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

Faculty Of Computer Information Systems And Software Engineering
(full name of faculty)
Computer Systems And Networks Department
(full name of department)

QUALIFYING PAPER

For the degree of

Bachelor
(degree name)

topic: **Development of computer network for the University of Liberia**
Розробка комп'ютерної мережі для університету Ліберії

Submitted by: fourth year student _____ , group ICI-42
specialty 123 Computer Engineering
(code and name of specialty)

	_____ (signature)	Thomas Stephen sk. (surname and initials)
Supervisor	_____ (signature)	Holotenko O.S. (surname and initials)
Standards verified by	_____ (signature)	StadnykN.B. (surname and initials)
Head of Department	_____ (signature)	Osukhivska H.M. (surname and initials)
Reviewer	_____ (signature)	Bodnarchuk I.O. (surname and initials)

Ternopil
2021

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

Faculty Faculty Of Computer Information Systems And Software Engineering
(full name of faculty)

Department Computer Systems And Networks Department
(full name of department)

APPROVED BY
Head of Department

_____ Osukhivska H.M.
(signature) (surname and initials)

« » 2021

ASSIGNMENT

for QUALIFYING PAPER

for the degree of *bachelor*
(degree name)

specialty *123 Computer Engineering*
(code and name of the specialty)

student Thomas Stephen sk.
(surname, name, patronymic)

1. Paper topic *Development of computer network for the University of Liberia*

Paper supervisor Holotenko Oleksandr Serhiyovych,, PhD, Assoc. Prof.
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of « » 20 _ №

2. Student's paper submission deadline 27/06/2021

3. Initial data for the paper *Computer network requirements analysis, physical topology of a computer network, calculation of logical addressing, organization of Internet access.*

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

Introduction. 1. The Open Systems Interconnect (OSI) reference model. 2. Ethernet. 3. Design part. 4. Special part. 5. Occupational safety and health. Conclusions.

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

1. Block diagram of the computer network of the College of Social Sciences and Humanities of the University of Liberia. 2. Physical topology of a computer network. 3. Scheme of computer network connections. 4. Logical topology of a computer network. 6. Simulated computer network in the Cisco Packet Tracer environment.

6. Advisors of paper chapters.

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
Occupational safety and health			

7. Date of receiving the assignment.

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
	Analysis of technical task		
	Analysis of characteristics of the object		
	Computer network requirements analysis		
	Information resources and services		
	Computer network structure		
	Selection of active network equipment		
	Organization of Internet access		
	Occupational safety and health		
	Graphic materials		
	Preparation to the qualification work presentation		
	Qualification work presentation		

Student _____ Thomas Stephen sk
(signature) (surname and initials)

Paper supervisor _____ Holotenko O.S.
(signature) (surname and initials)

ABSTRACT

Development of computer network for the University of Liberia //Qualifying paper // Thomas Stephen sk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, group ICI-42 //Ternopil, 2021 // p. - 51, fig. - 8, tabl.- 10, code snip. -5, append. - 2, bibliogr. - 15.

Keywords: Ethernet, physical topology, network equipment, switching, routing, sharing services, system.

In this diploma thesis developed a computer network of the College of Social Sciences and Humanities University of Liberia. Basic documentation has been prepared: network diagrams at the physical, channel and network levels, IP-addressing plan, list of devices. Access to the Internet, private and public servers from all network devices of the school is organized. Wi-Fi is also provided in the building.

TABLE OF CONTENT

INTRODUCTION

Modern conditions of information technology development dictate the need for their accelerated use as the most efficient means of control, management and data exchange, both within a single unit and on the scale of a large enterprise or university.

With the emergence and development of data networks, a new, highly efficient way of interacting between people has emerged.

The main purpose of computer networks is to share resources and establish communication both within one unit or organization. Resources should be understood as programs, data, applications, peripherals.

Networks allow a large number of users to simultaneously "own" programs, databases, devices, and so on.

Today, most organizations store and share large amounts of critical data, special programs designed for sharing on local area networks, such as a number of banking programs, accounting programs, and more.

The main purpose of this work is to design a computer network for the College of Social Sciences and Humanities for the University of Liberia.

To achieve this goal, it is necessary to solve the following tasks:

- to analyze the current network architecture of the «College of Social Sciences and Humanities of the University of Liberia», to identify places that need further improvement;

- justify the choice of network architecture for a computer network, access methods, topology, type of cable system, operating system, applications, protocols;

- justify the choice of network management method;

- justify the choice of network equipment;

- prepare basic documentation: network diagrams at the physical, channel and network levels, IP addressing plan, list of devices;

- simulate the network in the Cisco Packet Tracer emulator.

This network must provide uninterrupted communication between workstations in the network. Increase productivity by simplifying data exchange between employees of different departments. Also, the developed network must ensure high reliability and security of information.

1 THE OPEN SYSTEMS INTERCONNECT (OSI) REFERENCE MODEL

As is known, the OSI model (Open Systems Interconnection) describes 7 layers that computers and interactive systems use to transmit over a network. It was the first known network communication model, adopted by all top communication and hardware companies in the first half of the1980s.

Today Internet is based on the simpler TCP/IP model, but not on OSI. In fact, the OSI seven-layer model usually still often used, as known it helps visualize and communicate how networks work, and also helps isolate and fix network problems.

Open Systems Interconnection was shown in 1983 by the largest computer and telecommunications companies, and was adopted as an international standard in 1984 (ISO).

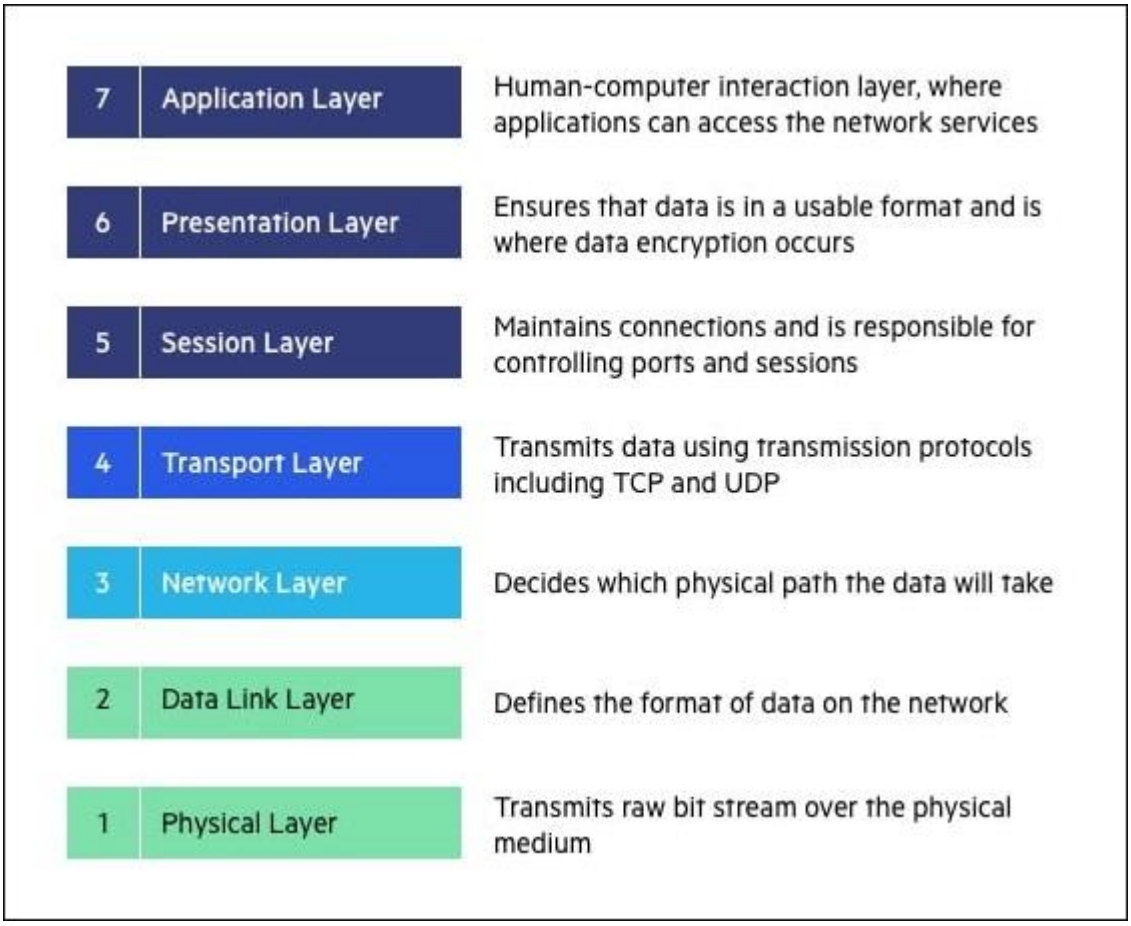

Fig. 1.1 OSI reference model

The OSI network model consists of 7 layers. Such structure is due to the following thoughts:

1) Each Level is created as needed for a separate level

abstraction.

2) Levels must perform a specific function.

3) Functions for each level should be performed with

taking into account the creation of standardized international protocols.

4) The boundaries between the levels are chosen so that the data flow between the interfaces is minimal.

5) The number of levels should be sufficient so that the different functions do not combine, but not too large to architecture did not become cumbersome.

The OSI model is not a network architecture because it does not describe it services and protocols used at each level. It simply determines what each level should do. Below we consider level models, it is customary to start counting from the bottom.

1. The physical layer.

As it known the lowest layer is the physical layer that directly transfers the data stream. It provides electrical, mechanical and other functional aids. Usually this may be optical (laser, optical fiber) or electrical signals, sound or electromagnetic waves (obviously WiFI). Respectively the methods which used called the technical transmission process. Devices and network components related to the physical layer: antennas and amplifiers, diverse plug and sockets for network cable, repeaters, transceivers, bars, T-bands and terminators.

In fact, in computer networks now, information is usually transmitted in sequences of bits or symbols. However, in copper cables and radio transmissions, high-frequency electromagnetic waves that are information carriers are modulated in optical waveguides of light waves of a certain wavelength or other. The information carrier knows no bit strings, but can take many more different states than just “zero” or “one”. Therefore, an encoding must be defined for each type of transmission. This is due to the physical layer specification of the network.

Typical equipment on this layer are repeaters, cables, hubs, plugs.

2. Data Link Layer.

Data link layer - we need it for the interactivity of networks at the physical layer. Usually everyone has heard about the MAC address, as known a physical address. Link layer devices - switches, hubs, etc.

3. Network Layer.

Network layer - this layer defines the path through which data will be transferred. And, by the way, this is the third level of the OSI Network Model, but there are devices that are called – routers ("third-level devices").

We've all heard of the IP address, and that's what the Internet Protocol (IP) does. An IP address is just a network logical address.

There are a lot of protocols at this level (as example ping command - this is the ICMP protocol).

4. Transport Layer.

This layer ensures that data transmission from the sender to the recipient is safe.

As example of bad transmission, when we watch videos on the YouTube, sometimes we can see some artifacts, delays, noise, etc. Sometimes when we read text from a web page, the loss (or reduction) of letters is not permissible, and when we download programs, everything also goes without errors.

As a rule, we use UDP for music, video or audio calls, and for texting, programing, passwords, archives, etc.

5. Session Layer

The session layer organizes a communication between devices, as example is audio and video conference (which codec can encode the signal). Another example is the SMPP protocol. We use it to send SMS and USSD requests. One final example: PAP "Password Authentication Protocol" is an old protocol which can send a username and password to a server without encryption.

6. Presentation Layer.

The presentation layer can convert the data into the appropriate format. Using an example, it's easier to understand: those pictures (all images) that you see on the screen

are transmitted when transferring a file in the form of small portions of ones and zeros (bits). So, when you email your friend a photo, the SMTP Application Layer protocol sends the photo to the lower layer, i.e. to the Presentation level. Where your photo is converted into a convenient form of data for lower levels, for example, in bits (ones and zeros).

In exactly the same way, when your friend starts receiving your photo, it will come to him in the form of all the same ones and zeros, and it is the Representation level that converts the bits into a full-fledged photo, for example, a JPEG.

This is how this layer works with protocols (standards) of images (JPEG, GIF, PNG, TIFF), encodings (ASCII, EBDIC), music and video (MPEG), etc.

7. The application layer.

The application layer is the topmost layer of the model. It connects applications which users use to the network. We are all familiar with these applications: web browsing (HTTP), sending and receiving mail (SMTP, POP3), receiving and sending files (FTP, TFTP), remote control and access (Telnet), etc.

The functions of the Application Layers are:

- Helps you to identify all communication partners, determining resource availability, and synchronizing communication.
- It allows users to make log on to a remote host.
- This layer provides many services which helps to sending and receiving e-mails.
- This layer offers global database sources and access for global information, as example various objects and services.

Advantages of OSI Model.

The OSI model usually helps admins, users and computer networks operators

- It is a common model that guides the development of any network model.
- This is a model which is called layered. Changes to one level do not affect other levels, provided that the interfaces between the levels do not change dramatically.

- Definitely, it is flexible. It usually separates services, interfaces, and protocols. The protocols at each layer can be changed very conveniently depending on the nature of the network.
- It supports both connection-oriented and connectionless services.

Comparing the OSI and TCP/IP Models.

OSI and TCP / IP models are reference and usually are used to describe the data transfer process. Actually, the TCP / IP model is used for a set of TCP / IP protocols, and the OSI model is usually used to develop common communication for hardware and software from different developers.

The TCP / IP model describes the same node interaction procedure as the OSI model, but uses four levels instead of seven.

Comparing the layers of the TCP / IP model and the OSI model, the application layer of the TCP / IP model is a same to a combination of layers 5, 6, 7 of the OSI model, however the TCP / IP model does not have a separate presentation and session layer. The TCP / IP transport layer includes the OSI transport layer functions and some of the OSI model session layer functions. The network access layer of the TCP / IP model respectively encompasses the link and physical layers of the OSI model. As is known TCP / IP network layer does not take superiority of the sequencing and acknowledgment services which may be present in the OSI data link layer.

Actually, the OSI model named is a conceptual model. It is usually used to describe, discuss and understand individual network functions. However, TCP / IP is usually designed to solve some problems, not as a general description for all network interactions like the OSI model. The OSI model usually is general, protocol independent, but in our opinion all protocols and systems adhere to it, while the TCP / IP model is based on the standard known protocols.

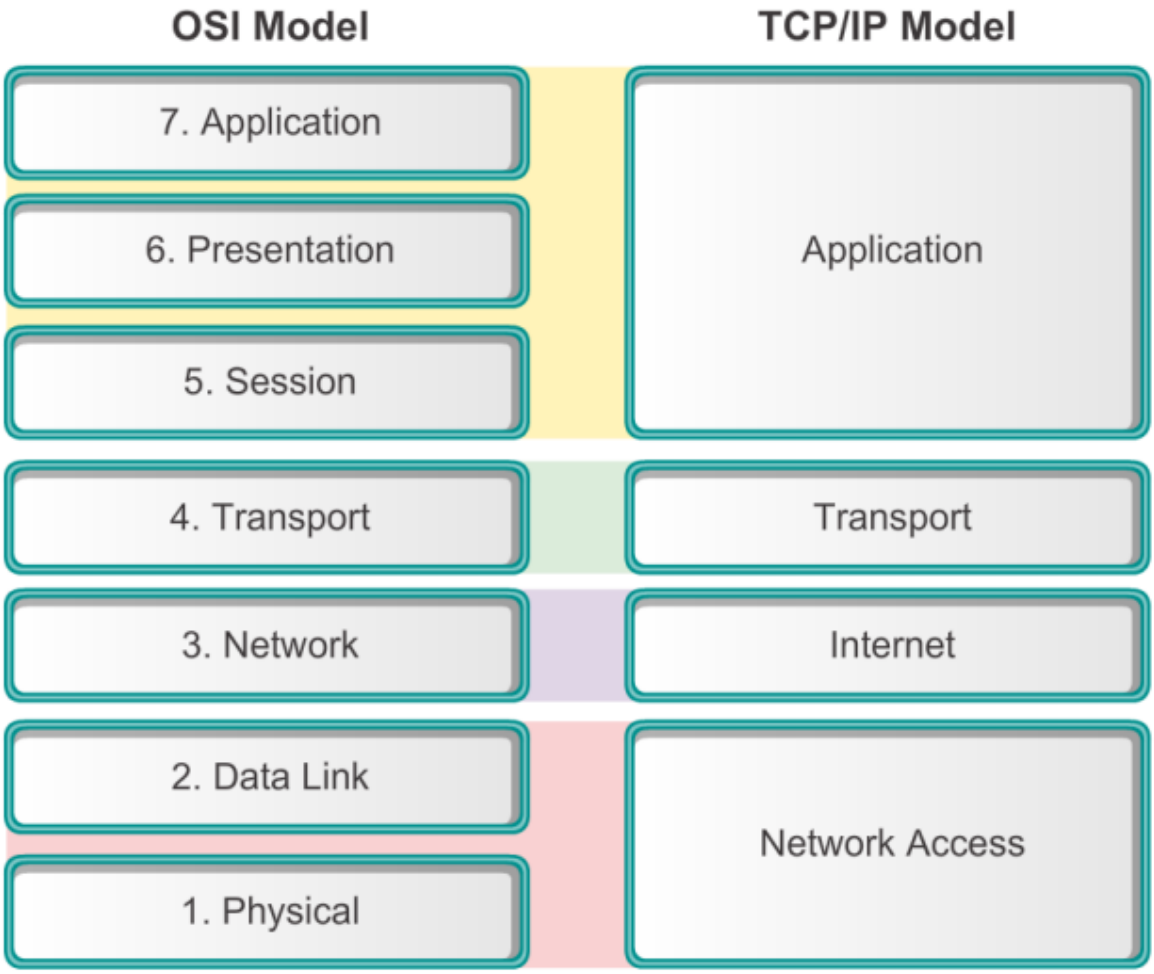

Fig.1.2 Comparing the OSI and TCP/IP Models

The TCP / IP model and commonly known the OSI model are conceptual models which used to describe all communications in the networks.

2 ETHERNET.

Numerous designs for personal use, local and the area of metropolitan networks have been systematized and named of IEEE 802. Over the past decades only few have managed to survive. The most dominant of the survivors are “802.3” and “802.11” (Ether an WLan), Bluetooth (wireless PAN) is extensively deployed but has now been systematize outside of “802.15”. With “802.16” (wireless MAN), it is too early to predict.

There are two kinds of Ethernet that exist: **classic Ethernet**, solves the multiple access problem using the techniques we have studied in this chapter; and **switched Ethernet**, devices such as switches are used to connect non- identical computers systems. Most importantly, both are referred to as Ethernet, but also different. Classic Ethernet is first generation and ran at the speed from 3 to 10 Mbps. While Switched Ethernet runs at 100, 1000, and 10,000 Mbps, in forms called new generation fast Ethernet, gigabit Ethernet, and 10 gigabit Ethernet. In practice, switched Ethernet is the one been used today.

2.1 Classic Ethernet Physical Layer

The foundation of Ethernet approximately begins at the time of ALOHA, an inspiring student named Bob Melancton Metcalfe graduated with his bachelor's degree at M.I.T. and then later moved up the river to get his Ph.D. at Harvard. Throughout his studies, dedicated himself to the work of Abramson's Norman. Mr. Metcalf became very interested and decided after graduating from Harvard, to spend the summer in Hawaii working with Norman Abramson, before been invited to research at Xerox PARC (Palo Alto Research Center). At PARC, he understood that the researchers there had designed and started the future what we now refer to as computers. Only than they were isolated. Bob With the knowledged, obtain with the help of Mr. Abramson's work, successively with his colleague David Boggs, designed and implemented the first-generation local area network (Metcalfe and Boggs, in 1976). It was used as a single long, thick coaxial cable that ran at 3 Mbps.

They called the system **Ethernet** after the luminiferous ether, which electromagnetic radiation was predicted to propagate. (19th-century British physicist James Clerk Maxwell originated that electromagnetic radiation could be described by

a wave equation, scientists presume that space must be filled with some ethereal medium by which radiation was generated. After the famous Michelson-Morley experimented in 1887, he discovers that electromagnetic radiation could be generated in a vacuum.)

The Xerox Ethernet was successful and regarded as the standard in 1978 for a 10-Mbps Ethernet mark by DEC, Intel, and Xerox, called the **DIX standard.** With minimum changes, the DIX standard became the systemized IEEE 802.3 standard in 1983.

Classic Ethernet was identified by its single long cable to which all the computers were connected. Architecture shown in Fig. 2.1. The first-generation variety, famously called **thick Ethernet,** resembled a yellow garden hose, with markings every 2.5 meters to show where to attach or connect a computer. (The 802.3 standard did not require that the cable be yellow, but suggest it was beneficial.) The **thick Ethernet** succeeded by **thin Ethernet,** bent more easily and made connections using industry-standard BNC connectors to computers. It was much cheaper and easier to install, but it could run only 185 meters per segment (instead of 500 m with thick Ethernet), each of which could handle only 25 to 30 machines (instead of 100).

Early version of Ethernet had a maximum cable length per segment (i.e., unamplified length) which the signal will generate. To allow larger or sizable networks, repeaters to propagate it desire result can connect multiple cables. Repeater has physical layer devices that amplifies, receives (i.e., regenerates) transmits and retransmits signals in both directions. Series of cable segments connected by repeaters is no way different from a single cable (except for minimum delay establish by the repeaters).

The Ethernet could contain multi cable segments and multi repeaters, but no two or three transceivers could be more than 2.5 km apart and no path between any two or three transceivers could traverse more than four or five repeaters.

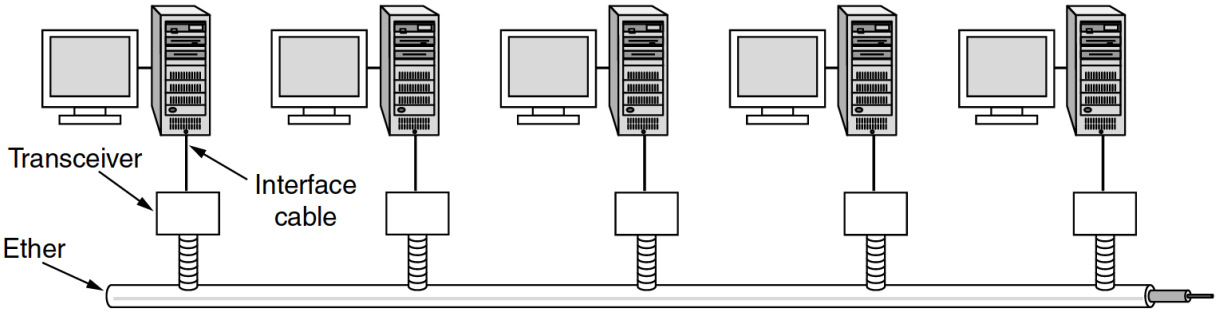

Fig. 2.1 Architecture of classic Ethernet.

2.2 CSMA/CD with Binary Exponential Backoff.

Classic Ethernet uses the 1-persistent CSMA/CD. This descriptor means that stations sense the medium when they have a frame to send and send the frame as soon as the medium becomes inactive. It monitors the channel for incompatibility as they send the frame. If there is a collision, they abort or terminate the transmission with a direct jam signal and retransmit after a statistical interval.

After a collision, time is diverge into slots by which length is equal to the worst-case roundtrip propagation time on the ether (2τ). To accumulate the longest path authorize by Ethernet, the discrete slot time set at 51.2 psec or 512 bit times.

After the first collision, the stations waits either 0 or 1 discrete slot times at random before retransmission. If there is a collision between stations each station picks the same random number, there will be a reoccurrence of collision. After the second collision, each one picks either 0, 1, 2, 3 or 4 at random and waits that number of discrete slot time. The probability of a third collision occurrence is 0.25).

Conventionally, after collisions, random number between 0 and 2^i - 1 is selected, and the chosen number of discrete slots is cavorted. Although, after 10 collisions have been reached, the unsystematic interval is preserved at a maximum of 1023 discrete slots. After numerous or 16 collisions, the regulators sent in the towel and reports failure back to the computer. Further recuperations is up to the higher layers.

This algorithm, called **binary exponential backoff,** selected dynamically to adapt the number of slot stations trying to send form. If the systemization interval for numerous collisions were 1023, the possibility of selected stations colliding for a second time would be at the minimum, but the standard wait time after a collision

would be the minimum of hundreds of slot times, introducing outstanding interval. Although, if individual stations delayed for either 0 or 1 slots, then if 100 stations ever tried to send at the minimum of one there will be a collision over and over until 99 of them picked 1 and the remaining station picked 0. This might take decades. By having unsystematic interval it grow exponentially as there will be more consecutive collisions occurring, the algorithm guarantee a ultra- low delay with not many collision, and also ensures that the collisions are solved in a feasible interval with only few stations colliding.

With no collision, the sender presume the frame was successfully deliver. Although, neither Ethernet nor CSMA/CD contribute commendation. Choice appropriate for wired and optical fiber channels that have ultra-low error rates. However, errors that do transpire must then be perceive by the CRC and recuperated by a much higher layer. For wireless channels that have a little more errors, it is necessary that commendations are employ.

2.3 Switched Ethernet/

Lately Ethernet began to develop away from the single long cable design of classic Ethernet. The few problems associated with locating the breaks or loose connections drove it toward a various kinds of wiring structure, by which each station has a exclusive cable running to a more central **core**. A **hub** simply connects all the attached wires electrically, as if they were fasten together. Configuration shown in Fig. 2.2 (a).

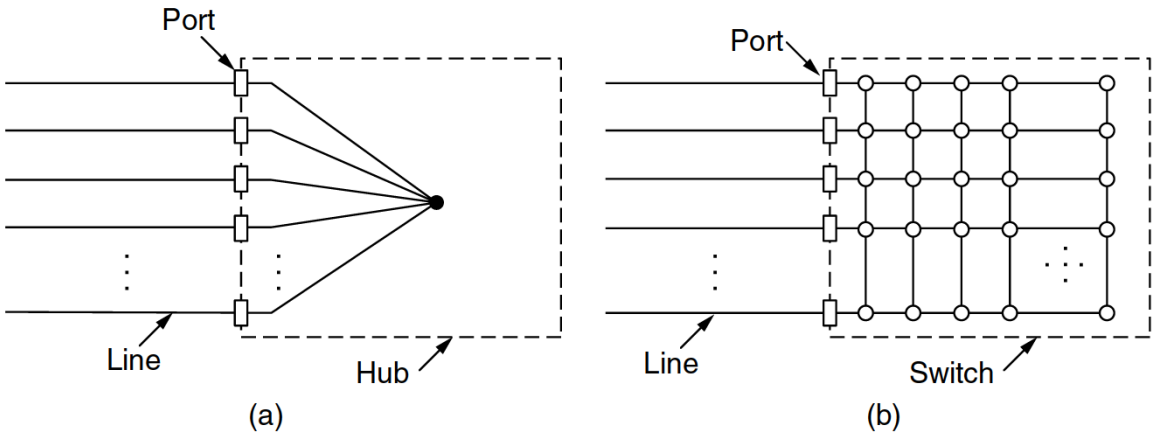

Fig. 2.2. (a) Hub. (b) Switch.

Telephone company perverted pairs, most office or newly home buildings were been wired by this structure and conventionally many spares were unoccupied. The

reuse was victorious, but with some reduction the maximum cable run from the core to 100 meters, (200 meters if high quality Category 5 twisted pairs employed). In addiction or subtraction, a station is simpler in this configuration, and cable penetration is detected. The advantages of being able to use preexisting wiring and ultra-low maintenance, twisted-pair hubs quickly became the commending form of Ethernet.

However, the capacity of the core do not increase because due to its logical equivalent to the single long cable of classic Ethernet. As more and more stations added, individual stations gets a low share of the selected capacity. However, the LAN will suffuse.

Importantly, with the help of modern technology there are numerous ways to increase load: switched Ethernet. The heart of this system is a switch containing a high-speed backplane that connects all of the ports, as shown in Fig. 2.2 (b). From the outside, a switch looks just like a hub or core. They are boxes, typically with 4 to 48 ports, with a standard RJ-45 connector for a twisted-pair cable. Individual cable connects the switch or core to a single computer, as shown in Fig. 2.3. A switch has the same advantages as a hub, too. It is easy to add or remove new stations by unplugging or plugging a wire, and faults can be easily detected with a flaky cable or port, which usually affect a single station. There is still a shared component that can fail—the switch itself—but if all stations lose connectivity the IT folks know what to do to resolve the problem: They usually replace the whole switch.

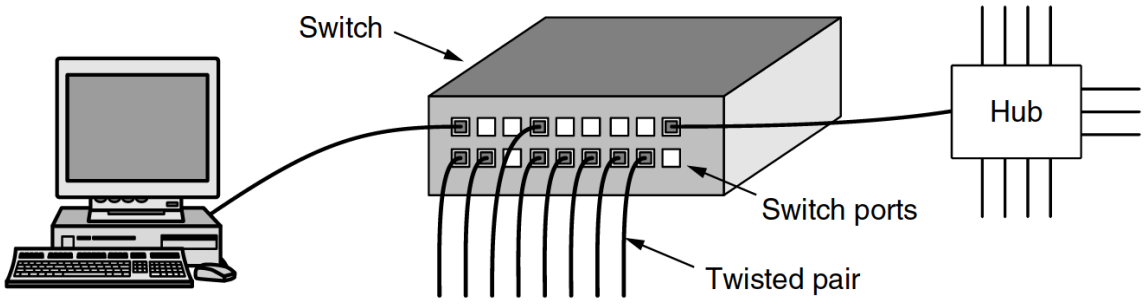

Fig. 2.3. An Ethernet switch.

In the switch, although, something very different is happening. Switches only the source frames to the ports for which these frames are selected. When a port of the switch receives a frame from computer or any station, the switch just clearly checks the Ethernet addresses to see which port the frame is intended to arrive. This step

requires the switch to be able to work out which ports correspond to which addresses, a process that we will describe in Sec. 4.8 when we get to the general case of switches connected to other switches. For now, just assume that the switch knows the frame's destination port. The switch then forwards the frame over its high-speed backplane to the destination port. The backplane usually runs at many gigabits pes second, using a proprietary protocol that does not systemization, due to it been hidden inside the switch core. The destine port then transfer the frame on the wire.

What happens if more than one of the stations or ports wants to send a frame at the same time? Again, switches differ from hubs. In a hub, all stations are in the same **collision domain**. They must use the CSMA/CD algorithm to schedule their transmissions or conveyance. In switch, individual port has its own independent collision domain. Normally the cable case is the full duplex; both the station and the port can send a frame on the cable simultaneously, without the interference of ports and stations. In the modern world, Collisions are now impossible and CSMA/CD is not require. However, if the cable is half-duplex, the station and the port must contend for transmission with CSMA/CD in the convention structure.

2.4 Fast Ethernet.

Many computers needed more bandwidth and numerous 10-Mbps LANs connected by repeaters, hubs, and switches.

Therefore, the IEEE convened a committee in 1992, with the condition of developing a faster local area network. After some discussion, the committee decided to keep 802.3 as it was originally, only to increase speed. With this strategy, everything change for technology and avoided unforeseen problems with a brand-new design. The new design would also be backward compatible. The people behind the losing proposition did what any self-respecting computer industry would do: they made standard of their own LAN which called 802.12. Which was a massive failure.

Due to the process everything was done unconventionally and resulted to the development of the, 802.3u, which was approved by IEEE in the year 1995.

As it known, the basic idea of fast Ethernet was to keep all the old frame formats, old interfaces, and just procedural rules, but only reduce the bit time just from 100 nsec to 10 nsec. In addition, the Ethernet will be better and much faster.

Choices had to be made, importantly supporting the best cable wire possible. One of the options to speed up the Internet was a twisted pair of category 3. This is because in almost every office where there are computers there were at least four twisted pairs of category 3, going to the phone cabinet within a radius of 100 meters. Quite often there were two such cables. So, using a twisted pair of category 3 would allow you to connect desktops with fast Ethernet without the need to upgrade office buildings, and this is a huge advantage for organizations.

Unfortunately, the main disadvantage of twisted pair category 3 is its inability to transmit a stable speed of 100 Mbps over a distance of 100 meters. However, the twisted pair of cat. 5 can easily carry 100 m, and the fiber can go much further. The chosen compromise was to provide all three possibilities, as shown in Fig. 2.4, but in the selection of a category 3 solution to provide it with the necessary additional load capacity.

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Figure 2.4. The original fast Ethernet cabling.

It involves sending ternary digits with three different voltage levels. This scheme is not likely to win any prizes for elegance, and we will skip the details. As it known, because standard telephone wiring usually had four twisted pairs on the cable, most offices can use existing wiring.

100Base-T4 fell by the wayside as many office buildings were rewired with Category 5 UTP for 100Base-TX Ethernet, which came to dominate the market. Actually, only two twisted pairs are used. Neither any binary coding (i.e., NRZ) nor Manchester coding is used. Instead, the 4B/5B encoding we described in Sec 2.5. Four data bits are encoded as 5 signal bits and sent at 125 MHz to provide 100 Mbps. This scheme is simple but has sufficient transitions for synchronization and uses the bandwidth of the wire relatively well. The 100Base-TX system is full duplex; stations

can transmit at 100 Mbps on one twisted pair and receive at 100 Mbps on another twisted pair at the same time.

Fast Ethernet allows interconnection by either hubs or switches. To ensure that the CSMA/CD algorithm continues to work, the relationship between the minimum frame size and maximum cable length must maintained it width as the network speed goes up from 10 Mbps to 100 Mbps. Therefore, either the minimum frame size of 64 bytes must go up or the cable length of 2500 m must come down, proportionally. The easy choice was for the maximum distance between different two stations to come down by a factor of 10, since a hub with 100-m cables falls within this new maximum already. However, 2-km 100Base-FX cables are too long to permit a 100-Mbps hub with the normal Ethernet collision algorithm. These cables must instead be connected to a switch and operate in a full-duplex mode so that there are no collisions.

3. DESIGN PART

3.1 Characteristics of the object.

The “College of Social Sciences and Humanities” (Liberia College) was founded in 1862 to provide educational access to the citizens and other nationals in Liberia.

The “College of Social Sciences and Humanities”, for which a computer network is being developed, consists of 4 buildings. In the building there are classrooms, laboratories, administrative premises (dean's office, departments, teachers), library, reading room and other additional office space.

The first building contains a room numbered from 1-01 to 1-32. The second - from 2-01 to 2-10. The third building - from 3-01 to 3-14. The fourth - from 4-01 to 4-14. Areas of educational buildings are given in table 3.1.

Table 3.1 - Area of the educational building

Building number	Building area, m^2
1	682
2	417
3	543
4	568

The “College of Social Sciences and Humanities of the University of Liberia” has one faculty, which consists of three departments: department A, department B, department C. Each department has its own classrooms, laboratories, teaching facilities, department premises, office of the head of the department.

In the first building of the college there are e-learning resources, namely: a library, a reading room, an area with Wi-Fi coverage. In the second building there is an administration and a set of e-learning resources.

The list of premises of The College of Social Sciences and Humanities of University of Liberia with the number of required information sockets is given in Table 3.2.

Table 3.2 - List of premises of Sunnyslope educational institution

№ building	Building name	Building area, m^2	Number of information sockets
1	2	3	4

1-01	Laboratory	50	8
1-02	Laboratory	52	9
1-03	Classroom	101	14
1-04	—	15	—
1-05	Department A	21	3
1-06	PTMV	21	—
1-07	Reading room	116	14
1-08	Library	46	7
1-09	Laboratory	46	7
1-10	—	78	—
1-11	Teaching A	25	4
1-12	—	24	—
1-13	Classroom	73	12
2-01	Head of the Department C	16	3
2-02	—	16	—
2-03	—	16	—
2-04	VTMV -1	14	—
2-05	Dean	18	3
2-06	Deanery	30	5
2-07	—	11	—
2-08	Teaching C	29	5
2-09	WI-FI Zone	163	1
2-10	—	12	—
3-01	Laboratory	51	8
3-02	—	51	—
1	2	3	4
3-03	Laboratory	51	8
3-04	—	51	—
3-05	Head of the Department A	14	2
3-06	—	12	—

3-07	—	16	—
3-09	Head of the Department B	15	2
3-10	—	50	—
3-11	Classroom	50	8
3-12	Classroom	52	8
3-13	Laboratory	52	8
3-14	—	6	—
3-15	—	13	—
3-16	VTMV -2	13	—
3-17	Department B	19	3
4-01	Department C	36	6
4-02	—	56	—
4-03	Laboratory	56	8
4-04	—	56	—
4-05	Classroom	56	9
4-06	VTMV -3	15	—
4-07	—	15	—
4-08	—	18	—
4-09	Teaching B	18	3
4-10	—	18	—
4-11	—	56	—
4-12	Classroom	56	9
4-13	Office	56	9
4-14	Laboratory	56	9

So, the total number of required sockets in the College of Social Sciences and Humanities in the University of Liberia is 195.

3.2 Computer network requirements analysis.

In accordance with the tasks set before us, the computer network must provide adequate operation in three main modes:

- full-time;
- maintenance mode;
- emergency.

The normal mode of operation should be the main mode of operation of all components of the computer network and ensure the use of backup facilities to ensure load balancing between the main and backup software and hardware of the information and communication system of the organization.

The emergency mode of operation must guarantee full or partial availability of public access services at the expense of the provided means of reservation. The reason for the use of means of redundancy may be a one-time failure of the main set of telecommunications.

Developed technical solutions for creating a computer network should ensure its operation 24/7/365. Temporary restriction of full-featured availability of certain information resources is allowed:

- as a result of abnormal situations caused by one-time failures in the operation of hardware and / or software of the computer network; ·
- during the periods of routine maintenance of software and hardware and software of the computer network, provided by the operating documentation.

To organize interconnection, the TCP / IP v4 / v6 protocol stack should be used as the main one for all modern information and telecommunication systems.

Shared information services: DNS, HTTPS.

Information services with limited access: DHCP, FTP.

The structural composition of a computer network includes a central (primary) telecommunication node (PTMV), which logically forms the core level, secondary

telecommunication nodes (VTMV), which determine the level of aggregation, and local telecommunication nodes (LTMV), which determine the access level.

Telecommunication nodes PTMV and VTMV must be located in separate dedicated technical rooms. It is allowed to place LTMV in telecommunication cabinets of the closed type of wall execution.

The service "Internet access" is provided subject to the following requirements:

- use of the main wired communication channel at speeds up to 100 Mbps;
- use of a backup wired communication channel up to 20 Mbit / s;
- provision of additional services of the Internet provider:
  - allocation and routing of a block of permanent IP addresses from the address space of the operator;
  - routing of the autonomous system of the organization;
  - support for domain names of the organization on the primary and secondary DNS servers;
  - access to the statistics server and service management server;
  - protection against DDoS attacks;
  - remote antivirus protection;
  - remote content filtering of Internet traffic.

The wireless access network should be built using the following standards:

- IEEE 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA;
- IEEE 802.11b/g, IEEE 802.11n, IEEE 802.11s, IEEE 802.11h, IEEE 802.11d;
- IEEE 802.1X;
- IEEE 802.3af.

The wireless access network must provide:

- a continuous coverage area within the established limits selected during design in coordination with the customer;
- secure and guest access;
- productivity. Designed for peak loads for each zone;

- extensibility without interrupting the network
- ensuring continuous communication of the subscriber when switching from one wireless access point to another.

3.3 Description of information resources and services.

3.3.1 Sharing services.

HTTP is a well-known simple request-response protocol that typically works on TCP. It determines which messages clients send to servers and which they receive in response. Requests and answers are submitted in ASCII, SMTP. Content is presented in a format similar to MIME, as in SMTP. This model simplified development and deployment and contributed to the early success of the Internet.

The main purpose of the HTTP protocol is to transfer web pages (text files with HTML markup), although it successfully transmits other files that are related to web pages (images and applications) and not related to them (in this HTTP competes with more complex FTP). HTTP assumes that the client program - a web browser - is able to display hypertext web pages and other types of files in a user-friendly form. To display correctly, HTTP allows the client to learn the language and encoding of the web page and / or request the version of the page in the desired language / encoding using MIME notation. Usually, the HTTP port number is 80. HTTP is an application layer protocol, similar to FTP and SMTP. The exchange of messages follows the usual "request-response" scheme. HTTP uses global URIs to identify resources. Unlike many other protocols, HTTP does not retain its state. This means that there is no intermediate state between the request-response pairs. Components that use HTTP can independently store information about the status associated with recent requests and responses. The server can store the IP addresses and request headers of recent clients.

DNS (Domain Name System) is a distributed computer system for obtaining information about domains. It is most often used to obtain an IP address by host name (computer or device), to obtain information about mail routing, hosted nodes for protocols in the domain (SRV-record).

A distributed DNS database is supported by a hierarchy of DNS servers that interact over a specific protocol.

The modern DNS system includes three main components:

- distributed database of domain names (DNS database);
- name servers;
- client programs for determining IP addresses (name resolver).

The domain name space resembles a tree-like file structure (see Figure 3.1).

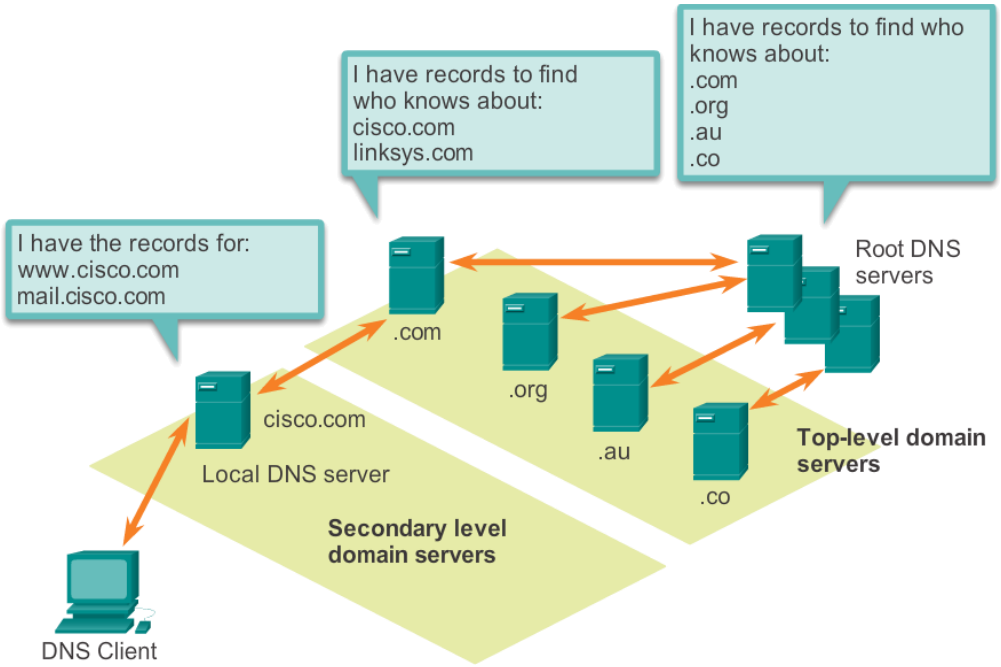

Fig. 3.1 - Fragment of the structure of the domain name space/

The root of this tree is marked with the symbol "." (point). This character must be at the end of each domain name, but it is not placed in the user interface format. In records in the database, the absence of this point is a gross error.

The contents of the DNS database are adjusted manually in text files, after which the program creates database lines from these files, called resources records. This database has the following six fields:

– NAME – resource name (255 byte);
– TYPE – resource type;
– CLASS – resource class;
– TTL – the time the resource record is stored in the user's memory;
– RDLENGTH – data field length (number to 65535);
– RDATA – data (up to 65535 byte);

DNS servers relative to the source of information are:

- primary or primary (Primary Name Server), in which the database is filled in and adjusted manually;

- auxiliary or secondary (Secondary Name Server), in which the database is regularly copied from the main server;

- caching (Cache only Server), storing cached information.

The master and slave DNS servers must be located on different networks. It is necessary that there is at least one auxiliary server. The server can be both master for some zones and auxiliary for others.

3.3.2 Restricted services.

SYSLOG is a standard for sending and registering messages about events in the system, used in computer networks running over the IP protocol. The essence of the Syslog mechanism is simple and remains unchanged to this day with minor variations: the sources generate simple text messages about events in them and send them to the Syslog server (called "syslog", "syslog daemon", or "syslog server"). using one of the IP networks protocols (UDP or TCP). Event messages are generated and transmitted according to certain rules, called the Syslog protocol. Typically, the message is small (up to 1024 bytes) and sent in the open. However, when using special tools (such as Stunnel, sslio or sslwrap), it is possible to encrypt messages and send them via SSL / TLS.

Because message sources and the Syslog server can be located on different machines, this allows you to organize the collection and storage of messages from multiple geographically disparate sources in a single repository, which is extremely important for network administrators who may not have physical access to all devices and computers. users in the network.

Also, Syslog servers can usually not only register messages, but also forward them to other Syslog servers, based on the level of importance of the message (Severity) and the category of message generated entity (Facility), which allows you to organize, for example, a hierarchical storage system. And this can help, for example, reduce staff response time to critical events. Suppose there is a large network consisting of several

segments. Each segment has its own Syslog server, which receives messages only from sources within its segment.

The current version of Syslog offers an improved message format that allows you to use accurate estimation of message creation time and reliable identification of the message source, as well as apply UTF-8 encoding to the message text, which solves the problem of internationalization. Optional additional fields (structured data) can be used to transmit various information, for example, about the errors of the local clock of the message source and the accuracy of their synchronization with the external clock of the exact time, the language in which the message is written, etc. to unlink a specific transport, Syslog can use any of the message delivery mechanisms described in the individual RFCs, but TLS transports are preferred.

DHCP (Dynamic Host Configuration Protocol) is a standard protocol that allows computers to automatically obtain the IP address and other settings needed to work on a network. To do this, the computer accesses the DHCP server. The network administrator can specify a range of addresses to be distributed between computers. This avoids manually configuring network computers and reduces errors. DHCP is used in most large TCP / IP networks.

DHCP is an extension of the BOOTP protocol previously used to provide diskless workstations with IP addresses when they load. DHCP retains backward compatibility with BOOTP.

In addition to the IP address, DHCP can also inform the client of additional parameters required for normal network operation. These parameters are called DHCP options. A list of standard options can be found in RFC 2132. Some of the most commonly used options are:

- IP address of the default router;
- subnet mask;
- DNS server addresses;
- DNS domain name.

Some software vendors may specify their own, optional DHCP options.

The DHCP protocol works on the client-server scheme. When the system starts, the computer, which is a DHCP client, sends a request to the network for an IP address.

The DHCP server responds and sends a response message that contains the IP address and some other configuration settings. The DHCP server can operate in various modes, including: dynamic distribution, automatic selection, static distribution.

DHCP is built so that a client can request multiple servers at once.

A DHCP client that requires an address sends a broadcast DHCPDISCOVER packet in search of a server. The package contains the hardware address of the client requester. Then one or more DHCP servers consider the request and send a response to the DHCPOFFER packet containing the proposed IP address and "lease time".

The client selects the address from the received DHCPOFFER packets. The choice of the client depends on his destination - for example, he can choose the address with the longest rental time. The client then sends a DHCPREQUEST packet to the address of the selected server.

The selected server sends a confirmation (DHCPACK) and the negotiation process is completed. The DHCPACK package contains the agreed address and rental time. The server marks the selected address as busy - until the end of the lease, this address cannot be assigned to another client. The client only has to configure himself according to the sent data and you can start working in the network.

Therefore, multiple servers can respond to a DHCPDISCOVER request. The client must select one of the offers and send a DHCPREQUEST packet in response with the ID of the selected server. Other servers review the DHCPREQUEST package and conclude based on the server ID that their offer was rejected. This way, they know that the IP addresses they offer are free to assign to other clients.

If the server cannot accept the configuration, it sends a DHCPNAK (denial of confirmation) packet, forcing the client to start the negotiation process again.

Based on this, if there are two DHCP servers in the network with different configurations, there is no guarantee that the client will select a specific server.

3.4 Rationale for the physical topology of a computer network.

Computer network topology is the physical location of network computers relative to each other and the way they are connected by communication lines.

The choice of topology has a great influence on a number of network characteristics. The ease of connecting new nodes, which is inherent in some topologies, makes the computer network easily extensible. Economic considerations often lead to the choice of topologies, which are characterized by a minimum total length of communication lines.

The "extended star" physical topology was chosen to build the computer network. In this topology, each computer is connected by a separate cable to a common device - in this case a switch.

Each node included in the central device is the center of another star.

The main advantage of this topology is significantly increased reliability. Any cable problems only affect the computer to which the cable is connected, and only a switch failure can disable the entire network. In addition, the switch can act as an intelligent filter for information coming from the nodes to the network, and if necessary, block the transmissions prohibited by the administrator.

The disadvantage of the extended star topology is the higher cost of network equipment, due to the need to purchase switches. In addition, the ability to increase the number of nodes in the network is limited by the number of ports on the switch. Sometimes it makes sense to build a network using multiple switches, hierarchically interconnected by connections such as "extended star".

Today, the "extended star" is the most common type of connection topology in both local and global networks.

3.4.1. Consolidated calculation of options for technical means of telecommunications.

The following types of equipment were selected to build the computer network of the College of Social Sciences and Humanities of University of Liberia:

- router;
- firewall;
- OSI model level 3 switch, 24 x 100Mbps, 2 x 1000Mbps;
- OSI level 2 switch (unmanaged), 8 x 100Mbps;
- OSI model level 2 switch (unmanaged), 16 x 100Mbps;
- wireless access point;

Tables 3.3 - 3.7 show the comparative characteristics of network devices.

Table 3.3 - Comparative characteristics of firewalls

Name	Cisco ASA5505-K8	D-Link DFL-260E
Interfaces	6xRJ-45 10/100Base-Tx, 2xRJ-45 10/100Base-Tx, PoE	7xRJ-45 10Base-T/100Base-Tx/1000Base-Tx
Another ports	3xUSB 2.0, 1xRJ-45 (consol)	2xUSB 2.0, 1xRJ-45 (consol)
Slots	1xSSC	no
Capacity, Mbps	150/100(3DES/AES/VPN) /75(AIP-SSC-5)	150/45(VPN)/60(IPS)
Number of simultaneous sessions.	10000 (25000 з Cisco ASA 5505 Security Plus license)	25000
Number of VPN sessions	10(IPSec)/2(SSL)	100 (IPSec)
NAT	support	support

Table 3.4 - Comparative characteristics of level 3 switches

Name	Cisco Catalyst 3560-24TS	D-Link DES-3828
Fast Ethernet ports	24	24
Gigabit Ethernet ports	2	2
VLAN	4 000	4,000 static and 255 dynamic groups
MAC table	12 00 records	16 000 records
Cash	128 mb	32 Mb
Port Trunking	support	support
Management	command line interface	Web, SNMP, command line interface
Energy consumption	27 W	24 W
NAT	support	support

Table 3.5 - Comparative characteristics of 8-port level 2 switches

Name	Cisco SB SG110D	TP-LINK TL-SG1008P
Interfaces	8x Gigabit Ethernet (10/100/1000 Mbps)	8x Gigabit Ethernet (10/100/1000 Mbps)
The speed of the switching matrix	16 Gbps	16 Gbps
Energy consumption	32 W	63 W
MAC address table size	4000	1000
Remote control	Unmanageable	Unmanageable
PoE support	support	support

Table 3.6 - Comparative characteristics of 16-port level 2 switches

Name	Cisco SF 110D-16	D-Link DES-1016C
Interfaces	16x Fast Ethernet, (10/100/1000 Mbps),	16x Fast Ethernet, (10/100/1000 Mbps),
Jumbo Frame	9 216 bytes	9 216 bytes
The speed of the switching matrix	3,2 Gbps	3,2 Gbps
Energy consumption	64 W	5 W
MAC address table size	8 000	8 000
Remote control	Unmanageable	Unmanageable

Standart support	IEEE 802.3 10 BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000 BASE-T Gigabit Ethernet, IEEE 802.3z Gigabit Ethernet, PoE	Auto MDI/MDIX, Jumbo Frame, IEEE 802.1p (Priority tags)

Table 3.7 - Comparative characteristics of wireless access points

Name	Cisco SB WAP121-E-K9-G5	TP-LINK TL-SG1008P
Operating mode	Access point, repeater, bridge	Access point
Wi-Fi speed	300 Mbps	867 Mbps
Wi-Fi version	802.11 b/g/n	802.11 a/b/g/n/ac
Wi-Fi frequency	2,4 GHz	2,4 GHz, GHz
Antenna design	internal	internal
PoE support	support	support
Power	12 B, 1A DC, 802.3, PoE	PoE or from an external power source 12 V, 1,5 A DC

The Cisco ASA5505-K8 firewall, Cisco 2811 router, Cisco Catalyst 3560-24TS Layer 3 switch, 8-port Cisco SB SG110D Layer 2 Unmanaged 2-Port Unit, 16-Port Unmanaged Cisco Switch 2 were selected to design the College of Social Sciences and Humanities University of Liberia computer network. SF 110D-16 and TP-LINK TL-SG1008P wireless access point.

3.4.2 Computer network structure.

The main logical segments of the computer network of the College of Social Sciences and Humanities University of Liberia are:

- network for shared servers;
- network for restricted access servers;
- network for wireless access point;
- networks for computers located in the first case;
- network to connect network devices.

Each segment of the computer network must have access to the Internet. A firewall is used to protect against external attacks.

Figure 3.2 shows the general block diagram of the network.

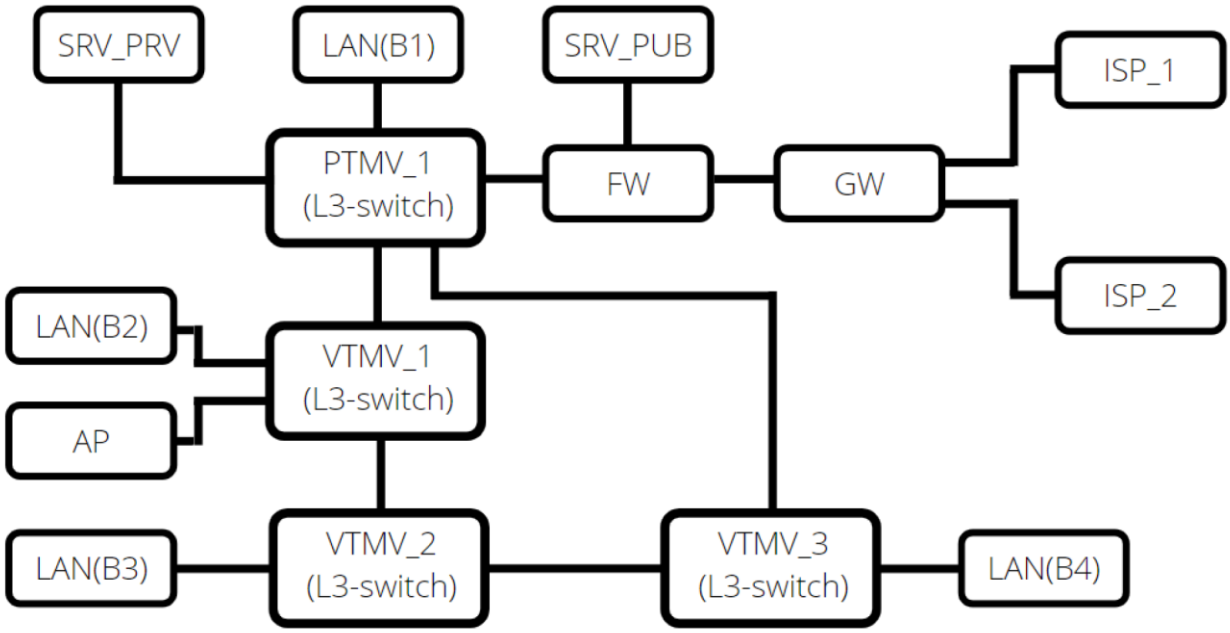

Fig. 3.2 - Block diagram of a computer network

4 SPECIAL PART

4.1 Selection of active network equipment.

In accordance with the requirements of the network and the plan of the premises for the operation of the designed computer network, the following network equipment must be provided.

Building 1:

• 1 router to connect to Internet service providers;

• 1 firewall;

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 3 switches of 2 levels of the OSI model (unmanaged), 8 x 100 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

Building 2:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 2 level 2 switches of the OSI model (unmanaged), 8 x 100 Mbps;

• 1 wireless access point.

Building 3:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

Building 4:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 1 switch of the 2nd level of the OSI model (unmanaged), 8 x 100 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

Table 4.1. lists the active network equipment, its description and characteristics.

Name	Classroom	Model	Number of ports	
			Fast Ethernet	Gigabit Ethernet
1	2	3	4	5
PTMV_1	1-06	Cisco Catalyst 3560-24TS	24	2
Firewall	1-06	Cisco ASA5505-K8	8	—

PTMV_GW	1-06	Cisco 2811	3	—
SW_101	1-01	Cisco SF 110D-16	16	—
SW_102	1-02	Cisco SF 110D-16	16	—
SW_103	1-03	Cisco SF 110D-16	16	—
SW_107	1-07	Cisco SF 110D-16	16	—
SW_108	1-08	Cisco SB SG110D	8	—
SW_109	1-09	Cisco SB SG110D	8	—
SW_111	1-11	Cisco SB SG110D	8	—
SW_112	1-12	Cisco SF 110D-16	16	—
SW_113	1-13	Cisco SF 110D-16	16	—
VTMV_1	2-04	Cisco Catalyst 3560-24TS	24	2
SW_206	2-06	Cisco SB SG110D	8	—
SW_208	2-08	Cisco SB SG110D	8	—
Access Point	2-09	TP-LINK TL-SG1008P	1	—
VTMV_2	3-16	Cisco Catalyst 3560-24TS	24	2
SW_301	3-01	Cisco SF 110D-16	16	—
SW_303	3-03	Cisco SF 110D-16	16	—
SW_311	3-11	Cisco SF 110D-16	16	—
SW_312	3-12	Cisco SF 110D-16	16	—
SW_313	3-13	Cisco SF 110D-16	16	—
VTMV_3	4-06	Cisco Catalyst 3560-24TS	24	2
SW_401	4-01	Cisco SB SG110D	8	—
SW_403	4-03	Cisco SF 110D-16	16	—
SW_405	4-05	Cisco SF 110D-16	16	—
SW_412	4-12	Cisco SF 110D-16	16	—
SW_413	4-13	Cisco SF 110D-16	16	—
SW_414	4-14	Cisco SF 110D-16	16	—

The total amount of network equipment required for the operation of the projected computer network:

- 4 Cisco Catalyst 3560-24TS switches;
- 16 Cisco SF 110D-16 switches;
- 6 Cisco SB SG110D switches;
- 1 wireless access point TP-LINK TL-SG1008P;
- 1 Cisco ASA5505-K8 firewall;
- 1 Cisco 2811 router.

4.2 Calculation of logical addressing.

To optimize network traffic and increase the security of the University of Liberia's computer network, the 10.14.0.0./16 logical network was segmented into the network IP address mask / 20. From the received 16 subnets / 20 IP addresses of the network are allocated on cases 2 ranges of IP addresses with a mask / 20, on a wireless access point / 20, on the main channels between TMB / 20, on the server of limited access / 20.

Appendix A provides a detailed scheme of network IP addressing.

4.3 Switching.

4.3.1 Switch Setup

Basic switch setup includes:

- Specifying a device name;
- Setting up a user database on the switch with the appropriate logins and passwords; ·
- Password setting in configuration modes;
- Setting up access via virtual communication lines;
- Setting up access over physical lines of communication;
- Banner settings;
- Enable password encryption in the configuration file;
- Initial closing of all communication interfaces;
- Security settings.

Appendix B lists the configuration files of the PTMV_1, VTMV_1, VTMV_2, VTMV_3 level switches.

4.3.2 VLAN settings

A virtual local area network (VLAN) is used to protect a network from unauthorized access. That is, at the channel level, frames from other VLANs will be discarded by the switch port regardless of the source IP address of the packet in that frame. VLAN also allows you to build a network whose logical structure does not depend on the physical.

Appendix B lists all virtual local area networks and their names according to the developed IP address scheme.

Appendix B lists all VLAN settings in the PTMV_1, VTMV_1, VTMV_2, VTMV_3 switch configuration files.

4.3.3 Configuring the connection redundancy protocol.

An effective solution when using redundant connections is the Spanning Tree Protocol (STP) - a channel layer protocol that is used to maintain a network state in which there is no network loops. Cisco has its own implementation of the STP protocol PVST (Per-VLAN Spanning Tree), which extends the functionality of STP and is designed to work with multiple VLANs. In PVST, there is an STP process for each VLAN that allows independent and flexible configuration for each VLAN, and also allows the use of load balancing due to the fact that a particular physical link can be blocked in one VLAN but work in another.

4.3.4 Organization of wireless access.

To provide wireless access in the first case, you must configure DHCP Server in the range of 10.14.193.0/24 and configure the wireless access point accordingly.

4.4 Routing.

4.4.1 Configuring routers.

In order to provide all nodes of the College of Social Sciences and Humanities University of Liberia network with uninterrupted Internet access to the PTMV_1-GW router, two Internet providers (main and backup) were connected at the same time.

Configuring PTMV_1-GW router interfaces:

```
!
interface FastEthernet 0/0
description link-to-isp1
ip address 194.44.136.1 255.255.255.252
!
ip nat outside
duplex auto
speed auto
!
interface FastEthernet 0/1
description link-to-isp2
ip address 205.7.5.129 255.255.255.252
ip nat outside
duplex auto
speed auto
!
interface FastEthernet 1/0
description link-to-inside
ip address 201.100.11.6 255.255.255.248
ip nat inside
duplex auto
speed auto
!
```

Specify the pool of external addresses to which internal addresses will be broadcast:

ip nat pool NAT-POOL 201.100.11.8 201.100.11.15 netmask 255.255.255.248

Enabling NAT on the PTMV_1-GW router:

ip nat inside source list NAT-ACL pool NAT-POOL overload

This command tells the router that for all packets received on the internal interface and allowed by the NAT-ACL access list, the sender's address will be broadcast to the address from the NAT pool "NAT-POOL". The overload key indicates that the broadcasts will be overloaded, allowing multiple internal nodes to be broadcast on a single IP address.

4.4.2 Interconnection.

The EIGRP protocol is used as the routing protocol for the VLAN in the College of Social Sciences and Humanities University of Liberia network.

EIGRP is a proprietary routing protocol based on the old IGRP protocol. EIGRP is a remote-vector routing protocol that has been optimized to reduce protocol instability after topology changes of the network, avoid the problem of route looping and more efficient and economical use of router capacity.

The route determination algorithm is based on the Dijkstra depth search algorithm on the graph. EIGRP calculates and takes into account 5 parameters for each section of the route between network nodes:

- Total Delay - total transmission delay (to the nearest microsecond);
- Minimum Bandwidth - minimum bandwidth (in Kbps - kilobits / second);
- Reliability - reliability (score from 1 to 255; 255 - the most reliable);
- Load - download (score from 1 to 255; 255 - the most reliable);
- Maximum Transmission Unit (MTU) (not taken into account when calculating the optimal route, taken into account separately) - the maximum block size that can be transmitted along the route.

The EIGRP protocol settings on the PTMV_1 and VTMV_1, VTMV_2, VTMV_3 switches are listed in Appendix B.

4.5 Organization of Internet access

4.5.1 Internet access technology

A firewall is a network access control device designed to block all traffic except permitted data. This is different from a router, the function of which is to deliver traffic to the destination in the shortest possible time.

The firewall also hides the internal network addressing scheme.

To ensure secure, reliable, and efficient interoperability of LAN devices, you must also configure Access Control Lists.

With NAT (Network Address Translation) technology, you can connect almost any number of computers to your network using one or more external IP addresses issued by your ISP.

NAT is a mechanism for changing the network address in the headers of IP datagrams as they pass through the routing device to display one address space to another.

4.5.2 Hardware means of Internet access.

To provide Internet access at the University of Liberia, using two Internet providers (primary and backup) uses a limit device such as a Cisco 2811 router.

The Cisco ASA5505-K8 firewall is used to secure the school's network. This device monitors incoming and outgoing network traffic and, based on an established set of security rules, decides to skip or block specific traffic.

5. OCCUPATIONAL SAFETY AND HEALTH

Occupational safety and health issues are considered for the design and development phase of climate data analysis and visualization system.

Occupational safety is a system of legal, socio-economic, organizational and technical, sanitary and hygienic and treatment and prevention measures and tools aimed at preserving human life, health and ability to work. Working conditions at the workplace, safety of technological processes, machines, mechanisms, equipment and other means of production, condition of collective and individual protection means used by the employee, as well as sanitary and living conditions must meet the requirements of the law. An employee has the right to refuse the assigned work if a work situation has arisen that is dangerous to his life or health or to the people around him, or to the work environment or the environment. He must immediately notify his immediate supervisor or employer. The existence of such a situation is confirmed, if necessary, by labor protection specialists of the enterprise with the participation of a representative of the trade union of which he is a member or a person authorized by employees on labor protection (if the trade union was not established), as well as an insurance expert [12]. The task of labor protection is to minimize injuries and illnesses of the employee while ensuring comfort with maximum productivity. The main objectives of labor protection are the formation of specialists with the necessary knowledge and practical skills on legal and organizational issues of labor protection, industrial sanitation, safety, fire safety.

4.1. General characteristics of the room and workplace

The development of the analysis and visualization system is performed in a room located on the fourth floor of an eight-storey building with general and local lighting. The room has one-sided lighting, the windows are oriented to the east, the windows have shutters. White ceiling with a reflection coefficient of 0.7, light brick walls with a reflection coefficient of 0.5. There are 4 people working in the room, in accordance with this we obtain input data for the analysis of potentially dangerous and harmful production factors, which are given in table. 5.1.

Table 5.1

Incoming data

Room parameters	**Value**
Length x width x height	6.6 x 6.1 x 2.7 m
Area	40.26m²
Volume	108,70 m³
Workplace number	**Specifics of work**
I workplace	Front-end programmer (web application client development specialist)
II workplace	Back-end programmer (specialist in the development of the server part of web applications and database design)
III workplace	Business analyst (also acts as a product manager)
IV workplace	UI-UX web designer
Technical means (quantity)	**Name and characteristics**
Monitor (4 pcs.)	HP 22Xi / 21.5 "/ 1920x1080px / IPS
Computer (4 pcs.)	HP ProBook 440 G6, 14 "IPS screen (1920x1080) Full HD, Intel Core i7-8565U (1.8 - 4.6 GHz) / RAM 16 GB / SSD 256 GB
Floor cooler (1 piece)	CRYSTAL YLR3-5V208
Air conditioner (1 piece)	DEKKER DSH105R / G / 26m2 / 2,65kW- 2.9 kW / 25x74.5x19.5 cm / 9 kg
General purpose luminaries (3 pcs.)	The lamp raster built-in 4x18W
Local lamps (4 pcs.)	Delux Decor TF-05/1 x 40W

According to NPAOP 0.00-7.15-18 [14], the area S 'allocated for one workplace with a personal computer must be at least 6 m2 and the volume - at least 20 m3. There are 4 workplaces in the room, which fully meets the required standards.

We calculate the actual values of these indicators by dividing the volume of the room and the total area by the number of employees.

Therefore, based on the results obtained in terms of area and volume, the room meets the standards.

Table 5.2

Workplace characteristics

№	The name of the parameter	Value	
		in fact	Normative
1.	Height of a working surface, mm	780	680 – 800
2.	Width of a working surface, mm	1500	not less than 600
3.	Depth of a working surface, mm	750	not less than 600
4.	Height of space for legs, mm	750	not less than 600
5.	Width of space for legs, mm	800	not less than 500
6.	Depth of space for legs, mm	750	not less than 450
7.	Seat surface height, mm	480	400 – 500
8.	Seat width, mm	500	not less than 400
9.	Seat depth, mm	500	not less than 400
10.	Height of a basic surface of a back, mm	550	not less than 300
11.	Width of a surface of a back, mm	470	Not less than 380
12.	Length of armrests, mm	300	not less than 250
13.	Width of armrests, mm	60	50 – 70
14.	Distance from eyes to the screen, mm	650	600 – 700

It is possible to draw a conclusion that the sizes of a workplace of the programmer correspond to the established norms, proceeding from the set parameters.

4.2. Analysis of potentially dangerous and harmful production factors in the workplace

When creating a system of analysis and visualization, the work is performed sitting without physical effort, so it belongs to the category of light Ia.

Premises for work must be equipped with heating, air conditioning or supply and exhaust ventilation in accordance with DBN B.2.5-67: 2013. Normalized parameters of the microclimate, ionic composition of air, content of harmful substances meet the requirements of LTO 3.3.6.042-99, GN 2152-80, GOST 12.1.005-88, DSTU GOST 12.0.230: 2008 and DSTU GOST 12.4.041: 2006. Ventilation is understood as a set of measures and means designed to ensure meteorological conditions and cleanliness of the air environment that meet hygienic and technical requirements at permanent places and service areas. The main task of ventilation is to remove polluted, humid or heated air from the room and supply clean fresh air.

The sources of noise in the room are the fan of the system unit, laptop and air conditioner. The sound generated by the fan and air conditioner can be classified as constant.

According to DBN B.2.5-28: 2018 the work belongs to the category of visual works. The use of natural, artificial and mixed lighting is envisaged.

The computer is a single-phase consumer of electricity powered by 220V AC from a network with grounded neutral. IBM PC refers to electrical installations up to 1000V closed version; all conductive parts are in the casings. According to the method of protecting a person from electric shock, computers and peripherals must meet 1 class of protection.

Technical methods of protection against electric shock is reduced to the use of current of safe voltage, protection in case of accidental touching current-carrying parts and against excessive currents, protection in case of voltage transfer to non-current-carrying metal parts of the installation.

Safe voltage is obtained from the high voltage grid (110-120 V) by means of step-down transformers.

Protection against contact with live parts of the installation is achieved by means of insulation, fencing off the use of blocking safety devices and inaccessibility of the location of the installations.

Switchboards are placed in closed metal casings-boxes.

Safety alarm is used in the form of posters and inscriptions. The best light alarms are double, which in the presence of voltage lights a red light, and in its absence - green.

Protection against excessive currents - short circuits and overload currents, which can cause insulation to ignite, is provided by fuses and circuit breakers, and protection against voltage transfer to live parts by means of protective earthing and protective disconnection.

Fire prevention is achieved by eliminating the formation of sources of ignition and combustible environment.

Fires of the following classes are possible in this room: A - combustion of solids, E - combustion of live electrical installations.

CONCLUSIONS

A computer network of the College of Social Sciences and Humanities University of Liberia was **DEVELOPED**.

The requirements for the computer network were analyzed, the choice of the physical topology "extended star" was substantiated, and the consolidated calculation of the network equipment was performed. The structural scheme, physical and logical topology, the scheme of connections and IP-addressing of a computer network are made and developed.

The choice of network architecture for the computer network, access methods, topology, type of cable system, operating system, applications, protocols is substantiated. The choice of network management method, network equipment is substantiated and simulated network in the Cisco Packet Tracer emulator.

Basic documentation has been prepared: network diagrams at the physical, channel and network levels, IP-addressing plan, list of devices.

Access to the Internet, private and public servers from all network devices of the school is organized. Wi-Fi is also provided in the building.

REFERENCES

1. Tanenbaum A. Computer networks 5-th edition / A. Tanenbaum, D. Wetherall. 2011. – 960 з.
2. Peterson L.L. / - Computer Networks: A Systems Approach, 6th edition / Peterson L.L., Davie B.S., 2021. – 850 p.
3. V. Olifer– Computer networks. Principles, technologies, protocols. / V. Olifer, N. Olifer, 2020/ – 1010 p.
4. James F. Kurose– Computer Networking. Sixth edition/ James F. Kurose, Keith W. Ross, 2009 / – 862 p.
5. White Russ – Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks 1st Edition/ White Russ, Banks Ethan, 2017 / – 1369 p.
6. Douglas E. Comer – Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th Edition) / Douglas E. Comer, 2013 / – 744p.
7. Quinn L., Russell R. Fast Ethernet. New York, John Wiley and Sons, 1997, 417 p.
8. Brian Hill – Cisco: The Complete Reference / Brian Hill, 2002 / – 838p.
9. Kulakov MA, Lyapun VO, Soft VO etc. Civil defense: a textbook. Kharkiv: Fakt, 2008.
10. Shobotov VM Civil defense: a textbook. K .: Center for Educational Literature, 2004.
11. Norms for determining the categories of premises, buildings and outdoor installations for explosion and fire hazard. NAPB B.03.002-2007. (approved by the order of the Ministry of Emergencies of Ukraine dated 03.12.2007 № 833).
12. LTO 3.3.6.042-99. Sanitary norms of microclimate of industrial premises [Text]. K., 2000. 16 p.
13. URL:https://www.researchgate.net/publication/2996873_The_OSI_reference_model

14. URL:http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.
15. URL:https://www.imperva.com/learn/application-security/osi-model.

APPENDIX A

IP addressing scheme

General network address 10.14.0.0/16

Table A1. Scheme of IP-addressing of cases and network segments of special use.

Network segment name	Network IP address	IP address mask	Function
IP network address - building 1	10.14.16.0	255.255.240.0	Summarized IP address
IP network address - building 2	10.14.32.0	255.255.240.0	Summarized IP address
IP network address - building 3	10.14.48.0	255.255.240.0	Summarized IP address
IP network address - building 4	10.14.64.0	255.255.240.0	Summarized IP address
IP- network address - WiFi	10.14.192.0	255.255.240.0	Summarized IP address
Network IP address - shared servers	201.100.11.0	255.255.255.224	IP addresses issued by the Boarding Service provider, summarized
Network IP address - restricted servers	10.14.208.0	255.255.240.0	Summarized IP address
Network IP address - Connection of network devices	10.14.224.0	255.255.240.0	Summarized IP address

Table A2. Scheme of IP-addressing of network segments of building 1.

Network segment name	Cabinet number	Number of PCs	Network IP address / IP address mask	Range of IP address nodes		Default IP address of the gateway	Belonging to a VLAN	
				First IP address	Last IP address		VLAN number	VLAN name
SW 101	1-01	8	10.14.16.0/27	10.14.16.1	10.14.16.29	10.14.16.30	**101**	Labl0l
SW 102	1-02	9	10.14.16.32/27	10.14.16.33	10.14.16.61	10.14.14.62	102	Labl02
SW 103	1-03	14	10.14.16.54/27	10.14.16.65	10.14.16.93	10.14.16.94	103	Class 103
PC 105	1-05	3	10.14.16.96/29	10.14.16.97	10.14.16.101	10.14.16.102	105	KafA105
SW 107	1-07	14	10.14.17.0/27	10.14.17.1	10.14.17.29	10.14.17.30	107	Readrooml07
SW 108	1-08	7	10.14.17.32/27	10.14.17.33	10.14.17.61	10.14.17.62	108	Library109
SW 109	1-09	7	10.14.17.64/27	10.14.17.65	10.14.17.93	10.14.17.94	109	Lab109
SW 111	1-11	4	10.14.17.96/28	10.14.17.97	10.14.17.109	10.14.17.110	**111**	TeachA111
SW 113	1-13	12	10.14.17.128/27	10.14.17.129	10.14.17.157	10.14.17.158	И3	Class 113

Table A3. Scheme of IP-addressing of network segments of building 2.

Network segment name	Cabinet number	Number of PCs	Network IP address / IP address mask	Range of IP address nodes		Default IP address of the gateway	Belonging to a VLAN	
				First IP address	Last IP address		VLAN number	VLAN name
PC 201	2-01	3	10.14.32.0 /29	10.14.32.1	10.14.32.5	10.14.32.6	201	ZavC201
PC 205	2-05	3	10.14.32.8 /29	10.14.32.9	10.14.32.13	10.14.32.14	205	Dec205
SW 206	2-06	5	10.14.32.16/28	10.14.32.17	10.14.32.29	10.1422.30	206	Dect206
SW 208	2-08	5	10.14.32.32/28	10.14.32.33	10.14.32.45	10.14.32.46	208	TeachC20S

Table A4. Scheme of IP-addressing of network segments of building 3.

Network segment name	Cabinet number	Number of PCs	Network IP address / IP address mask	Range of IP address nodes		Default IP address of the gateway	Belonging to a VLAN	
				First IP address	Last IP address		VLAN number	VLAN name
SW 3OÏ	3-01	8	10.14.48.0/27	10.14.48.1	10.14.48.29	10.14.48.30	301	Lab301
SW 303	3-03	8	10.14.48.33/27	10.14.48.33	10.14.48.61	10.14.48.62	303	Lab303
PC 305	3-05	2	10.14.48.64/29	10.14.48.65	10.14.48.69	10.14.48.70	305	Kaf3O5
PC 309	3-09	2	10.14.48.72/29	10.14.48.73	10.14.48.77	10.14.48.78	309	ZavK309
SW 311	3-11	8	10.14.48.96/27	10.14.48.97	10.14.48.125	10.14.48.126	311	Class311
SW 312	3-13	8	10.14.48.128/27	10.14.48.129	10.14.48.157	10.14.48.158	312	Class312
SW 313	3-13	8	10.14.48.160/27	10.14.48.161	10.14.48.189	10.14.48.190	313	Lab313
PC 317	3-17	2	10.14.48.192/29	10.14.48.193	10.14.48.197	10.14.48.198	317	KafB317

Table A5. Scheme of IP-addressing of network segments of building 4.

Network segment name	Cabinet number	Number of PCs	Network IP address / IP address mask	Range of IP address nodes		Default IP address of the gateway	Belonging to a VLAN	
				First IP address	Last IP address		VLAN number	VLAN name
SW 401	**4-01**	6	10.14.64.0/28	10.14.64.1	1014.64.13	10.14.64.14	401	KafC401
SW 403	4-03	8	10.14.64.32/27	10.14.64.33	10.14.64.61	10.14.64.62	403	Lab403
SW 405	4-05	9	10.14.64.64/27	10.14.64.65	10.14.64.93	10.14.64.94	405	Class405
PC 409	4-09	3	10.14.64.96/29	10.14.64.97	10.14.64.101	10.14.64.102	409	TeachB409
SW 412	4-12	9	10.14.64.128/27	10.14.64.129	10.14.64.157	10.14.64.15S	412	Class412
SW 413	4-13	9	10.14.64.160/27	10.14.64.161	10.14.64.1S9	10.14.64.190	413	Office413
SW 414	4-14	9	10.14.64.192/27	10.14.64.193	10.14.64.221	10.14.64.222	414	Lab414

Table A6. Wireless IP network addressing scheme.

Network segment name	Access **Point**	Network IP address / IP address mask	Range of IP address nodes		Access Point IP	Default IP address of the gateway	Belonging to a VLAN	
			First IP address	Last IP address			VLAN number	VLAN name
SSID: Liberia WIFI	2-09	10.14.193.0/24	10.14.193.1	10.14.193.252	10.14.193.253	10.14.193.254	209	WLAN

Table A7. Scheme of IP addressing of server's network segments.

Server name	Network IP address / IP address mask	Server IP	Default IP address of the gateway	Belonging to a VLAN	
				VLAN number	VLAN name
Shared servers					
DNS-SRV	201.100.11.0/29	201.100.11.1	201.100.11.6	807	SRV-PUE
HTTPS-SRV	201.100.11.0/29	201.100.11.2	201.100.11.6	807	SRV-PUE
Restricted servers					
DHCP-SRV	10.14.209.16/28	10.14.209.17	10.14.209.30	806	SRV-PRV
FTP-SRV	10.14.209.16/28	10.14.209.18	10.14.209.30	806	SRV-PRV

Table A8. Scheme of IP addressing of server's network segments.

Network segment name	Network IP address / IP address mask	IP addresses of network device interfaces		Interface type and number	
		Connection A	Connection B	Connection A	Connection B
GW-ISP1	194.44.136.0/30	194.44.136.1	194.44.136.2	FE0/0	FE0/0
GW-ISP2	205.7.5.128/30	205.7.5.129	205.7.5.130	FE0/1	FE0/1
FW-GW	201.100.11.0/29	201.100.11.5	201.100.11.6	FE1/0	FE1/0
PTMV 1-FV	10.14.224.8/29	10.14.224.9	10.14.224.10	FE0/24	FE0/24
PTMV 1-VTMV 1	10.14.224.16/29	10.14.224.17	10.14.224.1S	G0/1	G0/1
VTMV 1-VTMV 2	10.14.224.24/29	10.14.224.25	10.14.224.26	G0/2	G0/2
VTMV 2-VTMV 3	10.14.224.32/29	10.14.224.33	10.14.224.34	G0/2	G0/2
PTMV 1-VTMV 3	10.14.224.40/29	10.14.224.41	10.14.224.42	G0/2	G0/2

APPENDIX B

LISTING THE PTMV_1 CONFIGURATION FILE

```
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname PTMV_1
!
!
enable secret 5 $1$mERr$lzcRN5XvcTQ4nMIgxvLCe0
!
!
ip routing
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 description Lab101
 switchport trunk allowed vlan 101
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 description Lab102
 switchport trunk allowed vlan 102
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 description Class103
 switchport trunk allowed vlan 103
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 description KafA105_PC_1
 switchport access vlan 105
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/5
 description Readroom107
 switchport trunk allowed vlan 107
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 description Library108
 switchport trunk allowed vlan 108
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 description Lab109
 switchport trunk allowed vlan 109
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 description TeachA111
 switchport trunk allowed vlan 111
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 description Class113
 switchport trunk allowed vlan 113
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
```

```
!
interface FastEthernet0/20
 description FTP-SRV-PRV
 switchport access vlan 806
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet0/21
 description DHCP-SRV-PRV
 switchport access vlan 806
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 description PTMV_1-FW
 no switchport
 ip address 10.14.224.10 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description PTMV_1-VTMV_1
 no switchport
 ip address 10.14.224.17 255.255.255.248
 duplex auto
 speed auto
!
 interface GigabitEthernet0/2
  description VTMV_3-PTMV_1
  no switchport
  ip address 10.14.224.41 255.255.255.248
  duplex auto
  speed auto
 !
 interface Vlan1
  no ip address
  shutdown
 !
 interface Vlan101
  description Lab101
  mac-address 000b.beb7.1e01
  ip address 10.14.16.30 255.255.255.224
 !
 interface Vlan102
  description Lab102
  mac-address 000b.beb7.1e02
  ip address 10.14.16.62 255.255.255.224
 !
 interface Vlan103
  description Class103
  mac-address 000b.beb7.1e03
  ip address 10.14.16.94 255.255.255.224
!
interface Vlan105
 description KafA105
 mac-address 000b.beb7.1e04
 ip address 10.14.16.102 255.255.255.248
!
interface Vlan107
 description Readroom107
 mac-address 000b.beb7.1e05
 ip address 10.14.17.30 255.255.255.224
!
interface Vlan108
 description Library108
 mac-address 000b.beb7.1e06
 ip address 10.14.17.62 255.255.255.224
!
interface Vlan109
 description Lab109
 mac-address 000b.beb7.1e07
 ip address 10.14.17.94 255.255.255.224
!
interface Vlan111
 description TeachA111
 mac-address 000b.beb7.1e08
 ip address 10.14.17.110 255.255.255.240
!
interface Vlan113
 description Class113
 mac-address 000b.beb7.1e09
 ip address 10.14.17.158 255.255.255.224
!
interface Vlan806
 description SRV-PRV
 mac-address 000b.beb7.1e0b
 ip address 10.14.209.30 255.255.255.240
!
router eigrp 10
 redistribute static metric 100000 1000 255 1 1500
 network 10.0.0.0
 network 10.14.0.0 0.0.255.255
 no auto-summary
!
router eigrp 20
 auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.224.9
!
ip flow-export version 9
!
banner motd  Unathorized Access Phohibited! 
!
line con 0
 password 7 08311D
 login
!
line aux 0
!
line vty 0 4
 login
 transport input telnet
!
end
```

LISTING THE VTMV_1 CONFIGURATION FILE

```
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname VTMV_1
!
!
enable secret 5 $1$mERr$CIWHPGXc0UgeedU/DMThr.
!
!
ip routing
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 description ZavKafC201_PC_1
 switchport access vlan 201
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 description Decan205
 switchport access vlan 205
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3
 description Decanat206
 switchport trunk allowed vlan 206
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 description TeachC208
 switchport trunk allowed vlan 208
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 description WIFI-LAN
 switchport access vlan 209
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 description VTMV_1-VTMV_2
 no switchport
 ip address 10.14.224.25 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description PTMV_1-VTMV_1
 no switchport
 ip address 10.14.224.18 255.255.255.248
 duplex auto
 speed auto
```

```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan201
 description ZavKafC201
 mac-address 0001.4249.0201
 ip address 10.14.32.6 255.255.255.248
!
interface Vlan205
 description Decan205
 mac-address 0001.4249.0202
 ip address 10.14.32.14 255.255.255.248
!
interface Vlan206
 description Decanat206
 mac-address 0001.4249.0203
 ip address 10.14.32.30 255.255.255.240
!
interface Vlan208
 description TeachC208
 mac-address 0001.4249.0204
 ip address 10.14.32.46 255.255.255.240
!
interface Vlan209
 description WIFI-LAN
 mac-address 0001.4249.0205
 ip address 10.14.193.254 255.255.255.0
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
ip classless
!
ip flow-export version 9
!
banner motd Unathorized Access Prohibited!
!
!
line con 0
 password 7 08371D
 login
!
line aux 0
!
line vty 0 4
 login
 transport input telnet
!
!
end
```

LISTING THE VTMV_2 CONFIGURATION FILE

```
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname VTMV_2
!
enable secret 5 $1$mERr$48UrLx6VsZn.u0HP2vkj71
!
!
ip routing
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 description Lab301
 switchport trunk allowed vlan 301
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 description Lab303
 switchport trunk allowed vlan 303
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 description KafC305_PC_1
 switchport access vlan 305
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/4
 description ZavKafB309_PC_1
 switchport access vlan 309
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/5
 description Class311
 switchport trunk allowed vlan 311
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 description Class312
 switchport trunk allowed vlan 312
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 description Lab313
 switchport trunk allowed vlan 313
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 description KafB317_PC_1
 switchport access vlan 317
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
```

```
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 description VTMV_2-VTMV_3
 no switchport
 ip address 10.14.224.33 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description VTMV_2-VTMV_1
 no switchport
 ip address 10.14.224.26 255.255.255.248
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan301
 description Lab301
 mac-address 0090.21e6.cc01
 ip address 10.14.48.30 255.255.255.224
!
interface Vlan303
 description Lab303
 mac-address 0090.21e6.cc02
 ip address 10.14.48.62 255.255.255.224
!
interface Vlan305
 description KafC305
 mac-address 0090.21e6.cc03
 ip address 10.14.48.70 255.255.255.248
!
interface Vlan309
 description ZavKafB309
 mac-address 0090.21e6.cc04
 ip address 10.14.48.78 255.255.255.248
!
interface Vlan311
 description Class311
 mac-address 0090.21e6.cc05
 ip address 10.14.48.126 255.255.255.224
!
interface Vlan312
 description Class312
 mac-address 0090.21e6.cc06
 ip address 10.14.48.158 255.255.255.224
!
interface Vlan313
 description Lab313
 mac-address 0090.21e6.cc07
 ip address 10.14.48.190 255.255.255.224
!
interface Vlan317
 description KafB317
 mac-address 0090.21e6.cc08
 ip address 10.14.48.198 255.255.255.248
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
ip classless
!
ip flow-export version 9
!
banner motd Unathorized Access Prohibited!
!
line con 0
 password 7 08371E
 login
!
line aux 0
!
line vty 0 4
 login
 transport input telnet
!
end
```

LISTING THE VTMV_3 CONFIGURATION FILE

```
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname VTMV_3
!
!
enable secret 5 $1$mERr$GbpW8PdcyK7WPXe2vlun./
!
!
ip routing
!
!
spanning-tree mode pvst
!
!
interface FastEthernet0/1
 description KafC401
 switchport trunk allowed vlan 401
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 description Lab403
 switchport trunk allowed vlan 403
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 description Class405
 switchport trunk allowed vlan 405
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 description TeachB409_PC_1
 switchport access vlan 409
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/5
 description Class412
 switchport trunk allowed vlan 412
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 description Office413
 switchport trunk allowed vlan 413
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 description Lab414
 switchport trunk allowed vlan 414
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 description VTMV_3-PTMV_1
 no switchport
 ip address 10.14.224.42 255.255.255.248
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/2
 description VTMV_3-VTMV_2
 no switchport
 ip address 10.14.224.34 255.255.255.248
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan401
 description KafC401
 mac-address 00e0.8f70.5c01
 ip address 10.14.64.14 255.255.255.240
!
interface Vlan403
 description Lab403
 mac-address 00e0.8f70.5c02
 ip address 10.14.64.62 255.255.255.224
!
interface Vlan405
 description Class405
 mac-address 00e0.8f70.5c03
 ip address 10.14.64.94 255.255.255.224
!
interface Vlan409
 description TeachB409
 mac-address 00e0.8f70.5c04
 ip address 10.14.64.102 255.255.255.248
!
interface Vlan412
 description Class412
 mac-address 00e0.8f70.5c05
 ip address 10.14.64.158 255.255.255.224
!
interface Vlan413
 description Office413
 mac-address 00e0.8f70.5c06
 ip address 10.14.64.190 255.255.255.224
!
interface Vlan414
 description Lab414
 mac-address 00e0.8f70.5c07
 ip address 10.14.64.222 255.255.255.224
!
router eigrp 10
 network 10.0.0.0
 no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd Unathorized Access Prohibited
!
line con 0
 password 7 08371F
 login
!
line aux 0
!
line vty 0 4
 login
 transport input telnet
!
!
end
```

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
Ternopil Ivan Puluj National Technical University
Faculty of Computer Information Systems and Software Engineering

Computer Systems And Networks Department

“Approved”
Head of department
_____ Osukhivska H.M.

DEVELOPMENT OF COMPUTER NETWORK FOR THE UNIVERSITY OF LIBERIA

Degree Bachelor

“AGREED”
Supervisor
_____ Phd.,Assoc. Prof. O.S. Holotenko

“PERFOMER”
Student of group ICI-42
_____ Thomas Stephen sk.

Ternopil 2021

1. Terms

This document describes process of development of computer network for the University of Liberia. Main objective of the diploma project is to design a computer network for the College of Social Sciences and Humanities for the University of Liberia.

1.1. Full name of system and its identification

Full name of the diploma project: «Development of computer network for the University of Liberia».

Identification: CSDP 123.041.00.00

1.2. Order for system development

Order (№ 4/7-56, 01.02.2021).

1.3. Performer

Performer - student of ICI-42 group, department of computer systems and networks, Ternopil Ivan Puluj National Technical University, Thomas Stephen s k.

1.4. Input documents for system development

- specification of the object;
- computer network requirements;
- specification of sharing services;
- specification of restricted services;
- specification of network equipment;

- documentation of hardware means of Internet access.

1.5. The sequence of results presentation

Project consists the lists of documentation which response to the approved requirements of computer systems and networks department. Requirements response to the standards in the field of computer engineering development (ISO Standards).

Presentation of intermediate results of the diploma project is carried out according to the schedule approved by the supervisor.

1.6. Standards and regulatory documents

- Standard ANSI/EIA/TIA 568 - “Commercial Building Telecommunications Wiring Standard” and ANSI/EIA/TIA 569 - “CommercialBuilding Standard for Telecommunications Path wais and Spaces”.

2. Appliance and purpose of system design

2.1. Appliance of system

In accordance with the tasks set before us, the computer network must provide adequate operation in three main modes:

- full-time;
- maintenance mode;
- emergency.

The normal mode of operation should be the main mode of operation of all components of the computer network and ensure the use of backup facilities to ensure load balancing between the main and backup software and hardware of the information and communication system of the organization.

The emergency mode of operation must guarantee full or partial availability of public access services at the expense of the provided means of reservation. The reason for the use of means of redundancy may be a one-time failure of the main set of telecommunications.

Developed technical solutions for creating a computer network should ensure its operation 24/7/365. Temporary restriction of full-featured availability of certain information resources is allowed:

- as a result of abnormal situations caused by one-time failures in the operation of hardware and / or software of the computer network; ·
- during the periods of routine maintenance of software and hardware and software of the computer network, provided by the operating documentation.

To organize interconnection, the TCP / IP v4 / v6 protocol stack should be used as the main one for all modern information and telecommunication systems.

2.2. Objective of system design

The main purpose of this work is to design a computer network for the College of Social Sciences and Humanities for the University of Liberia.

To achieve this goal, it is necessary to solve the following tasks:

- to analyze the current network architecture of the College of Social Sciences and Humanities of the University of Liberia, to identify places that need further improvement;

- justify the choice of network architecture for a computer network, access methods, topology, type of cable system, operating system, applications, protocols;

- justify the choice of network management method;

- justify the choice of network equipment;

- prepare basic documentation: network diagrams at the physical, channel and network levels, IP addressing plan, list of devices;

- simulate the network in the Cisco Packet Tracer emulator.

2.3. Characteristic of design object

Developed network must provide uninterrupted communication between workstations in the network. Increase productivity by simplifying data exchange between employees of different departments.

Also, the developed network must ensure high reliability and security of information.

3. Systems requirements

3.1. Requirements in general

3.1.1. Characteristics of the object

The College of Social Sciences and Humanities, for which a computer network is being developed, consists of 4 buildings. In the building there are classrooms, laboratories, administrative premises (dean's office, departments, teachers), library, reading room and other additional office space.

3.1.2. Computer network requirements

The computer network must provide adequate operation in three main modes:

- full-time;
- maintenance mode;
- emergency.

The normal mode of operation should be the main mode of operation of all components of the computer network and ensure the use of backup facilities to ensure load balancing between the main and backup software and hardware of the information and communication system of the organization.

The emergency mode of operation must guarantee full or partial availability of public access services at the expense of the provided means of reservation. The reason for the use of means of redundancy may be a one-time failure of the main set of telecommunications.

3.1.3. Resources and services

In order to diagnose the system, it must be monitored using the appropriate tools included in the relevant system software. The tools should provide an easy interface for viewing diagnostic events and monitoring the program execution process.

3.1.4. Perspective of modernization

The system software and hardware can be modified to newer versions. Existing the hardware component of the computerized system should not be affected significant changes, and the system software should provide flexibility and scalability.

3.1.5. Requirements to the end users and their qualification

System administrators maintain the system in automatic or manual mode through management and monitoring. The minimum number of service personnel is one person.

3.1.6. Criteria of appliance

The system must be able to scale:

- by productivity;
- bycapcity of information process;

- Scaling capabilities must be provided by the basic software and hardware used.

3.1.7. Reliability requirements

The system must be operational and restored in the following situations:

- if the power system of the hardware operating system fails, causing a reboot;
- if a hardware operation error occurs (except for data carriers and programs), entrust the restoration of system functions to the OS;
- for errors related to software (operating system and device drivers). In order to protect the equipment against overvoltage and switching disturbances, use network filters and uninterruptible power supplies.

3.1.8. Safety requirements

The external elements of the technical measures of the system, which are under voltage, must have protection against accidental contact, and the technical measures themselves must have a zeroing or protective grounding GOST 12.1.030-81 and PUE. The power supply system must provide a protective switch during overloads and short circuits in the load circuits, as well as manual emergency shutdown. General fire safety requirements must comply with the standards for household electrical equipment. In the event of fire, no poisonous gases or vapors should be produced. After disconnecting the power supply, ensure that all fire extinguishers can be used. Harmful factors should not exceed the standards of SanPiN 2.2.2./2.4.1340-03 of 06/03/2003.

3.1.9. Requirements for operation, maintenance, repair and storage of system components

The microclimate in rooms with the corresponding hardware has to correspond to norms of an industrial microclimate on (GOST 12.1.005-88).

For normal operation of the network it is necessary to support (according to GOST 23.865-85):

- air temperature in the range from + 15C to + 20C;
- relative humidity at 20C in the range from 30% to 70%;
- atmospheric pressure 760mm Hg.

The technical means used must be regularly maintained according to the requirements of the technical documents, but not less than once a year. Regular

maintenance and testing of technical means should include maintenance and testing of all used means, including workstations, servers, cable systems and network equipment, and uninterrupted power supplies. According to the test results of technical means, the reasons for the defects should be analyzed and eliminated. The location of the premises and its equipment must prevent uncontrolled entry by outsiders and ensure the security of confidential documents located in these premises and technical means.

3.1.10. Requirements to standardization and unification

Compatible with common computer interfaces.

3.2. Requirements for types of collateral

3.2.1. Requirements to the system's hardware (technical characteristics of each devices in the system)

The designed computer network must be provided the following network equipment.

Building 1:

• 1 router to connect to Internet service providers;

• 1 firewall;

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 3 switches of 2 levels of the OSI model (unmanaged), 8 x 100 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

Building 2:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 2 level 2 switches of the OSI model (unmanaged), 8 x 100 Mbps;

• 1 wireless access point.

Building 3:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

Building 4:

• 1 switch of 3 levels of the OSI model, 24 x 100 Mbps, 2 x 1000 Mbps;

• 1 switch of the 2nd level of the OSI model (unmanaged), 8 x 100 Mbps;

• 5 switches of 2 levels of the OSI model (unmanaged), 16 x 100 Mbps;

3.2.2. Structure and contest of design system

The composition and content of system design work includes: (translate)

- design and coordination of the technical task for the system;

- system design;
- writing an explanatory note;
- design of graphic material;
- defense of the qualifyingpaper.

4. Technical and economic indicators

The cost of development should not exceed 3000 USD.

The service life of the device must be at least 18,000 thousand hours. (2 years)

* Note: the cost of development may change during the calculation during development.

5. Stages of system design

Table 1 - Stages of system design

Numbero f stage	Paper stages	Paper stages deadlines Notes
1	*Development and approval of the technical task*	01.02-15.02.2021
2	*Analysis of the technical task*	16.02-28.02.2021
3	*Substantiation of possible technical solutions*	01.03-15.03.2021
4	*System design and implementation*	16.03-04.05.2021
5	*Testing of the designed system*	04.05-22.05.2021
6	*Section of labor protection and safety in emergency*	23.05-31.05.2021
7	*Registration of the qualifiying paper*	01.06-10.06.2021
8	*Preliminary defense of the qualifiying paper*	09.06-12.06.2021
9	*Defense of the qualifiying paper*	27.06.2021

6. The order of control and acceptance

The control of the process of execution of the diploma project is carried out by the head of the diploma project.

Normocontrol of the diploma project for compliance with the requirements of the standards is carried out at the Department of Computer Systems and Networks.

The presentation of the results of the diploma project is done by defending the diploma project at the relevant meeting of the SEC, illustrating the main achievements through the graphic material.

7. Requirements for documentation

The documentation must meet the requirements of ESKD and DSTU

Set of design documentation:

- explanatory note;
- applications;
- graphic material:

1. Block diagram of the computer network of the College of Social Sciences and Humanities of the University of Liberia.

2. Physical topology of a computer network.

3. Scheme of computer network connections.

4. Logical topology of a computer network.

5. Simulated computer network in the Cisco Packet Tracer environment.

* Note: The design documentation may be subject to change and addition during development.

8. Additional conditions

During the implementation of the thesis project, changes and additions may be made to this technical task.