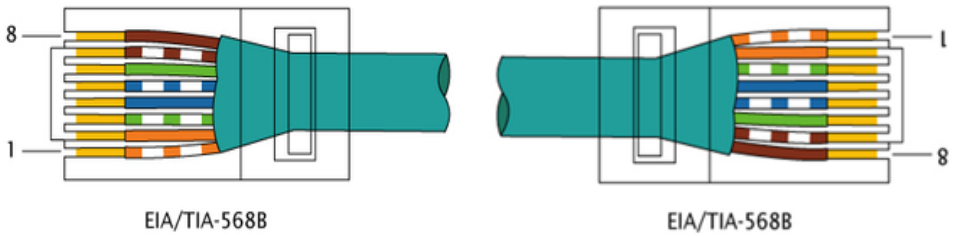


Figure 2.7. Straight crimp

Option for 1000 Mbps

For connections at speeds up to 1000 Mb / s, when making a "crossover" cable, one side must be crimped according to the EIA / TIA-568B standard.

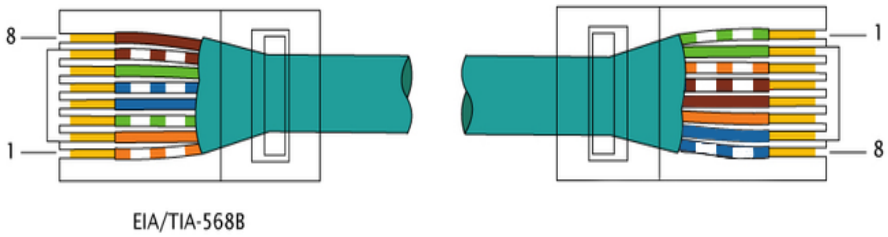


Figure 2.8. crimp crossover

Crimper

Crimper - Crimping tool (Fig. 2.9)

Figure 2.9. Crimper

Crimping part: for eight-, six-pin connectors and an adjustable cutter that allows you to remove the outer insulation without damaging the wires pairs.

Pair 1-2 (TDP-TDN) is always required for transmission from an MDI port to an MDI-X port, pair 3-6 (RDP-RDN) is always required for reception by an MDI port from an MDI-X port; pairs 4-5 and 7-8 are used as required and are usually bi-directional.

Using a cable that is not crimped according to the standard may lead (depending on the length of the cable) to the fact that the cable will not work or it will has a very large percentage of transmitted packets lost.

To check the correctness of the cable compression, in addition to visual control, special devices are used - cable testers (Fig. 2.10).

Figure 2.10. LAN tester

Such a device consists of a transmitter and a receiver. The transmitter in turn sends a signal to each of the eight cable cores, duplicating this transmission by lighting one of the eight LEDs, and on the receiver connected to the other end of the line, one of the eight LEDs lights up accordingly. If the LEDs on the transmission and reception light up in a row, it means that the cable is crimped without error. More expensive models of cable testers may have a built-in intercom, a break indicator indicating the distance to the break, etc.

OSI model divides the problem of transferring information between subscribers into seven smaller and therefore more easily solved problems. The concretization of each task was carried out according to the principle of relative autonomy. Obviously, the autonomous task is easier to solve.

Each of the seven areas of the information transmission problem is assigned one of the levels of reference model. Such model describes how information travels through a medium (eg, metal wires) from a source application process (eg, voice) to a destination process.

Within the framework of the OSI model, the interaction of two systems is actually presented in the form of two models - horizontal and vertical:

• within the framework of the horizontal model, direct interaction (data exchange) of the same levels in two end points (hosts) is considered; to organize such

interaction in each of the endpoints, the same protocols for this level must be supported;

• the vertical model considers the exchange of information (interaction) between adjacent levels of one system using API interfaces; in this model, each layer can provide its services to the upper layer and use the services of the lower layer (the extreme layers of the model in this sense are an exception - the application layer provides its services to the user, and the network layer does not use the services of other layers)

2.8 Conclusions to chapter 2

In the chapter, an analysis of the basic topological structures was carried out, standards were analyzed, which are required for organizing computer networks, typical equipment, materials and tools for organizing computer networks were reviewed.

The seven-level OSI model was analyzed.

CHAPTER 3
RESULTS OF NETWORK DESIGN

3.1 Configuration of server computers

The project will create local facilities for the primary laboratory of the university to have a file server and a proxy server. The hardware storage file server contains an Intel Core Extreme i7 processor with 16 gigabytes of RAM, as well as SATA Raid from 2 Western·Digital·Caviar·Green·IntelliPower hard drives with a total volume of 4TB, which ensures a large disk array capacity, high productivity there is that small hour access to server files.

A proxy server is needed to secure access to the web for other computers. The storage includes an Intel· Core· i7-3770· processor, and the storage capacity is 8 gigabytes. 1 hard drive Western·Digital·Caviar·Green was assigned to the file server. The storage volume of the disk array is 500 GB.

Table 3.1 File server configuration

Name	Model	Quantity
CPU	Intel Core Extreme i7-3970X 3.5GHz (TB up to 4.0GHz) 15Mb 4xDDR3-1600 TDP-130w LGA2011 OEM	1
Motherboard	Gigabyte LGA1155 GA-Z77X-UD5H Z77 4xDDR3-2400 3xPCI-E(16, 8+8+4) HDMI, DVI, DSub, DP 8ch mSATA 4xSATA 5xSATA3 10xUSB3 eSATA 1394 2xGLAN ATX	1

video card	NVIDIA GeForce 9800 GT	1
RAM	DIMM DDR3 4096MB PC12800 1600MHz Corsair XMS3 9-9-9-24 [CMX4GX3M1A1600C9] Retail	4
HDD	SATA-3 2Tb Western Digital Caviar Green IntelliPower [WD20EZRX] Cache 64MB	2
Case and power supply	Server Case Intel SC5600BRP 750W HS	1
Keyboard+Mouse	Gigabyte GK-KM5200	1
Monitor	LG Flatron E1942C	1

Table 3.2 Proxy server configuration

Name	Model	Quantity
CPU	Intel Core i7-3770 3.4GHz (TB up to 3.9GHz) 8Mb 2xDDR3-1333 HDGraphics4000 TDP-77w LGA1155 BOX w, cooler	1
Motherboard	Gigabyte LGA1155 GA-Z77X-UD5H Z77 4xDDR3-2400 3xPCI-E(16, 8+8+4) HDMI, DVI, DSub, DP 8ch mSATA 4xSATA 5xSATA3 10xUSB3 eSATA 1394 2xGLAN ATX	1
video card	NVIDIA GeForce 9800 GT	1
RAM	DIMM DDR3 4096MB PC12800 1600MHz Corsair XMS3 9-9-9-24 [CMX4GX3M1A1600C9] Retail	2
HDD	SATA-3 500Gb Western Digital Caviar Green [WD5000AZRX] Cache 64MB	1

Case and power supply	Server Case Intel SC5600BRP 750W HS	1
Keyboard+Mouse	Gigabyte GK-KM5200	1
Monitor	LG Flatron E1942C	1

3.2 Configuration of workstation technology

In the primary laboratory, it was planned to install computers with high productivity. On these computers there are Intel Core i7-2600K processors, Western Digital Caviar Green IntelliPower hard disks with a capacity of 1TB. Zagalniy obsyag operational memory warehouse 4GB. Motherboard ASUS LGA1155 P8B75-V B75. Qi computers ensure high productivity.

Table 3.3 Workstation configuration

Name	Model	Quantity
Monitor	LG 18.5" Flatron E1942C [LED, 1366x768, DC 5M:1, D-Sub]	20
Keyboard	A4-Tech X7-G700	20
Mouse	A4Tech X-710BK 3-Fire Extra High Speed Oscar Edition USB	20
Case	Miditower ATX AirTone IC-601	20
Motherboard	Плата ASUS LGA1155 P8B75-V B75 4xDDR3-2200 2xPCI-Ex16(16+4) DVI/DSub 8ch 5xSATA 1xSATA3 4xUSB3 GLAN ATX	20
CPU	Intel Core i7-2600K 3.4GHz (TB up to 3.8GHz) 8Mb 2xDDR3-1333 HDGraphics3000 TDP-95w LGA1155 BOX	20

	w, cooler	
video card	PCI-E Gigabyte GeForce GTX 660 2048MB 192bit GDDR5 [GV-N660OC-2GD] DVI HDMI DisplayPort	20
Memory module	DIMM DDR3 4096MBx2 PC12800 1600MHz Corsair XMS3 9-9-9-24 XMP [CMX8GX3M2A1600C9] Retail	20
HDD	SATA-3 1Tb Western Digital Caviar Green IntelliPower [WD10EZRX] Cache 64MB	20
power unit	Chieftec 750W (750W, ATX 2.0, APFC, 140mm fan, CM, 24+4+8, 8xSATA, PCI-E(8+8+6+6)) [CFT-750-14CS]	20

3.3 Network equipment

To organize a network, you must use the following equipment. The manufacturer D-Link was chosen because this brand is very common and has a good reputation in the market. The network will operate at a speed of 100 Mbit / s, since this speed is quite enough for the exchange of information.

Table 3.4 Network equipment

Components	Name
Switch 32 port	KVM Swith 32
Cable	UTP 4 .5e
Connectors	RJ-45
Closet	WALLBOX 9-65
cable channel	Efapel 10040

Patch panel	Patch Panel 19
router	D-link DIR-615
Sockets	RJ-45
patch cords	Patch Cord UTP 5e 1m

3.4 Conclusions to chapter 3

The chapter analyzes and selects computers that will play the role of servers and workstations. Their configuration and number are given. The selection of network equipment was also carried out.

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).

CONCLUSIONS

In the qualification work, the development of the computer system of the primary laboratory of the university is carried out.

The concept of a local computer network, its purpose and principles of operation were analyzed. An analysis of the type and topology of networks was carried out. For the project itself, I chose the Ethernet network type. The stages of network design are also analyzed and the necessary criteria that the designed network must satisfy are highlighted.

The existing network topologies, analyzes the standards used for the organization of computer networks, considers typical equipment, materials and tools for the organization of a computer network were analyzed.

The seven-level OSI model was analyzed.

The selection of computers that will play the role of servers and workstations was carried out. Their configuration and number are given. The selection of network equipment was also carried out.

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

15. Hosono, M (26–28 October 1982). Improved Automatic meter reading and load control system and its operational achievement. 4th International Conference on Metering, Apparatus and Tariffs for Electricity Supply. IEE. pp. 90–94.

16. Cooper, D.; Jeans, T. (1 July 2002). "Narrowband, low data rate communications on the low-voltage mains in the CENELEC frequencies. I. Noise and attenuation". IEEE Transactions on Power Delivery. 17 (3): 718–723.

17. Newbury, J. (January 1998). "Communication requirements and standards for low voltage mains signalling". IEEE Transactions on Power Delivery. 13 (1): 46–52

18. Duval, G. "Applications of power-line carrier at Electricite de France". Proc 1997 Internat. Symp. On Power Line Comms and Its Applications: 76–80.

19. Hoch, Martin (2011). "Comparison of PLC G3 and Prime" (PDF). 2011 IEEE Symposium on Powerline Communication and Its Applications: 165–169.

20. Glenn Elmore (August 2006). "Understanding the information rate of BPL and other last-mile pipes". Computing Unplugged magazine. Archived from the original on July 22, 2011. Retrieved July 22, 2011.

21. Glenn Elmore (27 July 2009). "Introduction to the Propagating TM Wave on a Single Conductor" (PDF). Corridor Systems. Retrieved 22 July 2011.

12. Jump up to:a b IEEE P1901.2. "IEEE 1901.2-2013 - IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications". Retrieved 23 December 2013.

23. "New Global Standard for Fully Networked Home". Itu.int. 12 December 2008. Archived from the original on 21 February 2009. Retrieved 11 October 2010.

24. G. Goldberg. “EMC PROBLEMS OF POWER LINE COMMUNICATION (PLC) SYSTEMS”. 2001;

25. https://en.wikipedia.org/wiki/Time-division_multiplexing

26. G.F. Bartak. “POWERLINE COMMUNICATION SYSTEMS. NORMATIVE AND REGULATORY ASPECTS FOR THEIR APPLICATION”. 2001;

27. Kourtis, A.; Dangkis, K.; Zacharapoulos, V.; Mantakas, C. (1993). "Analogue time division multiplexing". International Journal of Electronics. Taylor & Francis. 74 (6): 901–907.

28. "Understanding Telecommunications". Ericsson. Archived from the original on April 13, 2004.

29. White, Curt (2007). Data Communications and Computer Networks. Boston, MA: Thomson Course Technology. pp. 143–152. ISBN 978-1-4188-3610-8.

30. Guowang Miao; Jens Zander; Ki Won Sung; Ben Slimane (2016). Fundamentals of Mobile Data Networks. Cambridge University Press.