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

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

Department of Computer Science
(full name of department)

QUALIFYING PAPER

For the degree of

Bachelor
(degree name)

topic: Development of computer network project for companies office

Submitted by: fourth year student _____ , group ICH-43

specialty 122 Computer science

(code and name of specialty)

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

Ternopil
2022

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

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

Department Department of Computer Science
(full name of department)

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

ASSIGNMENT
for QUALIFYING PAPER

for the degree of Bachelor
(degree name)

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

student Owoo Larius
(surname, name, patronymic)

1. Paper topic Development of computer network project for companies office

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

Approved by university order as of « 19 » November 20 21 № 4/7-979
2. Student's paper submission deadline 27.01.2022
3. Initial data for the paper Literature sources about architecture, principles of operation and development of computer networks.

4. Paper contents (list of issues to be developed)
The OSI reference network model in overview. The OSI model. Stages of OSI model. Fast «Ethernet» network calculation. «Ethernet» technology. Fast «Ethernet» technology. Rules for building
a Fast «Ethernet» network. Stages of structured cabling design. Terms of reference of the customer. Construction of a technical model. Network documentation preparation. Plan for connecting equipment; Calculation of network bandwidth that is useful. Modeling of networks; Estimated cost of the project. Occupational health and emergency safety. Conclusion. References. Appendixes. The Building Plan. Block diagram of the current network. Structural diagram of the developed network
5. List of graphic material (with exact number of required drawings, slides)

6. Advisors of paper chapters

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

7. Date of receiving the assignment 06.09.2021

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	Analysis of the task for qualifying work. Selection	06.09.2021	*Completed*
	and work with literary sources.		
2	Writing chapter 1	13.09.21 - 04.10.21	*Completed*
3	Writing chapter 2	05.10.21 – 21.10.21	*Completed*
4	Writing chapter 3	25.10.21 – 11.11.21	*Completed*
5	Writing chapter 4	15.11.21 – 16.12.21	*Completed*
6	Standartization control	20.12.21 – 31.12.21	*Completed*
7	Plagiarism check	03.01.22 – 13.01.22	*Completed*
8	Preliminary defense of qualifying paper	17.01.2022	*Completed*
9	Defense of qualifying paper	27.01.2022	

Student ____________ Owoo Larius
(signature) (surname and initials)

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

ANNOTATION

Development of computer network project for companies office // Diploma thesis Bachelor degree // Owoo Larius // Ternopil’ Ivan Puluj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2022 // P. _67_, Fig. – _14_, Tables – _15_, Annexes – _3_, References – _30_.

Keywords: computer network, building the fast «Ethernet» network, network configuration, calculation of network bandwidth, modeling of networks.

Qualification work is devoted to the development of a computer network project for companies office.

The purpose of the work is to develop a computer network project taking into account the architectural features of the company's office building as well as the peculiarities of the company's operation.

In the first section of the qualification work the features of the OSI model are considered, according to which modern computer networks are designed.

The second section of the qualification work provides a rationale for the choice and calculation of Fast «Ethernet» technology as a basis for the designed computer network.

The third section of the qualification work presents the process of network design and the results obtained, in particular: construction of a technical model, network documentation preparation, plan for connecting equipment, calculation of network bandwidth, estimated cost of the project.

LIST OF SYMBOLS, UNITS, ABBREVIATIONS AND TERMS

ARP – Address Resolution Protocol.

BGP – Border Gateway Protocol.

DHCP – Dynamic Host Configuration Protocol.

DNS – Domain Name.

FDDI – Fiber Distributed Data Interface.

FTP – File Transfer Protocol.

GB – gigabit.

GRE – Generic Routing Encapsulation routes.

HTTP – Hypertext Transfer Protocol hypertext.

ICMP – Internet Control Message Protocol.

IEEE – Institute of Electrical and Electronic Engines.

IP – Internet Protocol.

KB – Kilobyte.

LAN – Local Area Network.

MAC – Media Access Control.

NTP – Network Time Protocol.

OSI – Open System Interconnection.

POP3 – Post Office Protocol Version 3 branch, version 3).

QoS – Quality of Service.

RADIUS – Remote Authentication in Dial-In User Service.

SCS – Structured Cable System.

SMTP – Simple Mail Transfer Protocol.

TCP – Transmission Control Protocol.

TELNET – Terminal Network.

TFTP – Trivial File Transfer Protocol.

TK – Terms of Reference.

UDP – User Datagram Protocol.

VLAN – Virtual Local Area Network.

CONTENTS

INTRODUCTION

Currently, there are several methods for connecting individual computers to a network. A wide range of hardware and software is available to manage them. This can make deciding on the type of network and software difficult through long period. As we know, in the event of an increase in the number of computers on the network or growing demands on speed and, as rule, volume of information transmitted, the wrong choice may result in the inability of programs to function. It is critical to understand enough principles of local area network construction (LAN Protocol) to competently choose hardware and software for network management. **The thesis's goal** is to design a local computer trading company network.

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

- an examination of the company's current network architecture in order to identify problem areas that require further attention;
- justification for computer network architecture, access method, topology, cable system type, systems for operating environment, protocols and applications;
- the kind of methods for network management that is chosen;
- justification of intermediate network equipment that selected;
- creation of basic documentation, including physical, channel, and network diagrams, an IP addressing plan, and a list of devices.

The object of research is the process of development of a computer network project for the companies office.

The subject of research is the design of a computer network for the companies office based on the use of principles and modern technical means to ensure the functioning of computer networks.

The Cisco Packet Tracer emulator is used to model networks. The proposed project's implementation will increase productivity, reduce the time it takes to receive and process information, perform accurate and complete data analysis, and ensure the receipt of all types of work-related reports. As a result, new temporary resources for the development and implementation of new projects are formed.

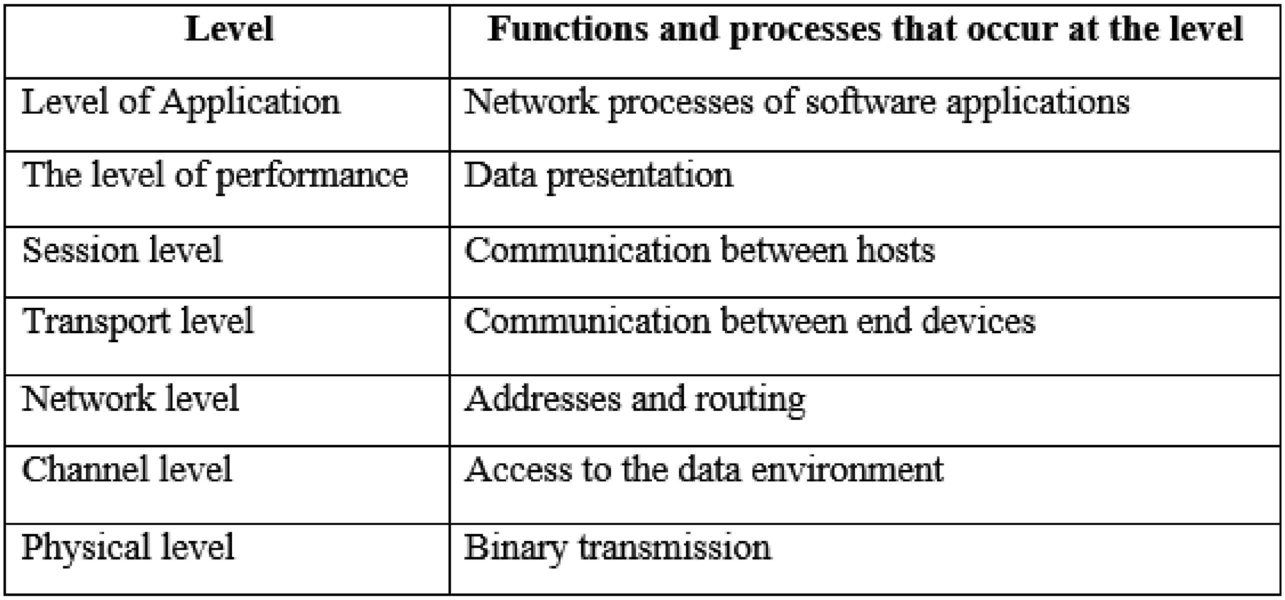
With the introduction of new technical and financial capabilities, the LAN must be designed to meet modern requirements for further development and expansion, provide connectivity to the "outside world" via the “Internet”. As rule, setting up a VLAN in an enterprise network is thought to allow for the organization of the network's logical structure on the basis of software, preventing physical device movement and resulting in cost savings.

1 THE OSI REFERENCE NETWORK MODEL IN OVERVIEW

1.1 The "OSI" model

Table 1.1 depicts the OSI Reference Model (Determination Protocol apart from the physical environment).

Table 1.1 – Reference OSI model



Level	Functions and processes that occur at the level
Level of Application	Network processes of software applications
The level of performance	Data presentation
Session level	Communication between hosts
Transport level	Communication between end devices
Network level	Addresses and routing
Channel level	Access to the data environment
Physical level	Binary transmission

This model is predicated on the world organization for Standardization's (ISO) development (Protocol on the Definition of the world organization for Standardization, ISO) and is that the initiative toward international standardization of protocols used at various levels. Because it connects open systems, i.e., systems which will communicate with other systems, this structure is understood because the reference model of interaction open systems.

1.2 Stages of OSI model

The “OSI” version is cut up into seven stages. The emergence of this sort of shape became resulting from the following factors:

1) A stage ought to be created each time a separate stage abstraction is required;

2) Each stage should carry out a particular function;

3) The features for each stage ought to be selected with the advent of standardized global protocols in mind;

4) The limitations among stages ought to be selected simply so statistics flows among interfaces are as minimum as possible;

5) the quantity of stages ought to be massive sufficient simply so exclusive features are not redundantly blended in a single stage, however now no longer so massive that the structure turns into cumbersome.

The “OSI” model is not a network architecture because it does not describe it services and protocols used at each level. These simple 10 determines what each level should do. Below we consider each level models starting from the bottom.

The physical layer, as we know, is liable for the particular transmission of raw bits over a channel. When designing a network, when one party transmits the unit, the receiving party receives the unit also, and not zero. the elemental questions here are:

1) What voltage is employed to display one and which to display zero;

2) What percentage microseconds a touch last;

3) Whether the transfer is often made simultaneously in two directions;

4) How the initial connection is established and the way it ends when each side have completed their tasks;

5) What percentage wires should a cable contains and what the function of every wire is. Mechanical, electrical, and procedural interfaces, also as physical media below the physical level, are the first development issues.

The channel level's main task is to be able to give transmit "raw" physical layer data, as rule, on a reliable line of communication. This task is accomplished, as rule, by dividing the input data, as we known, into frames of varying sizes ranging from a few hundred to several thousand bytes. Data frames is sent in a sequential order, with frame processing confirmations returned by the recipient.

Another issue, as rule, that arises at the channel level (and also at most, as rule, of the higher levels) is how to avoid situations in which, as rule, the fast transmitter overwhelms the receiver with data. Some regulatory mechanism that informs the transmitter of the presence of free space in the receiver buffer at the moment can be predicted.

Another issue at the channel level in broadcast networks is how to control access to the shared channel. This issue is addressed by the addition of a special additional sublevel of channel level - the sublevel of carrier access

Subnet operations are managed by the network layer. Important aspect here is determining the routes, as rule, for forwarding packets, as we known, from sources to destinations. They can be set rigidly in the type of tables and often change or, more times, change in automatic mode to avoid some components that have failed. Furthermore, they can be set, as rule, at the start of each connection, such as a terminal session, as rule, or connecting to a remote, as rule, machine. They can at end highly dynamic, meaning they are recalculated, as rule, for each, as rule, packet based, as rule, on the current, as rule, network load.

If there are in the subnet too many packets at the same time, then they can close the road to each other, creating traffic jams in the narrow places. Preventing such blockages is also, as rule, a network task level in conjunction, as rule, with higher levels that adapt downloads. In more general, the network layer, as rule, is concerned with providing a certain service, as rule, level (Protocol for delays, transmission time, synchronization issues).

When a packet, as rule, travels to another network from one, a number of issues may arise. Yes, the addressing method employed in one network may differ from that employed in another, as rule. Because the packages are too large, as rule, the network may refuse to accept them entirely. They may also have different protocols, etc. The network layer should resolve all of these issues, allowing you to combine disparate networks.

The “transport” layer's main function is to receive data, as rule, from the session level, break it up, if necessary, into small pieces, pass it, as rule, to the network level, and ensure, as rule, that these parts arrive in the correct shape. Furthermore, all of this must be, as rule, done efficiently and in such a way that higher levels are not affected by changes, as rule, in hardware technology over time.

Transport layer, as rule, also determines the type of service, as we know, provided to network users at the session level. The most common type of transport connection is an “error-free channel” between, as rule, two nodes that delivers messages or bytes, as rule, in the order they were sent. Transport level can provide other types of services, such as sending individual messages without guarantee of conformity with the order of their delivery or sending messages to multiple recipients at the same time using the broadcasting principle. When establishing a connection, the type of service is determined. Strictly speaking, it is absolutely impossible to create a channel due to errors when completely protected. They only discuss channels where the error rate, as rule, is low enough to be ignored, usually, in practice.

The transport level may be a true “end-to-end” level, delivering messages from the sender to the recipient. In other, as rule, words, a program on one machine communicates with a program, as rule, on another machine via message headers and control, usually messages. To care of connection at a lower level, as rule, connections are established between all neighboring machines through which messages pass.

The session level enables users from different computers to establish communication sessions with one another. Services of various types are provided, such as:

- dialog management (protocol definition of tracking the order of data transmission);
- marker management (protocol to determine the prevention of concurrent execution critical operation of multiple systems);
- synchronization (Protocol definition installation service tags inside long messages that allow you to continue transmission from the place where it broke, even after a failure and restoration).

In contrast to the lower levels, as rule, which are primarily concerned usually with the reliable transmission, as rule, of bits and bytes, the level of representation is primarily concerned, as rule, with the syntax and semantics usually of transmitted information. It is necessary to convert data formats to each other by transmitting them over a network, as rule, in some standardized form in order for computers, as rule, with different data representations for communicate with each other. The level of representation deals with these transformations, allowing for the definition and modification of higher-level data structures (Protocol definition, for example, database records).

The “application” layer includes a set of popular protocols that users must use. The hypertext, as rule, transfer protocol “HTTP”, which serves as the foundation for “World Wide Web” technology, is one of the most common. When a browser requests a web page, it sends its name (Addressing Protocol) and hopes that the server hosting the page uses “HTTP”. In response, the server sends a page. For file transfers, e-mail, and network mailings, other application protocols are used.

Because the lower levels (Protocol 1 to 3) OSI models control the physical delivery and communication over the network, they're often called levels data transmission medium (Protocol for determining media layers). Upper levels (Protocol 4 to 7) of the OSI model ensure accurate delivery of knowledge between computers on the network, in order that they often mentioned as host layer levels. In most networks devices implemented all seven levels. However, to hurry up execution operations in some networks, the network itself implements the functions of several levels.

1.3 Conclusion of the chapter 1

The OSI version is broken down into seven stages. Because it does not specify the services and usually protocols utilized at each level, the “OSI” model is not a network architecture. Physical layer, as rule, is responsible for the specific transmission of raw bits through a channel. What percentage of wires should a cable have, and what is each wire's role? First development difficulties include electrical, mechanical, and procedural interfaces, as physical media below the “physical” level. Major job of the channel level is to be able to send, as rule, "raw" physical layer data on a dependable line of communication that is free of undetected defects, as well as to disguise real errors, as rule, so that the network layer does not halt. Another issue that happens at the channel level (and at most more elevated levels) is the manner by which to keep away from conditions where the fast transmitter over-burdens the collector with information. One more test with, as rule, broadcast networks is the way usually to manage admittance to the common channel at the channel level. The organization layer is accountable for subnet tasks. Deciding the pathways for communicating parcels from sources to objections is the most basic part here. Forestalling such bottlenecks is an organization task that works pair with more elevated levels that change downloads. The organization layer, as a general rule, is worried about giving a given level of administration (Protocol for delays, transmission time, synchronization issues).

Moreover, addressing method, as rule, used in one network may, as rule, not be the same as that used in another. Network may, as rule, refuse to accept the packages fully because, as rule, they are too huge. The basic job of the “transport” layer is to take data from the session level, divide it up into small pieces, if necessary, pass it to the network level, and verify that these parts arrive in the correct shape. At the session level, the transport layer also determines the type of service supplied to network users. The type of service is determined upon establishing a connection. The “transport” level could be a genuine end-to-end level, conveying messages, as rule, from sender to recipient. Users from various computer usually can establish communication sessions with one another at the session level. In contrast to the lower levels, which are concerned, as rule, primarily with the reliable, as rule, transmission of bits and bytes, the level of representation is concerned primarily with the syntax and, as rule, semantics of sent information. Application layer includes a collection of well-known protocols that users must follow. The server responds by sending a page. Because the lowest levels of OSI models regulate physical distribution and communication through the network, they are frequently referred to as levels data transmission medium.

2 FAST «ETHERNET» NETWORK CALCULATION

2.1 «Ethernet» technology

In 1980, DEC, Intel, and Xerox (DIX Definition Protocol) proposed the «Ethernet» network specification, which later became, as we know, the “IEEE standard 802.3”.

As the transmission medium for the first versions of “«Ethernet»” Vice (Domain Name Service) 1.0 and 2.0, only coaxial, as we know, cable was used. “«IEEE 802.3»” standard allows for the use of twisted pair and fiber in the transmission medium's quality. The «IEEE 802.3»u (Fast «Ethernet» Definition Protocol) standard was adopted in 1995 at a rate of 100 Mbps, and the «IEEE 802.3»z standard was adopted in 1997. «IEEE 802.3»ab standard - Gigabit «Ethernet» on, as we know, twisted pair category 5 - was adopted in the fall of 1999.

In «Ethernet» notation (Protocol for determining 10BASE2, 100BASE-TX, etc.), the first BASE element indicates the data rate in Mbit / s; the second BASE element indicates that direct (Protocol unmodulated) transmission is used; and the third BASE element indicates the rounded value of the cable length in hundreds of meters (Protocol for determining 10BASE2 - 185 m, 10BASE5 - 500 m) or type of transmission

«Ethernet» is based on the method of multiple access to the environment carrier listening and collision detection - CSMA / CD (Carrier Sense with Multiple Access and Collision Detection), which is implemented on the hardware or firmware levels of each network node:

- all adapters include an environment access device (MAU detection protocol) - transceiver that is linked to a common (to be shared) environment data transmission protocol;
- before transmitting data, each node adapter listens for a line and waits for it to be absent (Protocol for determining the carrier);

- the adapter then generates a frame (Protocol definition frame), which starts with a synchronizing preamble and is followed by a binary data stream;
- other nodes receive the sent signal, synchronize on the preamble, and decode it into a bit sequence;
- the lack of carrier detected by the receiver determines the end of frame transmission;
- in the event of a collision (Protocol for collision of two signals from different nodes), the nodes stop transmitting the frame and then make a second attempt to transfer after line release at random intervals of time (Protocol for determining each through its own);
- in the event of another failure, the next attempt (Protocol determination and so on up to 16 times) is made, and the delay interval is increased;
- the collision, as we know, is the receiver for a non-standard, as rule, frame length that cannot, as you see, be less than 64 bytes (excluding the preamble).

Collision domain - a group of nodes, as rule, linked by a common environment, as we know, transmission (Protocol definition repeaters, cables). Length, as we know, of the collision domain is limited, usually, by the time it takes for signals to travel between, as rule, the nodes that are the most distant from each other.

The diameter, as rule, of the collision domain is the distance between the two end devices that are the furthest apart from each other.

Bit interval, as we know, is the amount of time it takes to transmit one bit. In «Ethernet» (Protocol for determination at a speed of 10 Mbps), the bitwise interval is 0.1 s. «Ethernet» technology's physical specifications include the following data transmission medium:

- 10 Base-5 - coaxial cable with a 0.5-inch diameter (protocol definition "thick" coaxial). The wave resistance is 50 ohms. The segment's, as we know, most period is 500m (Protocol for dedication without repeaters);

- 10 Base-2 - coaxial cable with a 0.25-inch diameter (Protocol definition skinny coaxial). The wave resistance is 50 ohms. The segment's most period is 185m (Protocol for dedication without repeaters). To growth the diameter, use repeaters. The rule "5-4-3" applies to coaxial network variants;
- 10 Base-T, usually, is a twisted pair, as we know, cable that is not shielded. It forms a star-shaped topology on the base hub. Between the hub, as we know, and the end node, the distance should not exceed 100 meters;
- Optical cable 10 Base-F. The topology is similar to that of the 10 Base-T standards. This specification comes in several flavors:
  - (Protocol for determining distances up to 1000 meters),
  - 10 Base-FL (Protocol for determining distances up to 2000 meters), and
  - 10 Base-FB (Protocol for determining distances up to 3000 meters) (Protocol for determining distances up to 2000 m). The rule "4 hubs" applies to using repeaters to increase the diameter of «Ethernet» networks built on twisted pair and optical cable.

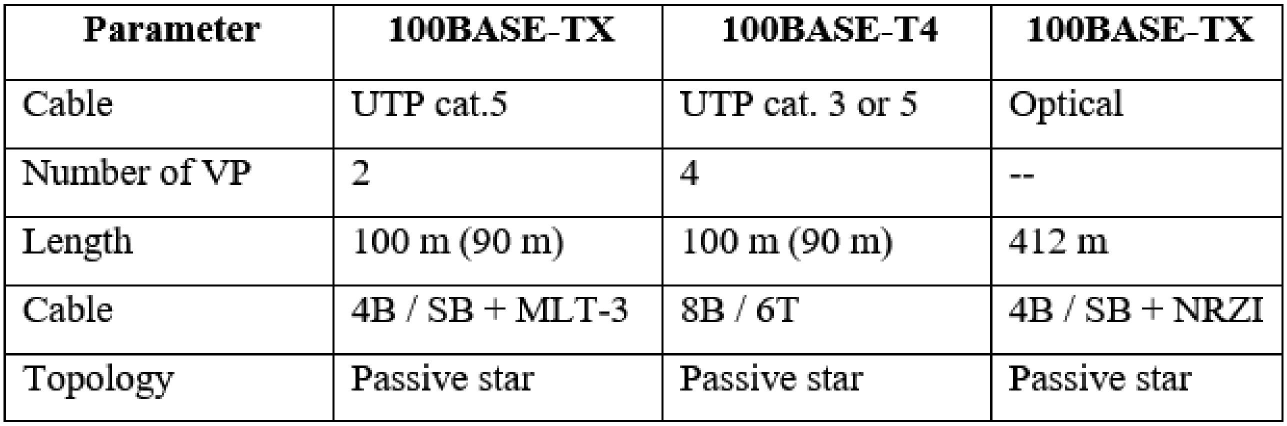
Now let us move to Fast «Ethernet» technology.

2.2 Fast «Ethernet» technology

The bit interval in Fast «Ethernet» technology is 0.01 s, resulting in a tenfold increase in data rate. In comparison to «Ethernet», the frame data amount and transmission channel access mechanism data remained unchanged with frame format.

Table 2.1 Shows the characteristics of the physical environment specifications for Fast «Ethernet».

Table 2.1 – The characteristics of the physical environment specifications for Fast «Ethernet»



Parameter	100BASE-TX	100BASE-T4	100BASE-TX
Cable	UTP cat.5	UTP cat. 3 or 5	Optical
Number of VP	2	4	--
Length	100 m (90 m)	100 m (90 m)	412 m
Cable	4B / SB + MLT-3	8B / 6T	4B / SB + NRZI
Topology	Passive star	Passive star	Passive star

The following data transmission, as rule, medium is included in the physical specifications, as rule, of Fast «Ethernet» technology:

- A network, as rule, with a hub center and a passive, usually, star topology is known as "100 Base-TX". Category 5 or higher, as rule, twisted pair (UTD) is used, which is related, as rule, to the required cable, as rule, bandwidth. 8-pin RJ-45 connectors use to connect, as rule, the cable. The length cable must be 100 meters. The standard also allows for shielded cable with two twisted pairs of wires to be used (Protocol for determining the impedance - 150 Ohm). A 9-pin shielded connector is used in this case. To date, the most common type of Fast network «Ethernet» is "100 Base-TX".
- The transfer is not two, but four unshielded twisted pairs in 100 Base-T4 (UTP detection protocol). The cable could be of lower quality (Protocol for determining category 3, 4 or 5). The 100BASE-T4 coding system was adopted. Although any of these cables will deliver the same 100 Mbps signal, the standard still recommends using a Category 5 cable. Data is exchanged using three-level differential signals on one transmitting twisted pair, one receiving twisted pair, and two bidirectional twisted pairs.

- Two multidirectional optical cables are used to connect computers to the hub using the 100 Base-FX passive star topology. The cables are connected to the adapter (Transceiver Identification Protocol) and the hub via SC, ST, or FDDI connectors. 412 meters is the maximum cable length between the computer and the hub (Protocol definition of this restriction is determined not by the quality of the cable, and installed temporal ratios). It is applied multimode or single-mode cable with a wavelength of 1.35 microns, according to the standard. The signal power loss in the segment (protocol definition of cables and sockets) should not exceed 11 dB in this case.

2.3 Rules for building a Fast «Ethernet» network

2.3.1 Calculation of the first model

The "IEEE standard 802.3" provides two models for determining, as rule, the performance of a Fast «Ethernet» network:

Transmission System **Model 2** and Transmission System **Model 1**. The first is based, as rule, on just a few basic rules. Based on the fact that all network, as rule, components (in particular, cables) have the worst possible temporal characteristics and thus always give a significant margin of error.

The second employs an accurate calculation system with real-time cable characteristics. In this regard, its application allows it to occasionally overcome the rigid limitations of model 1.

The first model of Fast «Ethernet». The model is actually a group network construction rule:

- electrical cable segments must not be longer, as rule, than 100 meters. This applies to all cable usually categories - 3, 4, and 5, as well as the segments "100BASE-T4" and "100BASE-TX";

- the length, as rule, of optical cable segments usually should not exceed approx 412 meters;
- if external adapters are used (Remote Sensing Protocol) transceivers, the transceiver cables (Protocol MII definition) shouldn't be longer than 50 centimeters.

There are, as rule, two types of repeaters defined by these standards:

1) Class I, as rule, repeaters convert input signals to digital view and then recode digital data into physical signals when they are transmitted again. Because it takes, as rule, time to convert signals to repeaters, only one Class I repeater is allowed in the collision domain.

2) Class II, as rule, repeaters transmit received signals without transformation, allowing, as rule, you to connect only segments, as rule, that use the same data encoding methods; no more than two Class II repeaters can be used in a single collision domain.

Model one identifies three Fast «Ethernet» configuration options:

1. Direct network connection of two subscribers (Protocol node definition), without the use of a repeater or hub (Protocol definition Fig. 2.1).

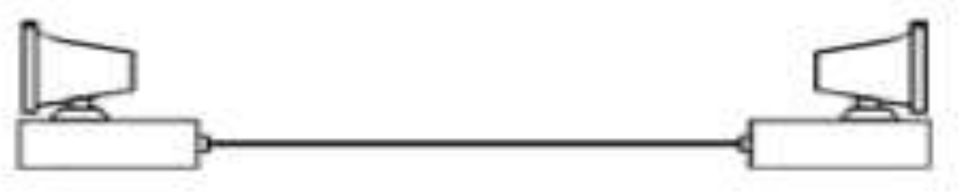


Figure 2.1 – Diagram of a direct connection of two network nodes

Subscribers are often not only computers but also network printer, switch, bridge, or router port. Yes, the mixture is named a “DTE-DTE” or two-point connection.

For this case, as rule, model one are simple: no electric cable should, as rule, be longer than one hundred meters, half-duplex fiber-optic no more than approx 412 meters, as rule, full-duplex fiber-optic no more than 2000 meters (the protocol for determining this does not take into account the signal delay in the cable, as the CSMA / CD method does not work).

2. Connecting two network subscribers with one Class one or Class two repeater hub (Protocol of definition.2.2)

Length of network cables, as rule, A and B must be limited according to table 2.2. Figure 2.2 shows how two network subscribers can be, as rule, connected by a single usually repeater hub.

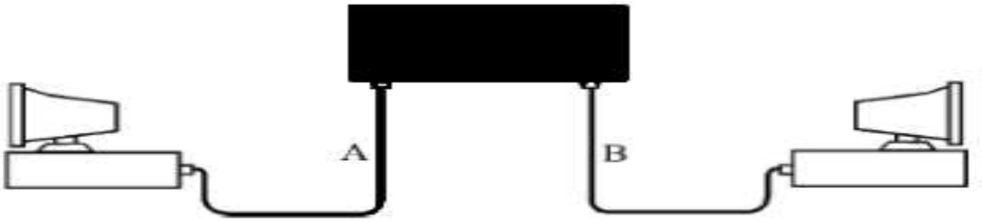
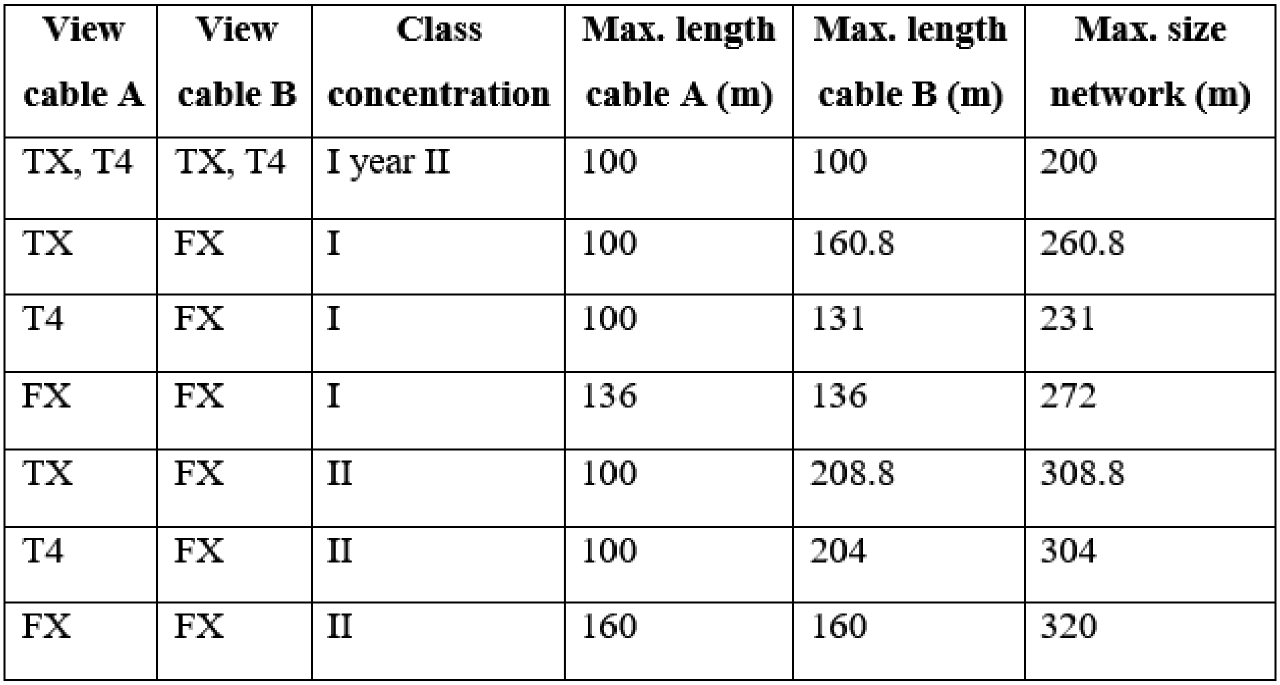


Figure 2.2 – The diagram showing how two network subscribers can be connected used a single repeater hub

Table 2.2 – The maximum cable length that can be used in a single hub configuration



View cable A	View cable B	Class concentration	Max. length cable A (m)	Max. length cable B (m)	Max. size network (m)
TX, T4	TX, T4	I year II	100	100	200
TX	FX	I	100	160.8	260.8
T4	FX	I	100	131	231
FX	FX	I	136	136	272
TX	FX	II	100	208.8	308.8
T4	FX	II	100	204	304
FX	FX	II	160	160	320

Two repeaters class two concentrators are used to connect two network subscribers. It is assumed that for communication hubs, an electric cable no longer than 5 meters in length should be used.

Because Class II hubs have less latency, there may, as rule, be two. Use of three hubs, as rule, in accordance with model one is not permitted. In this case, as rule, the lengths of two cables B and A must be limited, as rule, to table 2.2, respectively. By default, cable C is assumed to be five meters long. Table 2.3 shows maximum cable length in a two-hub configuration

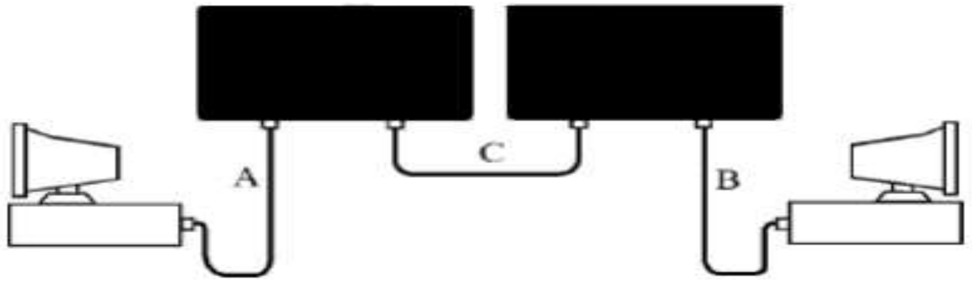
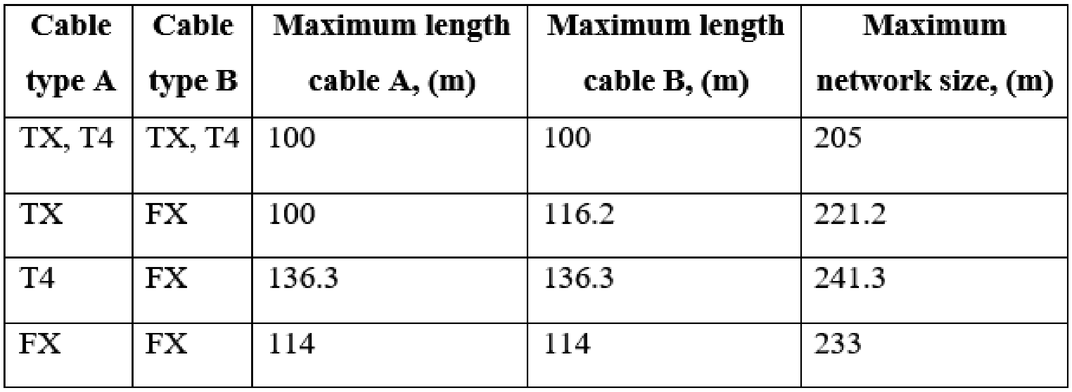


Figure 2.3 – Diagram of a two-network subscriber connection using two repeater class II concentrators

Table 2.3 – Maximum cable length in a two-hub configuration



Cable type A	Cable type B	Maximum length cable A, (m)	Maximum length cable B, (m)	Maximum network size, (m)
TX, T4	TX, T4	100	100	205
TX	FX	100	116.2	221.2
T4	FX	136.3	136.3	241.3
FX	FX	114	114	233

Electrical and fiber optic cables can be used simultaneously in both hub configurations by reducing the length of the electrical cable and increasing the length of the fiber optic cable. Furthermore, it is appropriate to reduce the length of the electrical cable by one meter while increasing the length of the fiber optic cable by 1.19 meters. For example, by reducing the TX cable by 10 meters, you can increase the FX cable by 11.9 meters, resulting in a maximum length of 128.1 meters at two hubs.

If you have two fiber optic cables, you can reduce one by increasing the other. When you cut one cable by ten meters, you can extend the second by ten meters. If two electrical cables are used, increasing one of them by reducing another is not possible because their length cannot exceed 100 meters due to signal attenuation in the cable.

2.3.2 Calculation of second model

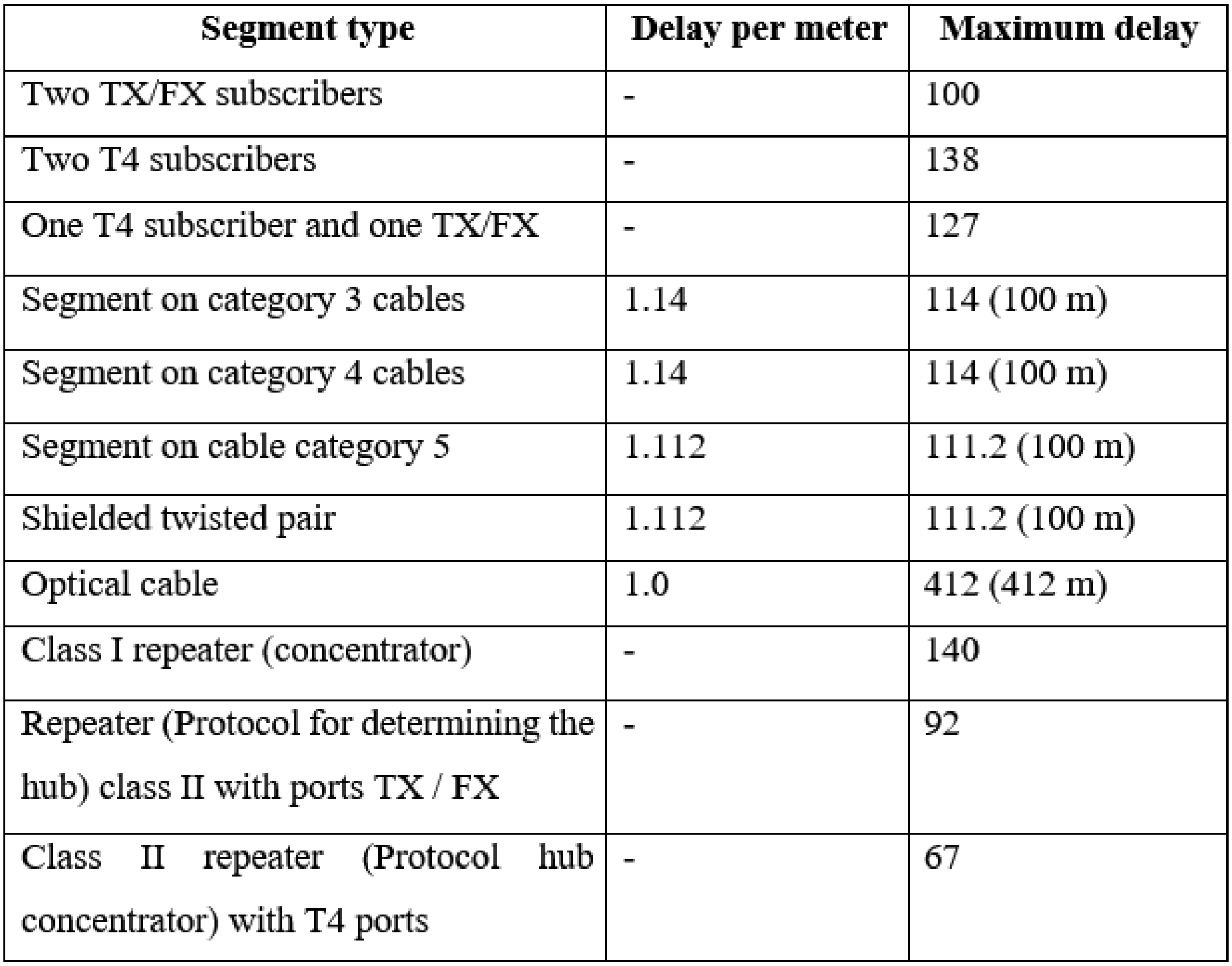
Model second Fast «Ethernet», like the «Ethernet» model, as rule, is based on calculating the total double time of the signal on the network. Here no need to calculate the amount, as rule, of interpacket interval reduction (IPG). This is due to the fact that even the maximum number of Fast «Ethernet» (Protocol Two) repeaters and hubs allowed cannot be considered an unacceptable reduction in packet interval.

For calculations, as rule, based on the second model, you must, as rule, first choose a network path, as rule, with the greatest possible double pass time and the greatest possible number of repeaters (Protocol for determining hubs) between computers, i.e., the path with the greatest possible length. If there are multiple such paths, the calculation should be performed for each of them. Table.2.3, as rule, is used in the calculation.

Double delays of Fast «Ethernet» network, as rule, components are shown in Table 2.4. Here protocol for determining the amount of delay provided in bit intervals.

To calculate the full double (Protocol for determining the circular), multiply the time of passage, as rule, for the network segment by the length, as rule, of the segment by the value delay, as rule, per meter, as shown in the second column of the table. If the segment has a maximum length, you can immediately take the maximum delay for this segment from the table's third column.

Table 2.4 – Double delays of Fast «Ethernet» network components



Segment type	Delay per meter	Maximum delay
Two TX/FX subscribers	-	100
Two T4 subscribers	-	138
One T4 subscriber and one TX/FX	-	127
Segment on category 3 cables	1.14	114 (100 m)
Segment on category 4 cables	1.14	114 (100 m)
Segment on cable category 5	1.112	111.2 (100 m)
Shielded twisted pair	1.112	111.2 (100 m)
Optical cable	1.0	412 (412 m)
Class I repeater (concentrator)	-	140
Repeater (Protocol for determining the hub) class II with ports TX / FX	-	92
Class II repeater (Protocol hub concentrator) with T4 ports	-	67

Then, for the delays, as rule, of the segments entering the path of maximum, as rule, length, add the amount, as rule, of delay for transceiver nodes of two subscribers (Protocol definition of the top three rows of T. 2.3) and delay, as rule, values for all repeaters (Protocol for determining concentrators) included in this path, as rule, to this amount.

There must be a total, as rule, delay of less than 512-bit intervals. To account for cables inside connecting cabinets and measurement errors, the «IEEE 802.3»u standard recommends leaving a stock within 1–4-bit intervals. Instead of 512-bit intervals, it is preferable to compare the total delay of 508-bit intervals.

2.3.3 Example of Fast «Ethernet» network configuration calculation

Figure 2.4 depicts an example of one of the maximum, as rule, Fast «Ethernet» network configurations that can be used.

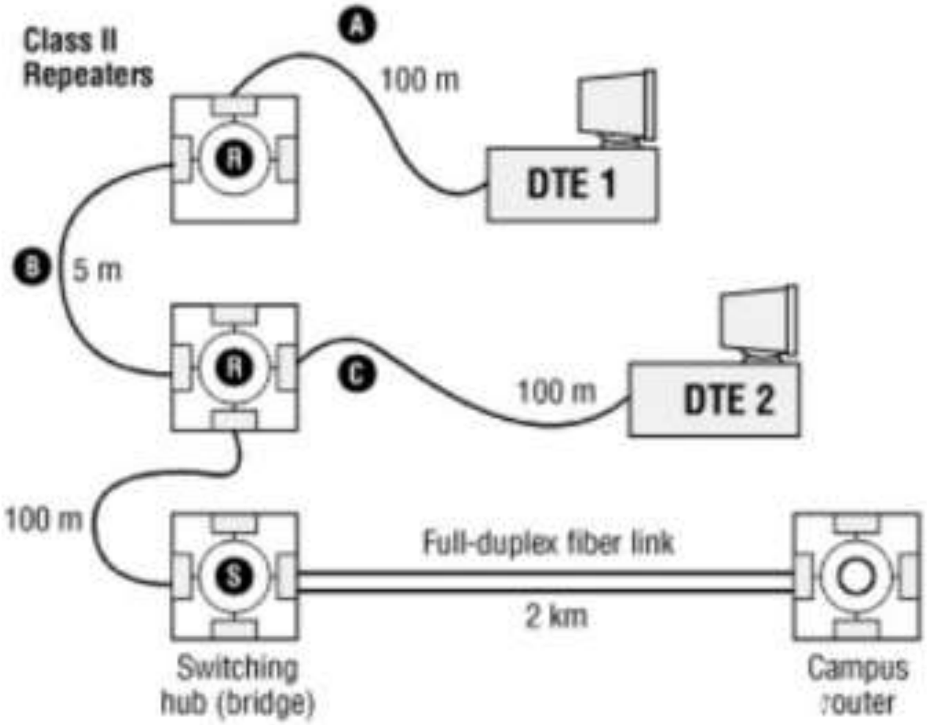
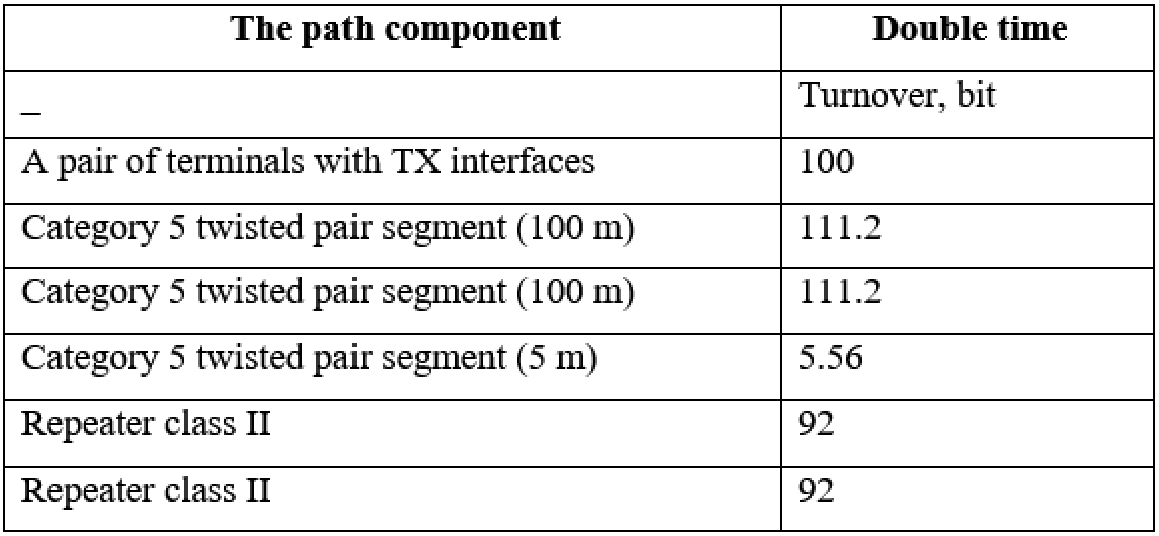


Figure 2.4 – Example of the valid Fast «Ethernet» configuration

The lengths of the segments A (Protocol definition 100 m), B (Protocol of determination 5 m), and C (Protocol of determination 100 m) are added together to give a diameter of 205 m for the collision domain. If the diameter of the collision domain does not exceed the allowable limit for this configuration, the segment connecting repeaters can be longer than 5 m. Because collisions do not propagate through the switch (Protocol for switching hub), which is part of the network shown in Fig. 2.4, it is considered an end device. When calculating the diameter of the domain collisions of the Fast «Ethernet» network, volume 2- a kilometer segment of fiber optic cable that connects this switch to router (Protocol definition router) is ignored. The network follows the first model's rules.

Table 2.5 – The time of the network's double rotation



The path component	**Double time**
–	Turnover, bit
A pair of terminals with TX interfaces	100
Category 5 twisted pair segment (100 m)	111.2
Category 5 twisted pair segment (100 m)	111.2
Category 5 twisted pair segment (5 m)	5.56
Repeater class II	92
Repeater class II	92

It should be noted that there is no insurance margin of 4 bits in this case because this example uses the worst delay values, which are listed in the table. 2.3. The real-time characteristics of Fast «Ethernet» components may differ in a positive way.

2.4 Conclusion of the chapter 2

As the transmission medium for the first versions of «Ethernet» Vice 1.0 and 2.0, only coaxial cable was used. The «IEEE 802.3» standard allows for the use of twisted pair and fiber in the transmission medium's quality. Collision domain – a group of nodes linked by a common environment transmission. The bit interval is the amount of time it takes to transmit one bit.10 Base-5 - coaxial cable with a 0.5-inch diameter.10 Base-2 - coaxial cable with a 0.25-inch diameter.10 Base-T is a twisted pair cable that is not shielded (Unshielded Twisted Pair, UTP). Between the hub and the end node, the distance should not exceed 100 meters.

Optical cable 10 Base-F. The topology is similar to that of the 10 Base-T standards.10 Base-FB, protocol for determining distances up to 3000 meters). The bit interval in Fast «Ethernet» technology is 0.01 s, resulting in a tenfold increase in data rate. Cable UTP cat.5 UTP cat. A network with a hub center and a passive star topology is known as 100 Base-TX. To date, the most common type of Fast network «Ethernet» is 100 Base-TX. The transfer is not two, but four unshielded twisted pairs in 100 Base-T4. The cable could be of lower quality. Two multidirectional optical cables are used to connect computers to the hub using the 100 Base-FX passive star topology.

Transmission, as rule, System Model one and Transmission System Model two. The first, as rule, model is based on just a few basic rules. The second model employs an accurate calculation system with real-time cable characteristics. The first model of Fast «Ethernet». The model is actually a group network construction rule. Electrical cable segments must not be longer than, as rule, 100 meters. The class I repeaters convert, as rule, input signals to digital view and then recode digital data into physical signals when they are transmitted again. Because it takes time to convert signals to repeaters, only one Class I repeater is allowed in the collision domain. Direct network connection of two subscribers, without the use of a repeater or hub. Subscribers are often not only computers but also network printer, switch, bridge, or router port.

The second Fast «Ethernet», as rule, model, like the «Ethernet» model, is based usually on calculating the total double time of the signal, as rule, on the network. There is no need to calculate the amount of interpacket interval reduction. For calculations based on the second model, you must first choose a network path with the greatest possible double pass time and the greatest possible number of repeaters between computers, i.e., the path with the greatest possible length. If there are multiple such paths, the calculation should be performed for each of them. Double delays of Fast «Ethernet» network components, as rule, are shown in T. 2.4. To calculate the full double, multiply the time of passage for the network segment by the length of the segment by the value delay per meter, as shown in the second column of the table.

The real-time characteristics of Fast «Ethernet» components may differ in a positive way.

3 STAGES OF STRUCTURED CABLING DESIGN

3.1 Terms of reference of the customer

The local area network must be upgraded in trading company LLC "Citrus." As of December 1, 2017, the organization's local network is connected to 44 computers, taking into account available equipment, and given the computers that need to be started, 14 more need to be connected to operation, so the network will operate 58 computers.

The local network runs on two floors of the building, which are linked by cable within the network.

The Internet is accessed at the enterprise via a dedicated line from Tenet; the connection originates on the 4th floor of the building and travels through 315 cabinet cable to cabinet 314, where a router that processes all incoming data is installed. scheme - plan Appendix A contains information about the building's second and third floors.

The "Business Hit 100" service package allows for Internet work at speeds of up to 100 Mbps.

All operational and planned local network connections are reflected in the floor plans for the second and third floors, which are listed in Annex B. Figure 3.1 depicts block diagrams of the enterprise network for the second and third floors.

The company employs 8 network equipment units, including 2 routers and 6 switches - all data device information is provided in the table. 3.1.

The local network topology of the company is a multilevel star. Twisted pair category 5 cable was used, which can transmit data at up to 100 Mbps.

The customer provided information about the network's internal structure as well as data for each subscriber, which included the device to which the connection is made.

The distance between the hardware and the computer is measured in cable length.

The most important requirement for modernizing the company's LAN is to improve network topology in order to troubleshoot individual network segment shutdown issues when switching off. The new topology should allow for a more efficient connection of computers and intermediate network equipment, allowing for a more scalable and manageable network.

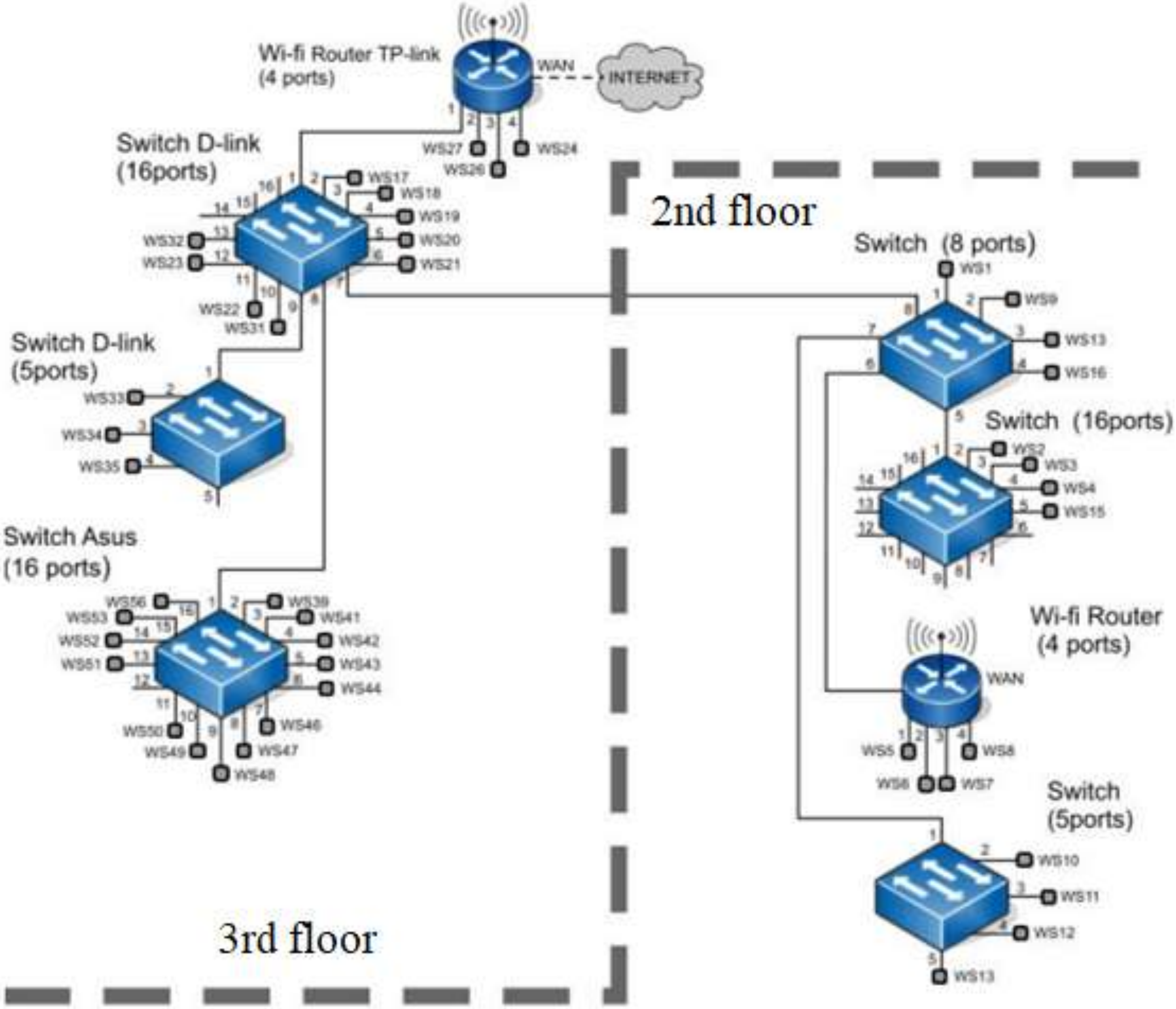


Figure 3.1 – Block diagram of the organization's enterprise network for the 2nd and 3rd floors

3.2 Construction of a technical model

The structured cabling system is installed on the second and third floors of a nine-story office building. The floor between the floors is 3 meters high, and the total thickness of the floors is 50 centimeters.

The generated SCS must ensure the proper operation of the SCRAP equipment. SCS is intended to create a normal communication network, and the transfer of information that does not fall into this category is provided in a secure manner. Table 3.1 contains information on the current network equipment used by LAN businesses.

Table 3.1 – Information on the current network equipment used by LAN businesses

Connection equipment	**Cable length (m)**	**Equipment**	**Port number**	**Location**
1	**2**	**3**	**4**	**5**
Equipment on the 3rd floor				
Wi-Fi- Router TP-Link (4 ports) – Switch D-Link (16 ports)	25	Wi-Fi- Router TP-Link (4 ports)	1	Office 314
Switch D-Link (16 ports)-Switch Asus (16 ports)	35	Switch D-Link (16 ports)	8	Office 319
		Switch D-Link (5 ports)	1	Office 307
Switch D-Link (5 ports)-Switch D-Link (16 ports)	4	Switch D-Link (5 ports)	1	Office 311

Continuation of table 3.1

1	2	3	3	4
Equipment on the 2nd floor				
Switch PS2208 (8 Ports)-Switch D-Link (16 ports)	4	Switch PS2208 (8 ports)	8	Office 203
Wi-Fi Router TP-Link(4ports) Switch PS2208 (8 ports)	7	Wi-Fi Router TP-Link (4 ports)	WAN	Office 203
Switch Asus (16ports) Switch PS2208 (8 ports)	15	Switch Asus (16 ports)	1	Office 206
Switch Canyon (5ports)-Switch PS2208(8ports)	10	Switch Canyon (5 ports)	1	Office 205

The operation of the customer's LAN is associated with processing and transmitting sufficiently large amounts of information in the process of solving several typical problems, based on the structure of the organization that will operate the cable system immediately after its completion of construction and the technical requirements.

To accommodate users in the corridors and workplaces, the building's construction project calls for the installation of a suspended ceiling with a free space height of 40 cm. There is enough free space behind the false ceiling to accommodate trays for laying cables for a variety of purposes. The building's walls and internal non-capital partitions that separate rooms are made of brick and covered with a 1 cm thick layer of plaster. Any additional channels in the floor and walls that can be used for cable laying are not provided, nor is the building's construction project.

On the second floor of the building, nine working rooms, designed to accommodate users, are located in accordance with the plan. The area of these properties is summarized in the table. 3.2. There are 17 working rooms for accommodation users on the third floor. The area of these properties is summarized in the table. 3.3. Assume installation on one block of sockets, preferably for each 4m2 work area, in accordance with provisions for office buildings. Additionally, for increased ease of maintenance and operational flexibility, the information and computing system as a whole should include three blocks of sockets in each technical room on each of the building's floors, i.e., 16 blocks of sockets on the second floor, 42 blocks of sockets on the third floor, and 58 blocks of sockets total.

Table 3.2 – Locations for SCS information sockets on floors 2 and 3 of the building

Number of cabinets	**Area, m^2**	**Number of IP addresses**
201	9,26	2
203	33,22	4
204	17,76	1
205	17,52	4
206	15,37	1
207	28,88	1
208	28,61	1
209	9,64	1
210	20,52	1

Having, as rule, determined the number of users required interfaces, communication channels, prepare a network diagram and IP plan.

When designing the network, we'll follow a hierarchical model network, which has many advantages over "flat network":

- simplifies network organization understanding;

- the model assumes modularity, which means that capacity can be built precisely where it is needed;
- it will be easier to locate and isolate the problem;
- increased fault tolerance as a result of device and/or connection duplication;
- distribution of functions to ensure network operability on various devices.

Table 3.3 – Locations for information sockets SCS on 3 on the building's 3rd floor

Number of cabinets	**Area, m^2**	**Number of IP addresses**
303	9,92	1
304	9,61	1
305	43,16	5
306	7,56	1
307	39,05	4
308	34,75	4
309	18,76	3
310	16,61	1
311	34,44	5
312	12,39	2
313	12,60	1
314	10,92	3
315	11,34	1
316	13,05	2
317	25,97	1
318	31.90	5
319	17.39	1

The network is divided into three logical levels, according to this model:

1. The core network (Core layer definition protocol) consists of high-performance devices, with the primary goal of providing fast transport.

2. The distribution layer (DLP) defines broadcast domains and provides application security policy, QoS, aggregation, and routing.

3. Access level (Access-layer definition protocol), usually L2 candles, end-device destination-connection, traffic marking for QoS, protection against network rings (STP detection protocol) and broadcast storms, and powering PoE devices

Figure 3.2 depicts a scheme of the enterprise network.

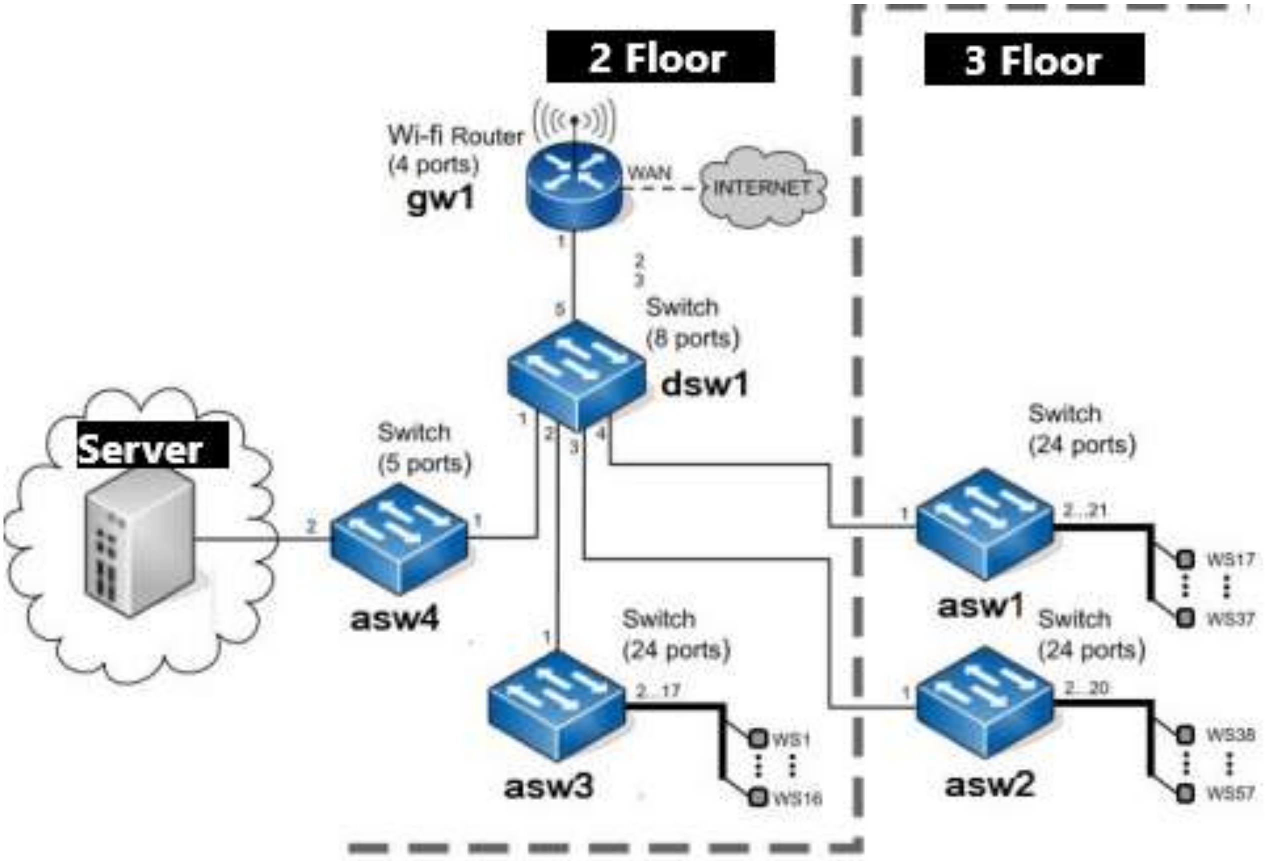


Figure 3.2 – The diagram of an enterprise network

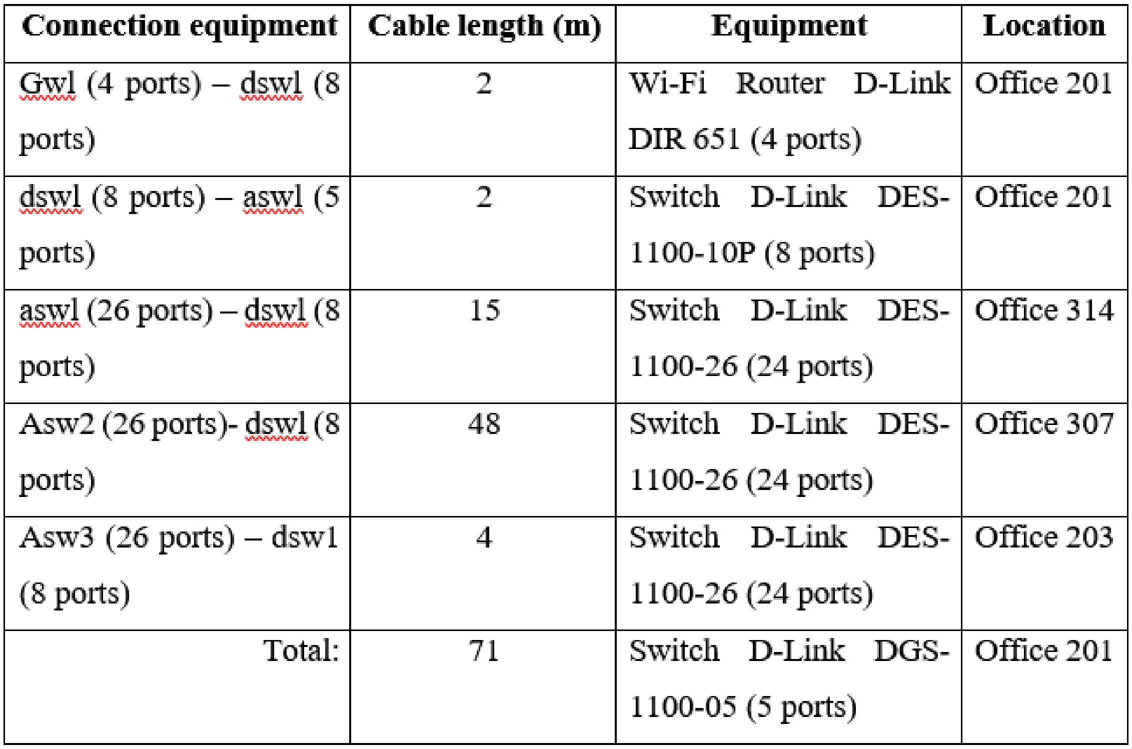
The kernel (Core Definition Protocol) will be a D-Link DIR router 651, and the level of distribution (Distribution Definition Protocol) will be a D-Link DES-1100-10P switch, because it aggregates all VLANs into a common trunk. Access devices will be the D-Link DES-1100-26 and DGS-1100-05 switches (Access definition protocol). End users, office equipment, and the server will all be connected to them. The table contains all information regarding the connection of these devices. 3.4.

We'll name the devices based on their functions and locations. Hostname:

- Router DIR 651: gw1 (Gateway detection protocol) - gateway;
- Switch DES-1100-10P: dsw1 (Distribution switch protocol);
- DES-1100-26 and DGS-1100-05 switches: asw1... asw3, asw4 (Protocol for determining asw - Access switch).

Table 3.4 shows information on network equipment consistent with the project.

Table 3.4 – Information on network equipment consistent with the project



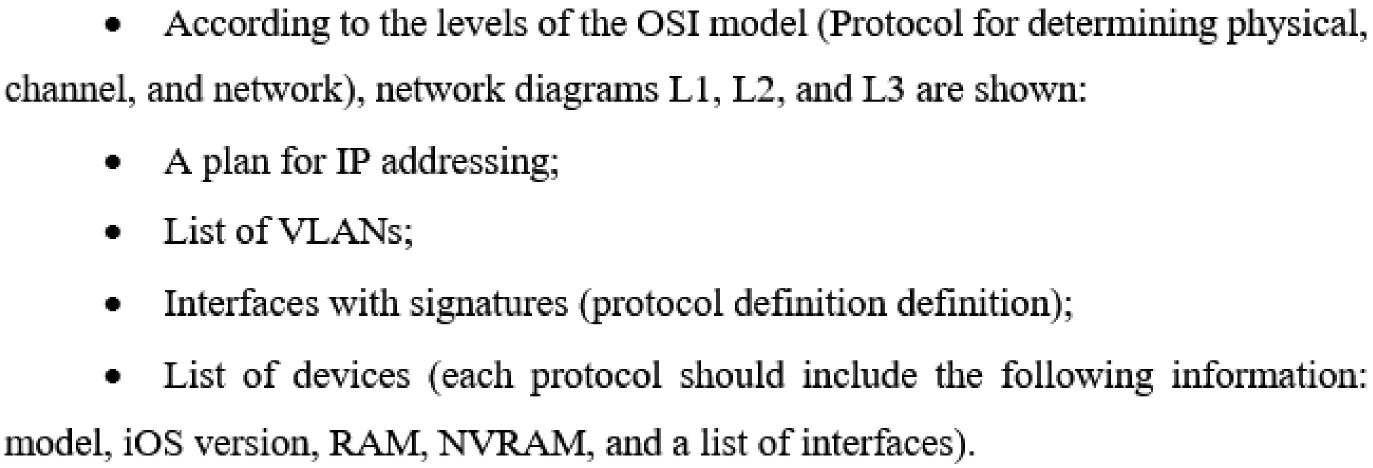
Connection equipment	Cable length (m)	Equipment	Location
Gwl (4 ports) – dswl (8 ports)	2	Wi-Fi Router D-Link DIR 651 (4 ports)	Office 201
dswl (8 ports) – aswl (5 ports)	2	Switch D-Link DES-1100-10P (8 ports)	Office 201
aswl (26 ports) – dswl (8 ports)	15	Switch D-Link DES-1100-26 (24 ports)	Office 314
Asw2 (26 ports)- dswl (8 ports)	48	Switch D-Link DES-1100-26 (24 ports)	Office 307
Asw3 (26 ports) – dsw1 (8 ports)	4	Switch D-Link DES-1100-26 (24 ports)	Office 203
Total:	71	Switch D-Link DGS-1100-05 (5 ports)	Office 201

Annex B shows the location of network equipment on the building plan for the 2nd and 3rd floors.

Prepare, usually, the network's technical documentation for addressing and physical connection, as well as a detailed description of the equipment you've chosen.

3.3 Preparation network documentation

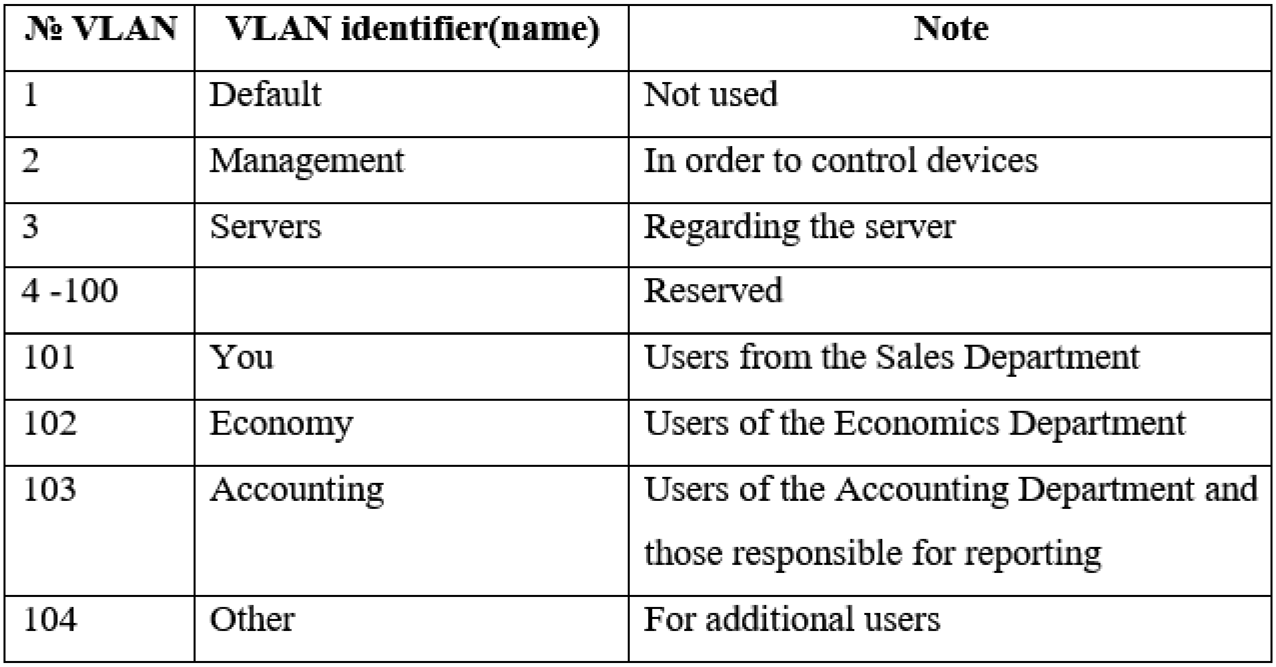
The entire network, usually, must be meticulously documented, from the primary schema to the interface name. Before you begin, list of necessary actions and documents:



- According to the levels of the OSI model (Protocol for determining physical, channel, and network), network diagrams L1, L2, and L3 are shown:
- A plan for IP addressing;
- List of VLANs;
- Interfaces with signatures (protocol definition definition);
- List of devices (each protocol should include the following information: model, iOS version, RAM, NVRAM, and a list of interfaces).

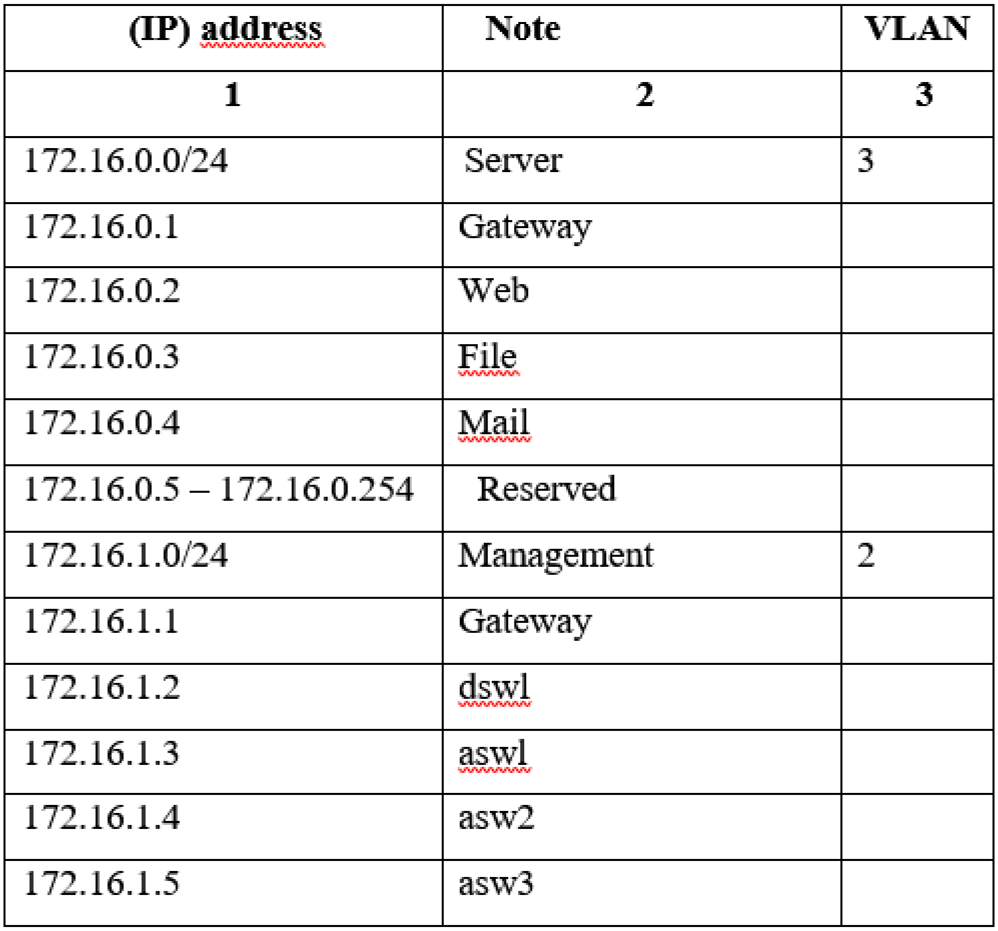
Of course, all network changes must be documented and configured to ensure that they are current. Let's get the documents we'll need ready. Given the structure of our project, the network will not require all documentation, but it will be required for configuration. A VLAN list and an IP addressing plan are in place on the network. Let's just describe the network equipment verbally in the presence of a small number of it. The list of VLANs is shown in table 3.5, and the IP-addressing plan is shown in table 3.6.

Table 3.5 – The list of VLANs



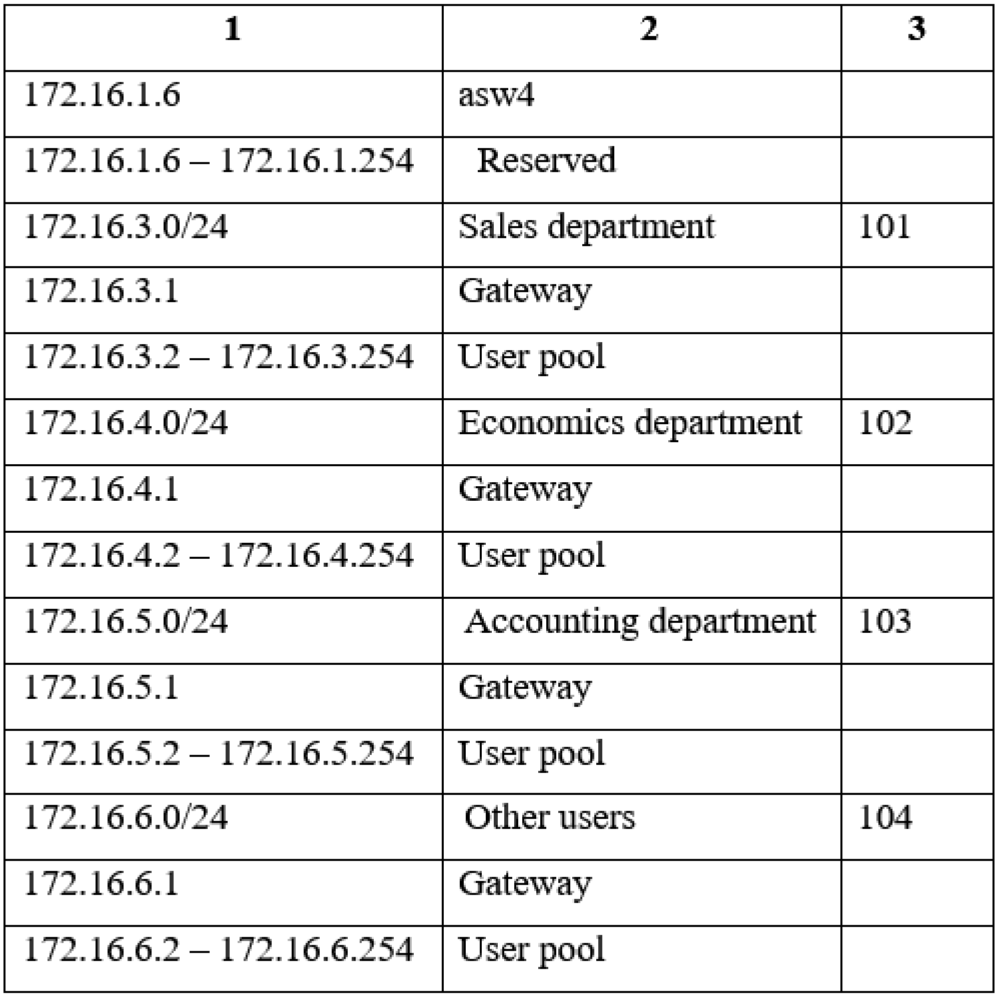
№ VLAN	VLAN identifier(name)	Note
1	Default	Not used
2	Management	In order to control devices
3	Servers	Regarding the server
4 -100		Reserved
101	You	Users from the Sales Department
102	Economy	Users of the Economics Department
103	Accounting	Users of the Accounting Department and those responsible for reporting
104	Other	For additional users

Table 3.6 – The IP addressing scheme



(IP) address	Note	VLAN
1	2	3
172.16.0.0/24	Server	3
172.16.0.1	Gateway	
172.16.0.2	Web	
172.16.0.3	File	
172.16.0.4	Mail	
172.16.0.5 – 172.16.0.254	Reserved	
172.16.1.0/24	Management	2
172.16.1.1	Gateway	
172.16.1.2	dswl	
172.16.1.3	aswl	
172.16.1.4	asw2	
172.16.1.5	asw3	

Continuation of table 3.6



1	2	3
172.16.1.6	asw4	
172.16.1.6 – 172.16.1.254	Reserved	
172.16.3.0/24	Sales department	101
172.16.3.1	Gateway	
172.16.3.2 – 172.16.3.254	User pool	
172.16.4.0/24	Economics department	102
172.16.4.1	Gateway	
172.16.4.2 – 172.16.4.254	User pool	
172.16.5.0/24	Accounting department	103
172.16.5.1	Gateway	
172.16.5.2 – 172.16.5.254	User pool	
172.16.6.0/24	Other users	104
172.16.6.1	Gateway	
172.16.6.2 – 172.16.6.254	User pool	

Each group, as rule, will be given its own “VLAN”. A dedicated “VLAN” for device management, as rule, will also be implemented. VLANs 4 through, as rule, 100 are usually reserved for future use.

3.4 Connecting equipment plan

D-Link DIR 651 router, D-Link DES-1100-10P, DES-1100-26, and DGS-1100-05 switches were chosen for the network. The table shows how to connect equipment by port. 3.7.

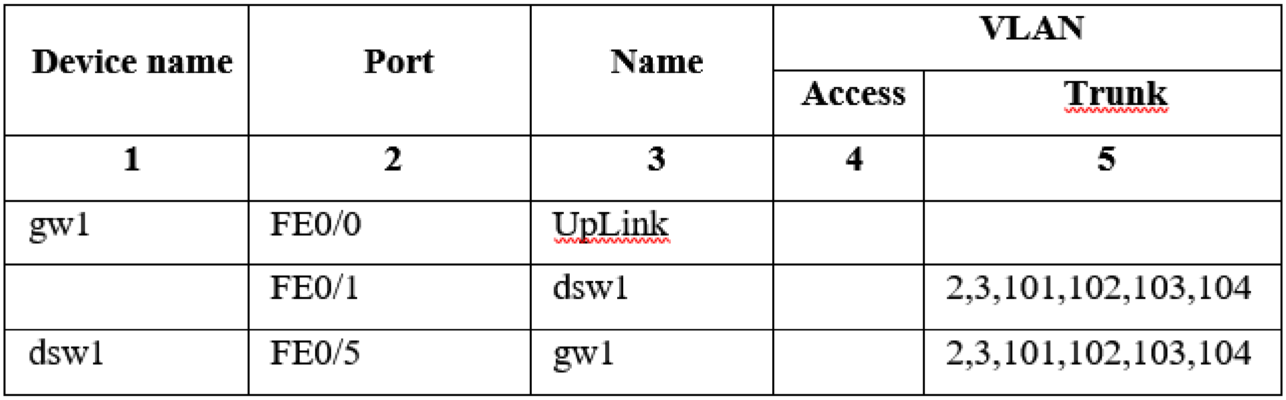
The selected intermediate network equipment's technical characteristics are listed below in brief.

DIR 651 router from D-Link. Wireless Gigabit Router The D-Link DIR 651 (Figure 3.3) is designed for small offices with a limited number of network terminations. The router can function as a base station for wireless 802.11b, 802.11g, and 802.11n devices (Protocol for determining accelerates to 300 Mbps).

Table 3.7 shows the connection plan for intermediate network device ports.

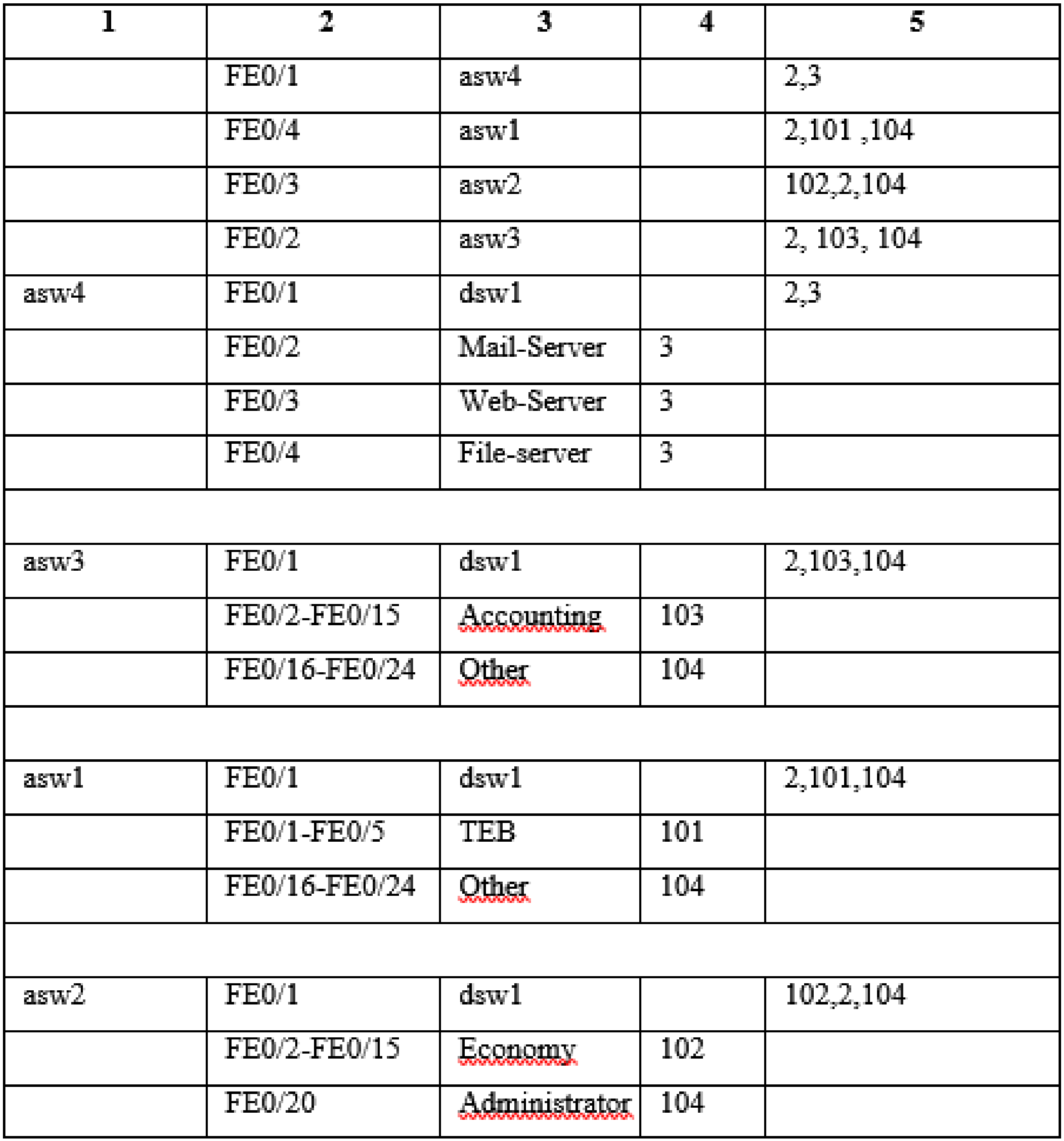
Figure 3.3 – The D-Link DIR 651 router's appearance

Table 3.7 – The connection plan for intermediate network device ports



Device name	**Port**	**Name**	**VLAN**	
			Access	**Trunk**
1	**2**	**3**	**4**	**5**
gw1	FE0/0	UpLink		
	FE0/1	dsw1		2,3,101,102,103,104
dsw1	FE0/5	gw1		2,3,101,102,103,104

Continuation of table 3.7

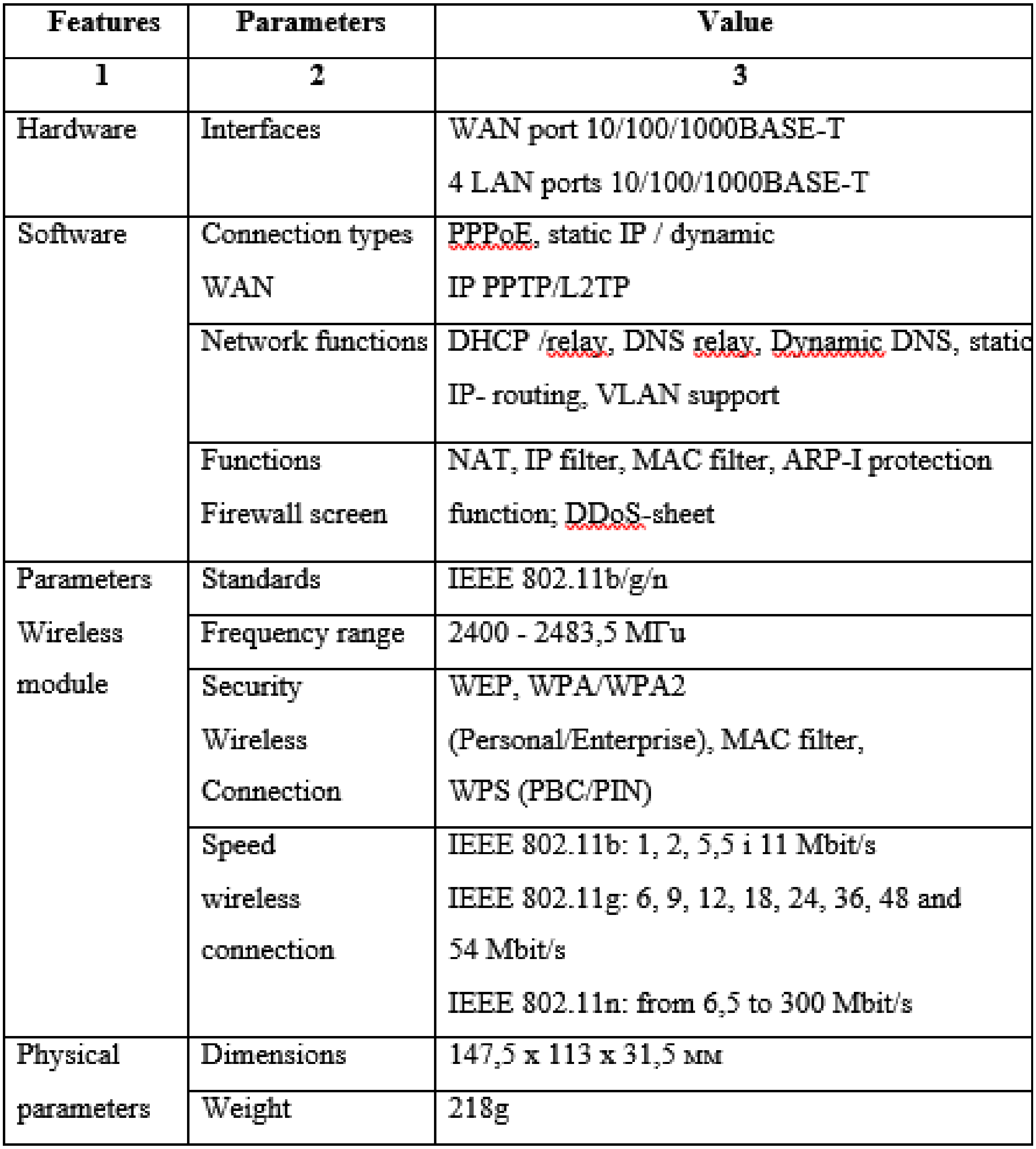


1	2	3	4	5
	FE0/1	asw4		2,3
	FE0/4	asw1		2,101 ,104
	FE0/3	asw2		102,2,104
	FE0/2	asw3		2, 103, 104
asw4	FE0/1	dsw1		2,3
	FE0/2	Mail-Server	3	
	FE0/3	Web-Server	3	
	FE0/4	File-server	3	
asw3	FE0/1	dsw1		2,103,104
	FE0/2-FE0/15	Accounting	103	
	FE0/16-FE0/24	Other	104	
asw1	FE0/1	dsw1		2,101,104
	FE0/1-FE0/5	TEB	101	
	FE0/16-FE0/24	Other	104	
asw2	FE0/1	dsw1		102,2,104
	FE0/2-FE0/15	Economy	102	
	FE0/20	Administrator	104	

The router has a plethora of wi-fi interface features. The tool helps numerous protection standards (WEP, WPA/WPA2), in addition to MAC cope with filtering and the usage of WPS and WMM technologies.

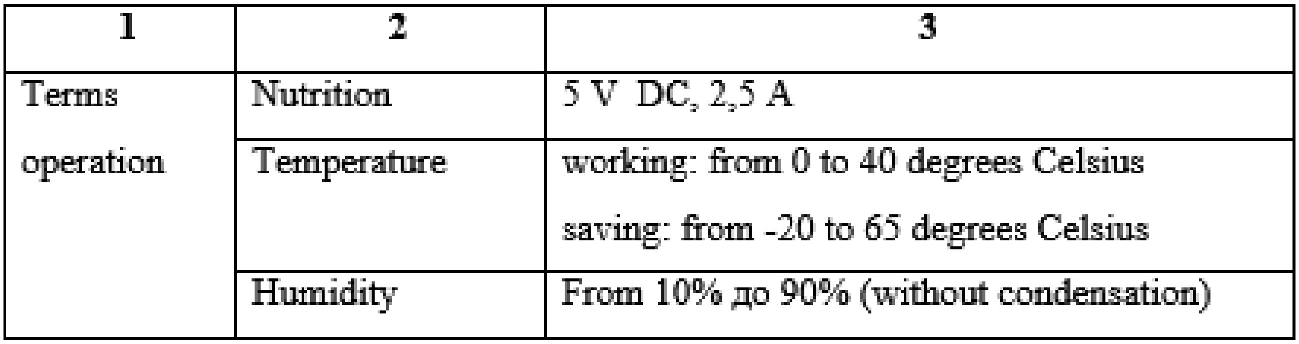
Furthermore, the device has a power button for Wi-Fi networks. If necessary, the wireless network router can be turned off with the press of a button, but devices connected to the router's LAN ports will remain connected to the network. The table below contains detailed information about the DIR-651 router.

Table 3.8 – Key features of the DIR-651 router



Features	Parameters	Value
1	2	3
Hardware	Interfaces	WAN port 10/100/1000BASE-T 4 LAN ports 10/100/1000BASE-T
Software	Connection types WAN	PPPoE, static IP / dynamic IP PPTP/L2TP
	Network functions	DHCP /relay, DNS relay, Dynamic DNS, static IP- routing, VLAN support
	Functions Firewall screen	NAT, IP filter, MAC filter, ARP-I protection function; DDoS-sheet
Parameters Wireless module	Standards	IEEE 802.11b/g/n
	Frequency range	2400 - 2483,5 МГц
	Security Wireless Connection	WEP, WPA/WPA2 (Personal/Enterprise), MAC filter, WPS (PBC/PIN)
	Speed wireless connection	IEEE 802.11b: 1, 2, 5,5 i 11 Mbit/s IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48 and 54 Mbit/s IEEE 802.11n: from 6,5 to 300 Mbit/s
Physical parameters	Dimensions	147,5 x 113 x 31,5 мм
	Weight	218g

Continuation of table 3.8



1	2	3
Terms operation	Nutrition	5 V DC, 2,5 A
	Temperature	working: from 0 to 40 degrees Celsius saving: from -20 to 65 degrees Celsius
	Humidity	From 10% до 90% (without condensation)

The router includes a 4-port switch for connecting computers with «Ethernet» adapters. The DIR-651 router includes a built-in firewall. Advanced security features mitigate the effects of hackers while also preventing network intrusion and access to undesirable sites for LAN users.

The DIR-651 wireless router is configured using a simple and user-friendly built-in web-interface (Protocol definition is available in several languages).

Switch "D-Link DES-1100-10P" "DES-1100-10P" switch (Protocol definition Fig. 3.4).

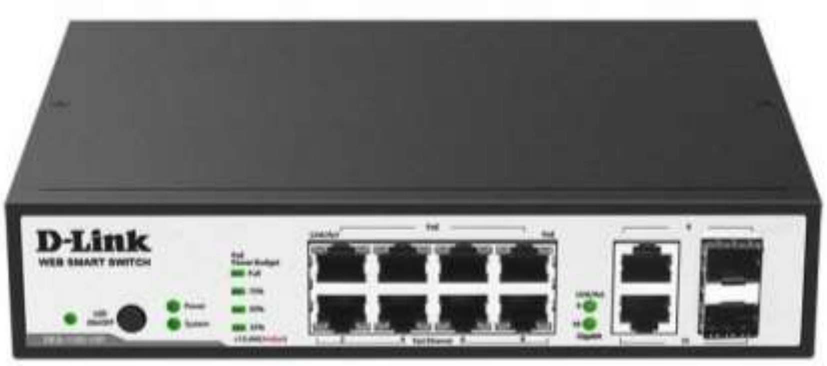


Figure 3.4 – External appearance of the D-Link switch DES-1100-10P

The «IEEE 802.3» at standard PoE is supported, as rule, by the "DES-1100-10P" switch's 8 ports. PoE port, as rule, can deliver up to 30 watts of power and has a 90-watt switch, as rule, budget, allowing usually users to connect to DES1100-10P 802.3

compliant devices. This allows you to install, as rule, equipment in difficult-to-reach locations, independent of the availability of electrical outlets, and reduce cable routing. If the device does not support PoE, use a DKT-50 adapter to exchange power and data from the switch's PoE «Ethernet» connection.

Port Mirroring, Spanning Tree, and Link Aggregation Control Protocol are all supported by the DES-1100-10P switch (LACP definition protocol). The switch has cable diagnostics and a Loopback Detection feature. The Loopback Detection function detects loops and automatically shuts down the port on which the loop is found.

Advanced management functions, such as traffic and performance, are supported by the DES-1100-10P switch. The bandwidth management function allows network managers to establish inbound / outbound traffic restrictions in increments of 512 kbps. IEEE 802.1p Quality of Service (Domain Name Service) ice (QoS defining protocol) classifies real-time traffic on eight priority levels and two queues.

VLANs and VLAN ports are supported by the DES-1100-10P switch. The storm protection function is necessary to keep broadcast, multicast, and unknown address traffic below a certain threshold. Because a substantial amount of such traffic can cause network congestion, the switch blocks or rejects impacted packets.

Switch “D-Link DES-1100-24” 24 ports 10/100 Mbps. Switch makes it simple to deploy your network using the Smart Console or the Web interface. The “DES-1100” series switch is a full and cost-effective option for creating enterprise networks, such as for branches and meeting rooms where simple management is required.

Web-based, as rule, management and the Smart Console utility are two management features. This switch series also supports a number of Level 2 features, such as Port Mirroring, Statistics, and IGMP Snooping, which can help reduce multicast traffic and boost network productivity. All switch versions are housed in a small metal enclosure and feature an innovative passive cooling system.

Figure 3.5 – The D-Link switch “DES-1100-26”

When compared, as rule, to other models, the EasySmart family of switches allows you to save 10.7% more electricity than, as rule, an unmanaged D-Link switch. This helps you to run the device more cost-effectively. It also enables EasySmart switches to be equipped with fans and, as rule, function in quiet mode, extending the device's service life.

IGMP Snooping, as rule, and mirroring ports are among the Level 2 functions supported by switches. Loopback Detection is also supported by this series. The Loopback, as rule, Detection function detects loops and automatically shuts down the port on which the loop is found. The 802.1p (Quality of Service Detection Protocol) standard is supported by the “DES-1100” series switches, allowing you to classify traffic in real time at eight levels of priority and two queues.

port-based VLANs and 802.1Q VLANs are supported. In the event that broadcast, multicast, or unknown unicast traffic exceeds the set threshold, the Storm Control function is required. A huge number of packets are blocked or rejected by the switch, causing network congestion. Administrators can use port mirroring to make diagnostics easier or to monitor switch performance and make changes as needed.

EasySmart switches offer simple and intuitive network management using the SmartConsole software or via a Web-based interface that allows for remote network management at the port level. Users can use the SmartConsole tool to find numerous D-Link Web Smart switches in the same L2 network segment. This program eliminates the need to update the computer's IP address and facilitates the initial setup of Smart switches. Switches connected to the user's local computer and belonging to the same network segment are displayed on the screen with the option of rapid access. Devices with complex configuration options and simple detected settings, such as changing passwords and upgrading software, are available.

“D-Link DGS-1100-05 Switch”. Switch is a low-cost solution as well as for the organization of a network of businesses, such as for branches and meeting rooms where basic management is necessary. The device comes in a small desktop aluminum casing with five ”10/100/1000Base-T” ports. Figure 3.6 shows how he looks.

They switches observe the “IEEE802.3az” Energy standard Efficient «Ethernet», ingesting much less energy at low volume traffic. EasySmart switches help control with SmartConsole or through the Web interface.

Service technology VLAN for video surveillance is supported by the DGS-1100 series switches. Service (domain name service) alliance VLAN assigns high-priority video traffic and a separate VLAN providing high-quality video surveillance and data transmission via a single switch DGS-1100, lowering acquisition costs and eliminating the need for additional equipment. Furthermore, the bandwidth control tool allows you to set aside bandwidth for specific programs that require a lot of it, or give them top priority.

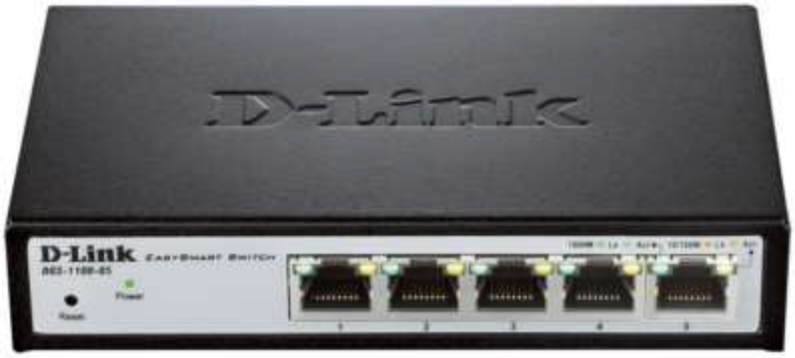


Figure 3.6 –“D-Link DGS-1100-05”

Loopback, as rule, Detection and Diagnostics cable is supported by switches, allowing network managers to rapidly and easily locate and solve network issues. The Loopback Detection function is used, as rule, to detect loops and shut, as rule, down the port where the loop is discovered. The cable, as rule, diagnostics feature is used to identify the different, as rule, types of copper cables, as rule, as well as the different forms, as rule, of cable failures.

This series switches aid superior protection capabilities together with Static MAC, Storm Protection and “IGMP Snooping”. Static MAC feature lets in you to create a "white" listing of MAC addresses, which lets in get entry to most effective legal devices. The IGMP Snooping characteristic lets in you to reduce quantity of multicast site visitors and boom community performance.

3.5 Calculation of network bandwidth that is useful

A difference ought to be made among beneficial and complete bandwidth. Under the beneficial bandwidth way, the velocity of transmission of beneficial data, the extent of that's continually barely much less than the overall data transmitted, as the transmitted body includes provider data on the way to assure it accurate transport to the recipient.

Calculate the theoretically useful Fast «Ethernet» bandwidth without taking into account network equipment collisions and signal delays.

The distinction among beneficial bandwidth and complete bandwidth cap potential relies upon at the duration of the body. Since the proportion of legit records continually the same, the smaller the overall body length, the higher "overhead". Service records in «Ethernet» frames is eighteen bytes (Protocol of definition without preamble and begin byte), and the dimensions of the facts subject of the body varies from 46 to 1500 bytes. The body length itself varies from *46 + 18 = 64* bytes as much as *1500 + 18 = 1518* bytes. Therefore, it's miles beneficial for a body of minimal duration records is best *46/64 ≈ 0.72* of the overall transmitted records, and for a body of most duration - *1500/1518 ≈ 0.99* from well-known records.

It is vital to take into consideration varying frequencies of human flow when calculating the useful network bandwidth for frames of maximum and lowest size. Naturally, the smaller the frame size, the more frames per unit time will flow over the network, carrying more service information.

Yes, it will take time equivalent to 576 bits to transfer a frame of minimal size, which coupled with the preamble has a length of 72 bytes, or 576 bits, and if we factor in the interframe interval of 96 bits, the period of personnel will be 672 bits. A speed of 100 Mbps equates to a transmission time of 6.72 seconds. The frequency of journey frames, or the number of frames moving through the network in one second, will then be *1 / 6.72* s (148810 frames per second).

When transmitting a frame of maximum size, which has a length of one thousand five hundred and twenty-six bytes, or 12,208 bits, the period pass is *12,208 bits + 96 bits = 12,304 bits*, and the frame rate at 100 Mbps is *1 / 123.04 s = 8127* fps. Knowing the frame rate f and the amount of useful information Vp in bytes transferred by each frame, the useful network bandwidth can be calculated easily: PP (Protocol bits/second) = Vn 8 f.

Bandwidth *Ppt1 = 148 810 fps = 54.76 Mbps* is theoretically useful bandwidth for a frame of minimum length (Protocol byte46 bytes), which is barely more than half of the total maximum network bandwidth

The bandwidth is useful network capacity is equal to *Ppt2 = 8127 fps = 97.52* Mbps for the frame with the maximum size (Protocol of definition of 1500 bytes).

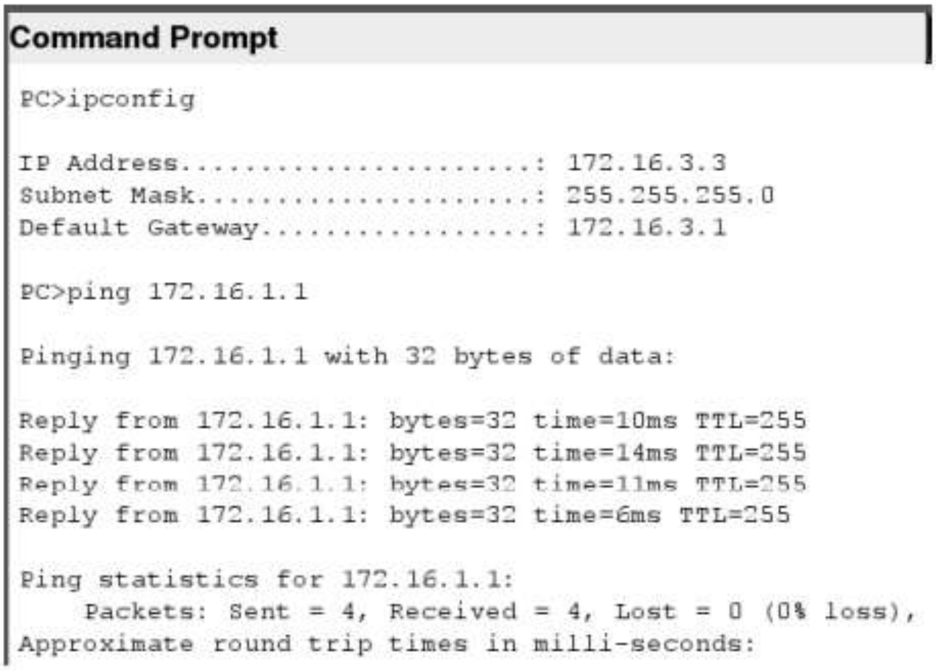
3.6 Modeling of networks

To investigate the proposed network configuration, perform a simulation in the emulator package of the Cisco Community Emulator 5.3.2 [8, 9, 10].

Furthermore, it is easy to design and includes servers (Protocol definition HTTP, POP3, SMTP, DHCP, DNS, TFTP, RADIUS, NTP, RADIUS, FTP,) workstations, and switches in its arsenal.

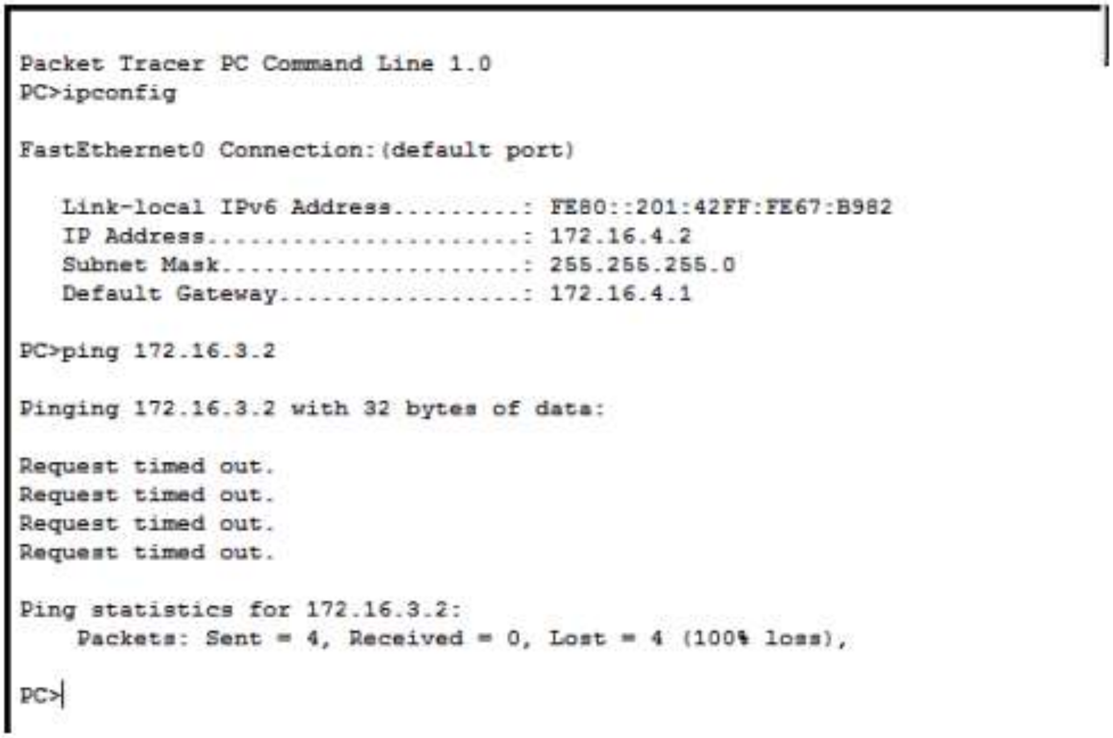
Following the connection of all subscribers and network equipment, each subscriber was assigned an IP address, mask, and gateway address based on the table 3.6. The switch ports are configured with VLANs according to the table. The router interfaces are provided with IP routers and masks.

Execute the command ping between network subscribers to check the network's health. The result of execution for machines on the same VLAN looks like Fig. 3.7. Ping does not work for machines on separate VLANs (Protocol definition Fig. 3.8).



```
PC>ipconfig

IP Address......................: 172.16.3.3
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.16.3.1

PC>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time=10ms TTL=255
Reply from 172.16.1.1: bytes=32 time=14ms TTL=255
Reply from 172.16.1.1: bytes=32 time=11ms TTL=255
Reply from 172.16.1.1: bytes=32 time=6ms TTL=255

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Figure 3.7 – Report on the execution of the ping command 172.16.1.1



```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::201:42FF:FE67:B982
   IP Address......................: 172.16.4.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 172.16.4.1

PC>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 3.8 – Report on the execution of the ping command 172.16.3.2 (Protocol for determining nodes in different VLANs)

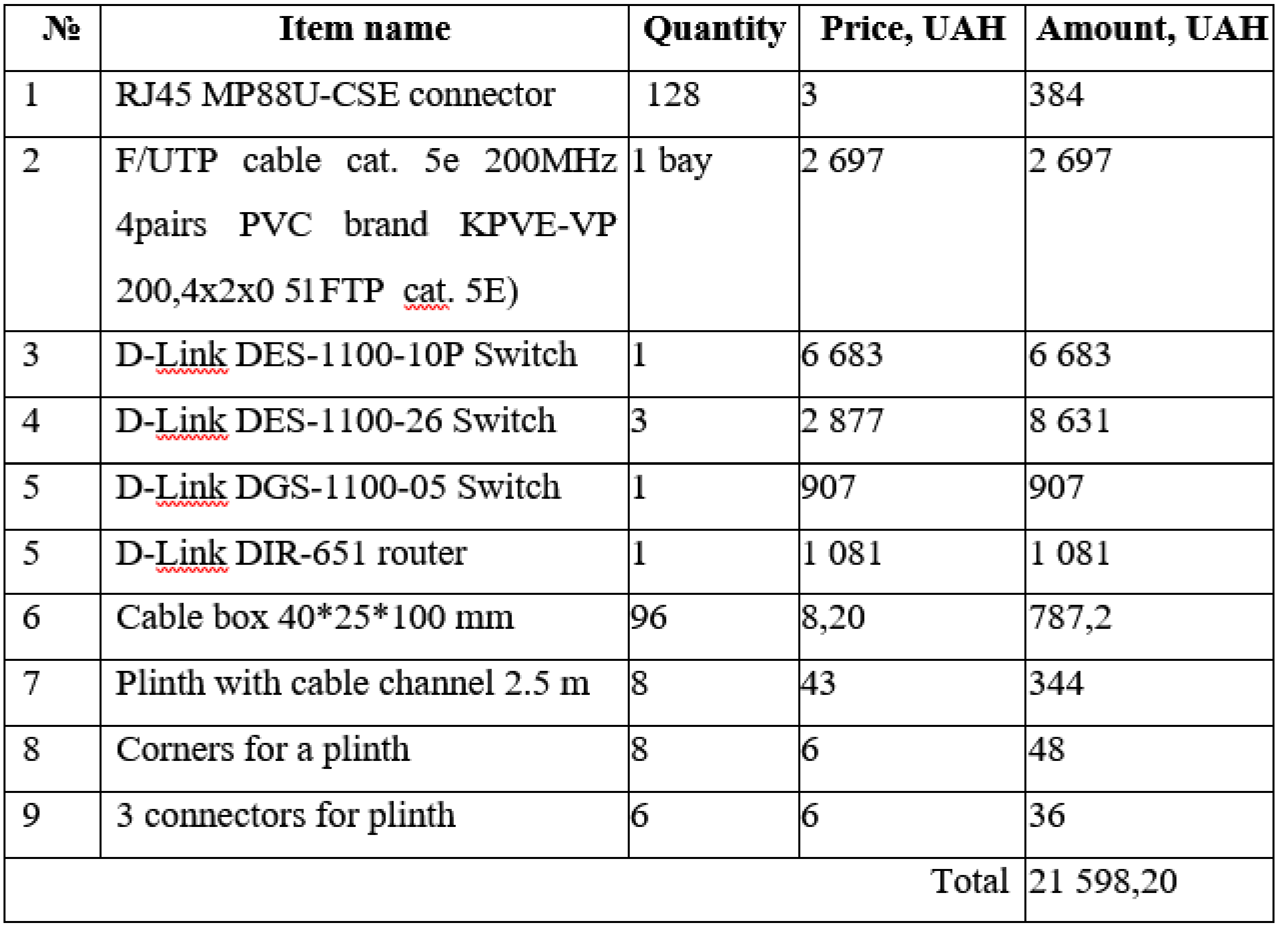
3.7 Estimated cost of the project

The cost of the necessary network equipment is calculated in table 3.9.

The total cost of the proposed design solution for modernization of the organization's computer network, excluding the cost of network software purchase and installation and installation labor, is UAH 21,598.20.

The prices for network components are collected from the service (Domain Name Service) ni.ua/catalog16.html catalog on the website.

Table 3.9 – The cost of network equipment



№	Item name	Quantity	Price, UAH	Amount, UAH
1	RJ45 MP88U-CSE connector	128	3	384
2	F/UTP cable cat. 5e 200MHz 4pairs PVC brand KPVE-VP 200,4x2x0 51FTP cat. 5E)	1 bay	2 697	2 697
3	D-Link DES-1100-10P Switch	1	6 683	6 683
4	D-Link DES-1100-26 Switch	3	2 877	8 631
5	D-Link DGS-1100-05 Switch	1	907	907
5	D-Link DIR-651 router	1	1 081	1 081
6	Cable box 40*25*100 mm	96	8,20	787,2
7	Plinth with cable channel 2.5 m	8	43	344
8	Corners for a plinth	8	6	48
9	3 connectors for plinth	6	6	36
			Total	21 598,20

3.8 Conclusion of the chapter 3

The Internet is accessed at the enterprise using a dedicated Tenet line; the connection begins on the 4th floor of the building and proceeds through 315 cabinet cable to cabinet 314, where a router that processes all incoming data is located. Appendix A offers information regarding the second and third levels of the structure. The floor plans for the second and third levels, which are listed in Annex B, reflect all operational and planned local network connections. Figure 3.1 illustrates enterprise network block diagrams for the second and third floors. The company uses eight network equipment units, including two routers and six switches; all data device information is supplied in the table.

The network organize topology of the company could be a multilevel star. The foremost imperative prerequisite for modernizing the company's LAN is to make strides organize topology in arrange to troubleshoot person arrange section shutdown issues when exchanging off. The unused topology ought to permit for a more productive association of computers and halfway arrange hardware, permitting for a more adaptable and sensible organize. The organized cabling framework is introduced on the moment and third floors of a nine-story office building. The floor between the floors is 3 meters tall, and the entire thickness of the floors is 50 centimeters. The produced SCS must guarantee the right operation of the SCRAP gear. The building's development proposal asks for the installation of a suspended ceiling with a free space height of 40 cm to accommodate users in the corridors and offices. The space behind the artificial ceiling is large enough to accommodate trays for laying wires for a variety of uses. Nine working rooms, designed to accommodate users, are positioned on the second floor of the building in accordance with the plan.

The list summarizes the area of these properties:

1) The core network (Core layer definition protocol) is made up of high-performance devices that are designed to provide quick transit.

2) The application security policy, QoS, aggregation, and routing are all provided by the distribution layer (DLP).

3) Access-layer definition protocol, usually L2 candles, end-device destination-connection, traffic marking for QoS, protection against network rings (STP detection protocol) and broadcast storms, and lighting PoE devices the D-Link DES-1100-26 and DGS-1100-05 switches will be used as access devices (Access definition protocol).

Switches on the DES-1100-26 and DGS-1100-05 are asw1. asw3, and asw4 (Protocol for determining asw - Access switch). From the primary schema to the interface name, the entire network must be properly documented.

A VLAN list and an IP tending to design are set up on the organization. Each gathering will be given its own VLAN. A devoted VLAN for gadget the board will likewise be executed. D-Link DIR 651 switch, D-Link DES-1100-10P, DES-1100-26, and DGS-1100-05 switches were picked for the organization. The table tells the best way to associate hardware by port. DIR 651 switch from D-Link. The switch has a plenty of wi-fi interface highlights.

Furthermore, the device incorporates a Wi-Fi network power button. A 4-port switch is included in the router for connecting computers using «Ethernet» adapters. D-Link DES-1100-10P switch features 8 10/100Base-TX ports with Roe support and 2 combo ports 100/1000Base-T / SFP (Protocol specification Fig. 3.4). The DES-1100-10P switch's 8 ports support «IEEE 802.3» at standard PoE. The DES-1100-10P switch supports port mirroring, Spanning Tree, and Link Aggregation Control Protocol (LACP definition protocol). The switch includes cable diagnostics as well as Loopback Detection. The DES-1100-10P switch supports advanced management tasks such as traffic and performance.

4 OCCUPATIONAL HEALTH AND EMERGENCY SAFETY

4.1 Introduction

Occupational health or occupational safety, is a multidisciplinary field concerned with the safety, health, and well-being of workers. These terms also refer to the field's objectives.

Word related wellbeing bargains with all components of wellbeing and security within the work environment, with a solid center on essential avoidance of dangers," concurring to the World Health Organization (WHO). "A condition of add up to physical, mental, and social well-being, not as it were the nonattendance of affliction or inability," as characterized by the World Health Organization. Occupational wellbeing could be a multidisciplinary teach of medicine that centers on permitting individuals to do their occupations within the most beneficial conceivable way. It is in line with the advancement of word related wellbeing and security, which centers on anticipating harm from threats.

Given the appeal in the public eye for wellbeing and security arrangements at work dependent on solid data, word related security and wellbeing (OSH) experts should find their underlying foundations in proof-based practice. Another term is "proof informed independent direction". A functioning meaning of proof-based practice could be: proof-based practice is the utilization of proof from writing, and other proof-based sources, for exhortation and choices that favor the wellbeing, security, prosperity, and work capacity of laborers. Lastly, proof-based data should be coordinated with proficient ability and the laborers' esteems. Context oriented variables should be viewed as connected with regulation, culture, monetary, and specialized potential outcomes. Moral contemplations ought to be noticed.

Managers led their ventures how they figured fit to produce a benefit in the late nineteenth and mid-20th hundreds of years. Worker security and wellbeing were immaterial to them. In actuality, in conventional terms, absolutely no part of this made a difference. In the United States, injured specialists needed to go to court to get pay for their wounds. Workers were effectively deterred from going to court because of the significant expense of doing as such. Moreover, workers were seldom fruitful in light of the fact that, under customary law, assuming the representative knew about the perils of the gig or then again assuming that the wounds were brought about by the representative's or a colleague's carelessness, the business was not responsible.

Work environments under the locale are administered by your commonplace regulation. The regulation spots obligations on proprietors, bosses, laborers, providers, the independently employed and project workers, to build up and keep up with protected and solid working conditions. The regulation is managed by your commonplace regulation. Your authorities are liable for observing consistence.

4.2 Rights, duties and responsibilities of employers and workers during outbreak and emergencies

Maintaining an appropriate and functional workforce, as well as ensuring the continuity of emergency response and vital health services, requires protecting the health and safety of health-care employees and other emergency responders. Employers must be prepared to adapt their usual practice in consultation with workers, their representatives, and technical experts in an emergency situation such as an outbreak, chemical spill, or radiation release, where workplace risk changes rapidly, in order to achieve a reasonable balance of safety versus obligation to work.

Workers in the emergency response field, particularly health-care professionals, have a contractual obligation and a duty of care to deliver services that may expose them to infections, toxins, injuries, and diseases. Despite their duty of care, emergency response professionals may have the right, depending on the national context, scenario, and practice, to remove themselves from a work situation that they have sufficient grounds to believe poses an urgent and serious threat to their lives or health.

Employers of emergency responders have a responsibility to ensure safe working conditions as well as the resources needed to execute acceptable OSH procedures. Employers have a responsibility to:

- these personnel must be suitably trained, equipped, and protected;
- give them the ability and knowledge to execute OSH methodologies;
- give clear guidance on the working circumstances for these workers, what is expected of them, and the inherent risks of the scenario;
- give adequate psychological assistance, as well as put in place measures to promote healthy behaviors;
- offer fair compensation for the services supplied by these individuals in the form of risk premiums and insurance for them and their families, as well as disability benefits for those infected;
- collect information in a systematic manner to support ongoing monitoring and evaluation of the effectiveness of OSH programs in providing protection.

4.3 Strategies and tools for protecting occupational safety and health in emergencies and outbreaks

During scourges and crises, the administration frameworks approach gives a general structure to overseeing OSH hazards. Certain strategies, methodology, and instruments exist for the avoidance and control of OSH dangers and dangers inside this structure. These devices can be custom fitted to the flare-up or crisis circumstance within reach. The "stepping stool of controls," the ICS, and disease counteraction and control measures are totally shrouded in this segment.

The Incident Command System (ICS) is a standardized on-scene incident management approach that allows responders to adopt an integrated organizational structure that is equal to the complexity and demands of any single incident or numerous incidents, regardless of jurisdictional boundaries. By establishing a reasonable span of control, the ICS enables integrated communication and planning. An ICS splits a disaster into five controllable functions: command, operations, planning, logistics, and finance and administration.

Organization structure of the ICS. The minimum ICS should consist of the following and can be expanded according to requirements:

- The Public Information Officer, Safety Officer, and Liaison Officer make up the command staff. They are directly responsible to the Incident Commander.
- The organizational level with functional responsibility for the key segments of incident management (operations, planning, logistics, finance/administration) is represented by sections. The section level is located between the branch and the Incident Commander in terms of organizational structure.
- Each sector is made up of smaller and smaller organizational units, such as a branch, division, group, unit, task force, strike force, and finally a single resource. A single resource is a single piece of equipment and its staff complement, or a pre-established crew or team of people with a designated work supervisor that can be deployed to respond to an incident.
- The ICS is created by identifying the primary tasks or functions that must be performed in order to respond to incidents efficiently. The demand for an organizational manager has grown as occurrences have become more complicated, challenging, and costly. The Incident Commander handles the organization, not the incident, in the ICS, especially in larger incidents.

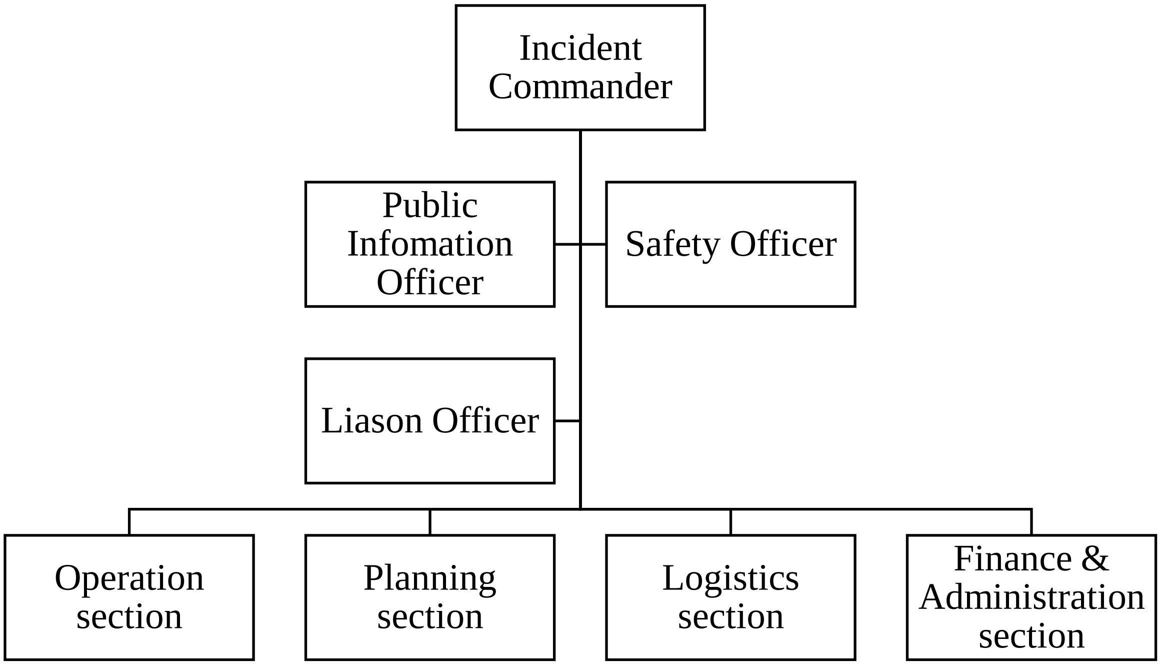


Figure 4.1 – Structure of Incident Command System

Roles and responsibilities:

- Command staffs are tasked with carrying out the staff responsibilities required to assist the Incident Commander. Interagency liaison, incident management, safety, and public communication are among these functions. Command staff jobs are created to delegate responsibility for critical operations that are not clearly listed in the general staff functions. In addition to those as required and assigned by the Incident Commander, these posts may include the Public Information Officer, Safety Officer, and Liaison Officer.
- The general staff is in charge of the ICS's operational aspects. The operations, planning, logistics, and finance/administration sectors are often part of the general staff.

The key responsibilities of the safety/OSH officer include:

- hazardous conditions must be identified and mitigated;
- guaranteeing that security messages are imparted and briefings are given;
- using emergency powers to halt and prevent dangerous activity;

- safety consequences are reviewed in the Incident Action Plan;
- appointing qualified specialists to assess unique threats.

4.4 Occupational safety and health controls

To manage the health and safety concerns posed by diverse hazards, strategies for both prevention and mitigation must be in place. The hierarchy of controls in occupational safety and health refers to the desired order of selecting control measures, from the most effective to the least effective. The basic principle is that it is always preferable to attempt to eliminate the hazard first. Where this is not possible, the hazard should be confined first at the source, then along the path, and finally at the person. Because each environment is unique, a workplace evaluation is required to identify hazards and propose management strategies.

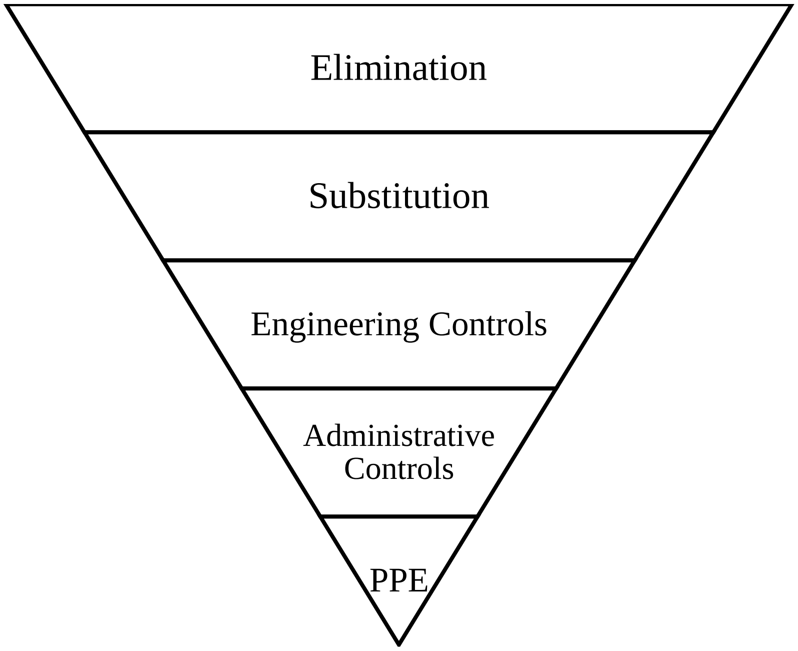


Figure 4.2 – Hierarchy of occupational safety and health controls

Where:

- Elimination; Physically remove the hazard;
- Substitution; Replace the hazard;
- Engineering Controls; Isolate people from the hazard;
- Administrative Controls; Change the way people work;
- PPE (Personal Protective Equipment); Protect the worker with personal protective equipment.

4.5 Conclusion of the chapter 4

Occupational safety and health (OSH), sometimes known as occupational health or occupational safety, is a multidisciplinary area that is concerned with worker safety, health, and well-being. Occupational health is a multidisciplinary branch of medicine that focuses on enabling people to perform their jobs in the most beneficial way possible. It is consistent with the advancement of online safety and security, which focuses on preventing harm from dangers.

Finally, evidence-based facts should be coordinated with professional ability and laborers' esteems. Contextual elements should be considered in relation to regulatory, cultural, monetary, and specialized potential outcomes. In reality, in traditional terms, none of this made a difference.

Places of work under the authority of the area are protected under the law. Maintaining an appropriate and functional workforce, as well as guaranteeing the continuity of emergency response and important health services, necessitates the protection of health-care professionals and other emergency responders' health and safety. Workers in the emergency response area, particularly health-care professionals, are contractually obligated and have a duty of care to provide services that may expose them to infections, poisons, injuries, and diseases. Employers of emergency responders are responsible for providing safe working conditions as well as the resources necessary to carry out approved OSH practices. The administration frameworks technique provides a fundamental structure for supervising OSH dangers during scourges and crises. These gadgets can be tailored to the specific flare-up or crisis situation at hand. The Incident Command System (ICS) is a standardized on-scene incident management approach that enables responders to adopt an integrated organizational structure that is capable of handling the complexity and demands of any single incident or a series of incidents, regardless of jurisdictional boundaries. The ICS provides integrated communication and planning by establishing a suitable span of control.

The following should be included in the minimal ICS and can be expanded if needed:

- The command staff consists of the Public Information Officer, the Safety Officer, and the Liaison Officer.
- Sections represent the organizational level with functional responsibility for the essential segments of incident management (operations, planning, logistics, finance/administration). In terms of organizational structure, the section level is placed between the branch and the Incident Commander.
- Each sector is composed of progressively smaller organizational units, such as a branch, division, group, unit, task force, strike force, and, lastly, a single resource. The requirement for an organizational manager has increased as events have become more sophisticated, difficult, and expensive etc.

The safety/OSH officer's main responsibilities are as follows: To deal with the health and safety risks caused by various hazards, preventative and mitigation techniques must be in place. The core premise is that attempting to eliminate the hazard first is always preferable.

CONCLUSION

The thesis describes the stages of local computer network design for the trading company LLC "Citrus." The organization currently uses a LAN, which has many issues and needs to be modernized. An improved structure of the organization's network is proposed, taking into account the customer's requirements in the work. Compilation of a plan for installing network connections and network location equipment. There are several types of users in the organization, including accounting, the economic department, the sales department, other users, and the server.

The thesis includes documentation such as a network IP addressing plan, a VLAN list, and a network device list. Estimated project development cost was provided. So, the total cost of the proposed project solution for modernization of the organization's computer network, excluding the cost of purchasing and installing network software provision and installation work, was UAH 21,598.20.

The enterprise network is modeled in the network by the work Cisco Packet Tracer emulators 5.3.2. Network testing has revealed the fidelity settings that have been made as well as the network performance.

As a general conclusion to the thesis, it should be noted that the hierarchical network model proposed in the project has the following advantages over the organization's current "flat network":

- network organization is made easier to comprehend;
- the concept implies modularity, which means it's simple to add capacity where it's needed;
- it's a lot easier to locate and isolate the issue this way;
- improved fault tolerance due to device and/or connection duplication;
- functions are distributed across devices to ensure network performance.

REFERENCES

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

2. Коломоец Г.П. Organization of computer networks: educational allowance. Zaporozhye: KPU, 2012. -- 156 p.

3. Таненбаум Э., Weatherall D. Computer networks. 5th ed. - SPb.: Peter, 2012. – 960 p.: ill.

4. Смирнова Е.В. Пролетарский А.В., И.В. Баскаков, Р.А. Федотов Construction of switched computer networks: textbook / E.V. Smirnova and others - M.: National Open University "INTUIT": BINOMIAL. Knowledge Laboratory, 2011. - 367 p.: ill.

5. Л. Куинн, Р. Рассел. Fast «Ethernet». - BHV-Kiev, 1998. -- 125 p.

6. Фоминов О.С. Fast «Ethernet» standards and applications // Networks. - 1995.– No. 9.

7. Open standard IEEE 802.1Q [Electronic resource]. Mode access: http://xgu.ru/wiki/802.1Q

8. Official site of Cisco Systems. Cisco Packet Tracer Software [electronic resource]. http://www.cisco.com/web/learning/netacad / course catalog / PacketTracer.html.

9. Джеймс Бони. Cisco IOS Guide. - SPb.: Peter, M: Publishing house "Russian edition", 2008. - 784 p.: ill.

10. Виджей Боллапрагада, Кэртис Мэрфи, Расс Уайт. Structure.

11. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі [навчальний посібник] / А.Г.Микитишин, М.М. Митник, П.Д. Стухляк, В.В.Пасічник. – Львів: «Магнолія 2006», 2013. – 256 с.

12. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 2 [навчальний посібник] / А.Г.Микитишин, М.М. Митник, П.Д. Стухляк, В.В.Пасічник. – Львів: «Магнолія 2006», 2013. – 328 с.

13. Operating system Cisco IOS. - M.: Publishing House "Williams", 2002. – 208 p.

14. Одом Уэнделл. Official Guide Cisco CCNA ICND2 200-11: routing and switching - M.: Publishing house "Вильямс", 2015.- 316

15. Джеймс Ф. Куроуз, Кит В. Росс. System Handbook administrator - M.: Eksmo Publishing House, 2016. - 512 p.

16. А. Сергеев. Основы локальных компьютерных сетей. – Лань, 2016. – 184 с.

17. А. Робачевский. Интернет изнутри. Экосистема глобальной сети 2-е издание. - Альпина Паблишер, 2017. – 224 с.

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

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

20. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach / The Morgan Kaufman series in Networking – 1999. – 776 p.

21. WWW Consortium (W3C) Official Page. (http://www.w3c.org/)

22. Cascio, W.F. (1986). Managing Human Resources Productivity, Quality of Life, Profit: New York: MC Graw-Hill.

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

24. Forestalling slips, outings, and falls among medical services work force. Public Institute for Occupational Safety and Health, Atlanta (GA), 2010.

25. Episode Command System. Washington (DC): Federal Emergency ManagementAgency;2008(https://training.fema.gov/emiweb/is/icsresource/resources/ reviewmaterials.pdf, accessed 22 November 2021).

26. Convention 155: Occupational Safety and Health, as well as the Working Environment (Occupational Safety and Health Convention). The International Labor Conference held its sixty-seventh session in Geneva in 1981. International Labor Organization, Geneva, 1981.

27. OSH management system: a tool for continuous improvement Geneva: International Labor Organization, 2011.

28. Encyclopedia. (2009). Workplace health and safety Encyclopedia Britannica 2009 Student and Home Edition is available at http: www. (Accessed March 20, 2011).

29. Cambridge University Press, 2008, 3rd edition, Cambridge Advanced school dictionary.

30. Prevent, protect, and provide when it comes to health care attacks. In an emergency, report on attacks on health care. World Health Organization, Geneva, 2016.

ANNEXES

Appendix A

The Building Plan

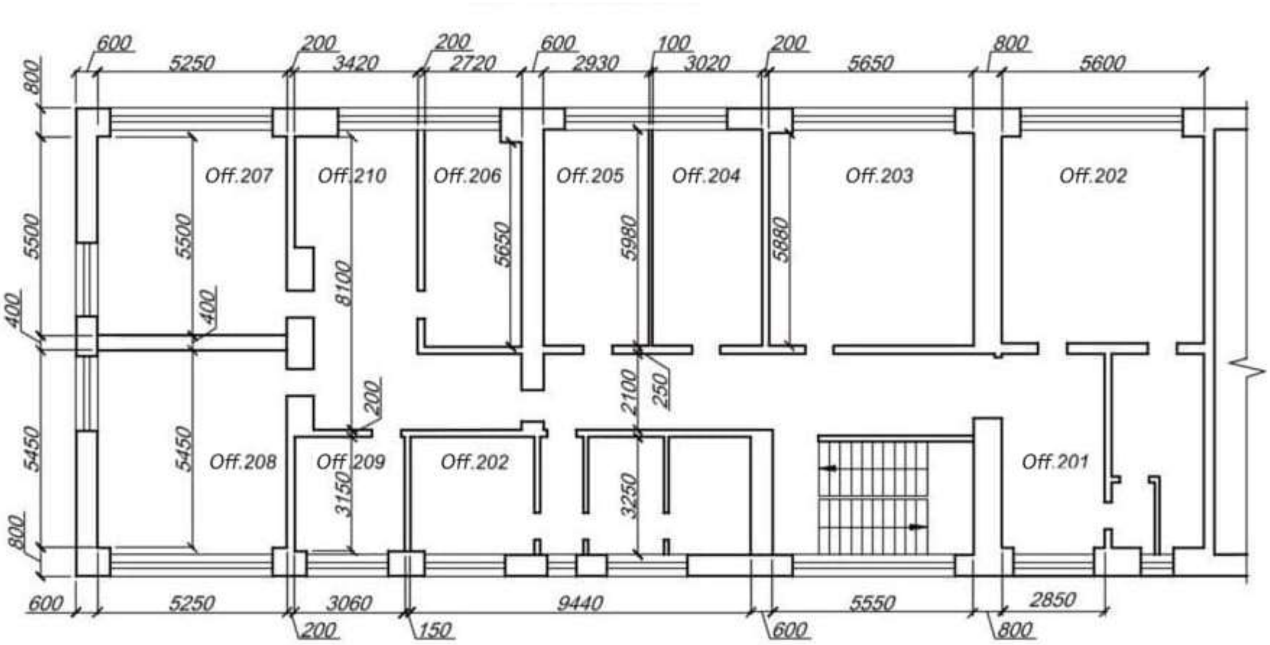


Figure A.1 – Plan of the Second Floor

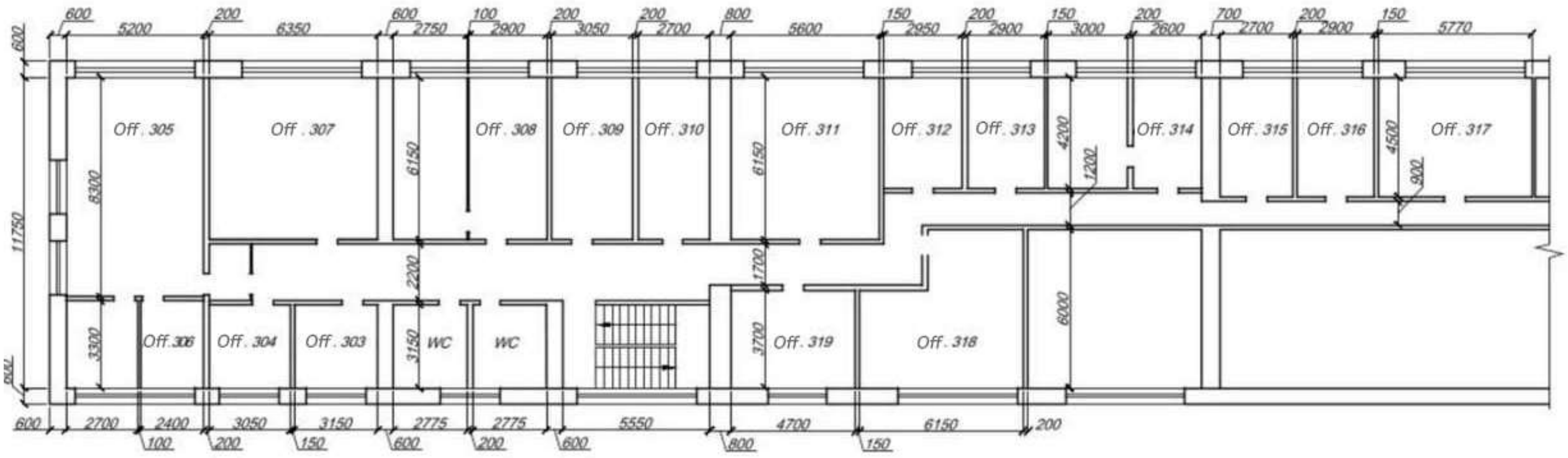


Figure A.2 – Plan of the Third Floor

Appendix B

Block diagram of the current network

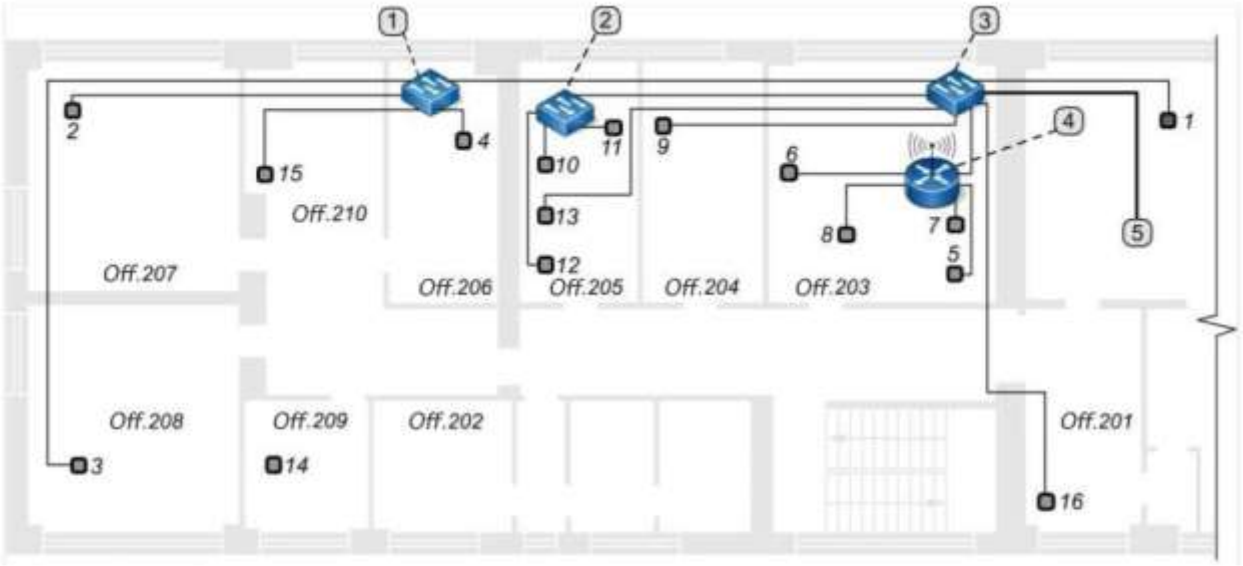


Figure B.1 – Structural diagram of the current network of the second floor

Legend:

1. Switch (16 port)
2. Switch (5 ports)
3. Switch (8 ports)
4. Wi-Fi Router (4 ports)
5. Switch on the 3rd floor

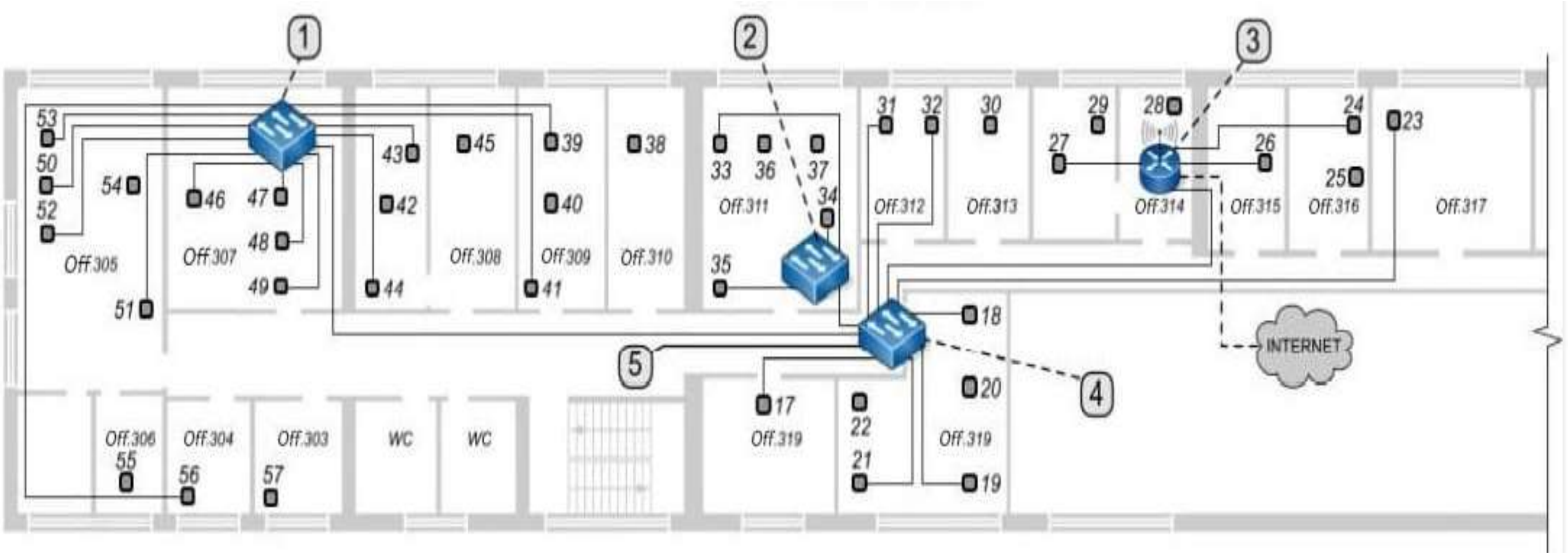


Figure B.2 – Structural diagram of the current network of the third floor

Legend:

1. Switch Asus (16 port)

2. Switch D-Link (5 ports)

3. Wi-Fi Router TP-Link (4 ports)

4. Switch D-Link (16 ports)

5. Switch to the 2nd floor

Appendix C

Structural diagram of the developed network

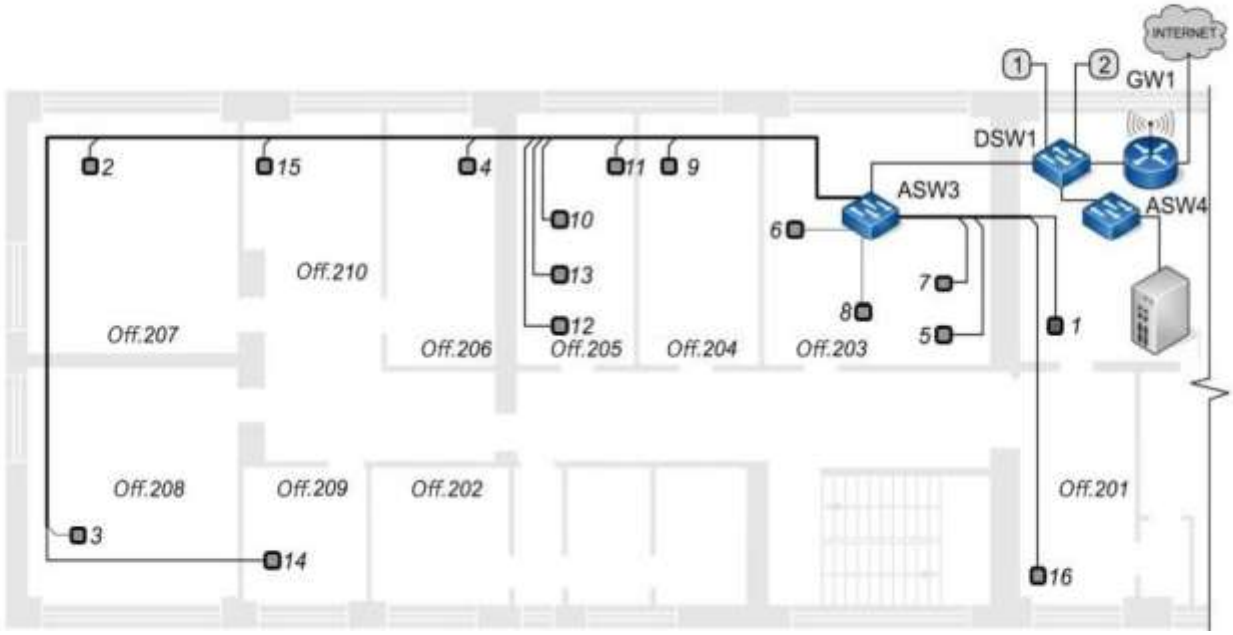


Figure C.1 – Structural diagram of the network of the second floor

Legend:

1. ASW1 on 3rd floor (24 ports)
2. ASW2 on 3rd floor (24 ports)

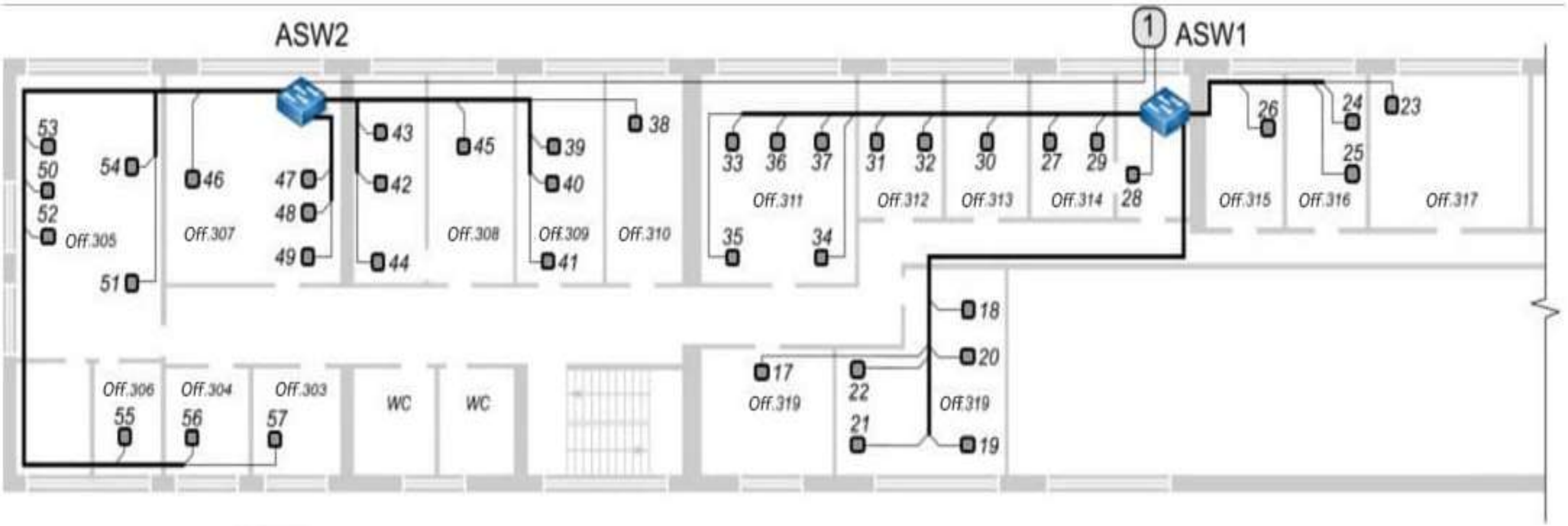


Figure C.2 – Structural diagram of the network of the third floor

Legend:

1. ASW1 on the 2nd floor