MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATIONS, ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING SYSTEMS

ADMIT TO DEFENCE
Head of the Department

____________ R. Odarchenko
"_____" ____________2022

DIPLOMA WORK

(EXPLANATORY NOTE)

BACHELOR'S DEGREE GRADUATE
BY SPECIALITY "TELECOMMUNICATIONS AND RADIO ENGINEERING"

Topic: «A multi-service communication network of a company on the basis of the existing infrastructure»

Performer:______________________________ R. Vashchenko
(signature)

Supervisor:______________________________ I. Terentieva
(signature)

N-controller:______________________________ D. Bakhtiiarov
(signature)

Kyiv 2022

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications .
Department of telecommunication and radio engineering systems .
Speciality: 172 "Telecommunications and radio engineering" .
Educational professional program: Telecommunication systems and networks .

ADMIT TO DEFENCE
Head of the Department

____________ R. Odarchenko
"_____"______ ______2022

TASK
for execution of bachelor diploma work

Vashchenko Roman
(full name)

1.Topic of diploma work: «A multi-service communication network of a company on the basis of the existing infrastructure»
approved by the order of the rector from «25» April 2022 №433/ст.

2. The term of the work: from 23.05.2022 to 17.06.2022.

3.Initial work data: multi-service network parameters, bit rate, quality, protocols, facilities

4. Explanatory note content: the modern multi-service communication networks were studied, particualry their basic concepts and architecture, in Chapter 1; Chapter 2 discusses the main features of multiservice networks construction; Chapter 3 is devoted to the construction of a multi-service communication network of a company on the basis of the existing infrastructure.

5. List of required illustrative material: figures, tables, algorithms.

6. Work schedule

№ n/p	Task	Term implementation	Performance note
1.	Develop a detailed content of the sections of the thesis graduated work	23.05.2022-25.05.2022	Done
2.	Introduction	25.05.2022	Done
3.	Analsis of modern multi-service communication network	26.05.2022-29.05.2022	Done
4.	Features of multi-service networks construction	30.05.2022-02.06.2022	Done
5.	Design of multi-service networks	03.06.2022-08.06.2022	Done
6.	Elimination of shortcomings and deferens of the graduate work	09.06.2022-17.06.2022	Done

7. Date of issue of the assignment: "25" April 2022.

Supervisor ____________________ I. Terentieva
(signature) (full name)

Accepted task for execution ____________________ R. Vashchenko
(signature) (full name)

ABSTRACT

Graduate work on the topic «A multi-service communication network of a company on the basis of the existing infrastructure». It contains p., table., Figures., sources.

KEYWORDS: MULTI-SERVICE NETWORK; NETWORK ARCHITECTURE; WIRELESS NETWORK; DATA ARCHIVING.

The object of research is the process of developing a multi-service network.

The subject of research is the corporate network of the enterprise

The purpose of the thesis is the analysis of opportunities and ways to develop a multiservice network

Research method - in the course of solving the tasks a comparative analysis of technologies, equipment and services was conducted.

Thesis materials are recommended for use in the construction of broadband access networks.

CONTENT

LIST OF ABBREVIATIONS

MSN - Multi-service network

NGN - Next Generation Net NGN

AN - Access Network

PCN - The public communications network

SCP - Service Control Point

SN - Service Node

SP- Service Provider

CP - Content Provider

OSA - Open Services Access

API - Application Programming Interface

SGSN - Serving GPRS Support Node

MSC - Mobile Switching Center

SSP - Service Switching Point

S-CSCF - Serving Call Session Control Function

MGC - Media Gateway Controller

OF - Optical fiber

RRL - Radio Relay Lines

LDAP - Lightweight Directory Access Protocol

FR - Frame Relay

MPLS - Multiprotocol Label Switching

QoS - Quality of Service

SIP - Session Initiation Protocol

VLAN - Virtual Local Area Network

INTRODUCTION

Actuality of theme. In the rest of the hour, radical changes appeared at the gallery, as if the activities of all telecommunication companies were bumped. First, there is an active promotion of new technologies for access, transport and services. In another way, the appearance of a wide range of new services and a decrease in the cost of traditional services of communication. At the link with the cim until prompted by that operation, the transfer of data is shown by arched vimogi. The security of the possibility of handy, cheap and cheap interchange and the creation of a highly efficient, protected means of data transmission is one of the most important and urgent problems in the field of telecommunications. The key to the solution of the problem is to encourage the current multi-service link

The purpose and objectives of the study. Analysis of opportunities and ways to develop a multiservice network

To achieve this goal, the following scientific problems are solved.

1. Analysis of multiservice network, its concepts, issues, architecture .
2. Research of existing technologies for multiservice networks and equipment.
3. Design of a multi-service network.

The object of study is the process of developing a multi-service network.

The subject of research is the corporate network of the enterprise

Research methods. In the course of solving the tasks a comparative analysis of technologies, equipment and services was conducted

The practical significance of the results obtained. Thesis materials are recommended for use in scientific and practical activities for planning the development of a multiservice network for the company

Approbation of the obtained results. The main provisions of the work were reported and discussed at the following conferences:

Scientific and practical conference "Problems of operation and protection of information and communication systems", Kyiv, 2022.

CHAPTER 1
ANALISIS OF MODERN MULTI-SERVICE COMMUNICATION NETWORKS

1.1. Introduction

Multi-service network (MSN) is a digital network based on the IP protocol, with the integration of various types of services - data, voice and video transmission.

The multi-service network is primarily intended for a company that is focused on intensive business development, cost optimization, business process automation, modern management methods and information security. Therefore, the growing popularity of multi-service communication networks is one of the most noticeable trends in the telecommunications services market in recent years.

Multi-service networks allow to support the following types of services:

- telephone and facsimile communication;
- dedicated digital channels with a constant transmission rate;
- transmission of video images, videoconferencing;
- a television;
- IP telephony;
- security, access control, time tracking;
- speakerphone;
- dispatching systems;
- broadband Internet access;
- interfacing of remote LANs, including those operating in different standards;
- creation of virtual corporate networks, switched and managed by the user.

The use of MCC makes it possible to simultaneously use the above services on one constructed data transmission network.

For large companies with disparate offices or industries occupying large areas, MSS allows you to increase the efficiency of information exchange by an order of magnitude, ensure data availability at any time, arrange conference calls and video conferences between offices or departments. All this reduces the response time to changes occurring in the company and ensures optimal management of all processes in real time [1].

The current stage in the development of world civilization is characterized by the transition from an industrial society to an information society, which assumes the presence of new forms of social and economic activity, which are based on the massive use of information and telecommunication technologies.

In our time, the development of infocommunication services is carried out mainly within the Internet, access to the services of which is provided through traditional communication networks. At the same time, in some cases, Internet services, due to the limited capabilities of its transport infrastructure, do not meet modern requirements for information society services. In this regard, the development of infocommunication services requires solving the problems of effective management of information resources while expanding the functionality of communication networks.

Taking into account the peculiarities of infocommunication services, promising communication networks should have the following properties:

- multi-service (independence of technologies for providing services from transport technologies);
- broadband (possibility of flexible and dynamic change of information transfer rate in a wide range);
- multimedia (ability to transmit multicomponent information (speech, data, video, audio));
- intelligence (possibility of service, call and connection control by the user or service provider);
- access invariance (possibility of organizing access to services regardless of the technology used);

- multi-operator (the possibility of participation of several operators in the process of providing services and sharing their responsibilities in accordance with their field of activity).

In addition, when forming requirements for promising multi-service networks, it is necessary to take into account the specifics of the activities of service providers. In particular, modern approaches to the regulation of interconnection services provide for the access of service providers, including those who do not have their own infrastructure, to the resources of the public network without discrimination.

Existing public communication networks with circuit switching (PCN) and packet switching (PSD) do not currently meet the above requirements. The limited capabilities of traditional networks are a deterrent to the introduction of new infocommunication services.

Multi-service networks are an independent class of networks built on the basis of the NGN concept, on the basis of which a wide range of both traditional and new services can be provided.

The definition of multi-service networks as an independent class means that their regulation should be carried out on the basis of a regulatory and technical base that takes into account the peculiarities of integrating various services and system and technical solutions within a single network[2].

1.2. Basic definitions related to the problems of multi-service communication networks

The following terms and definitions are used in the Conceptual Provisions for the Construction of Multi-service Networks:

Next generation communication network (Next Generation Net, NGN) - the concept of building communication networks that provide an unlimited range of services with flexible options for their management, personalization and creation of new services through the unification of network solutions. It involves the implementation of a universal transport network with distributed switching, the transfer of the functions of providing services to end network nodes and integration with traditional communication networks.

A multi-service network (MS) is a communication network built in accordance with the NGN concept and providing an unlimited set of services.

Multiprotocol network is a transport communication network that is part of a multi-service network that provides the transfer of various types of information using various transmission protocols.

Infocommunication network (earlier the terms “information network”, “computer network”, etc. were also used) is a technological system that includes, in addition to delivery means, also means of storing, processing and searching for information and is designed to provide users with electrical communication and access to the information they need.

The processes of integration and convergence of the telecommunications industry and informatization tools will contribute in the period up to 2015 to the transformation of telecommunication networks into infocommunication networks.

Access Network (AN) is a communication network that provides connection of the user's terminal devices to the terminal node of the multiprotocol network.

Traditional communication network - an existing communication network, such as the PSTN, PSTN, cable television network, and the like, originally designed to provide one type of communication service.

Infocommunication service (information society service) is a communication service that involves automated processing, storage or provision of information upon request using computer technology, both at the incoming and outgoing ends of the connection.

The unified telecommunication network consists of networks of the following categories:

- public communication network;
- dedicated communication networks;
- technological communication networks;
- special purpose networks.

The public communications network (PCN) is designed to provide telecommunication services to any user. The UE communication network includes networks with geographical (ABC) and non-geographic (DEF) numbering systems. The non-geographic numbering system is used in technological and special networks. The UE communication network is a complex of interacting communication networks, including communication networks for the distribution of television and radio broadcasting programs.

Dedicated, technological, as well as special-purpose communication networks form a group of restricted networks (RNG), since the contingent of their users is limited to corporate clients.

Dedicated communication networks are networks designed to provide services to a limited number of users. Such networks can interact with each other, but they are not connected to the public networks of the ESE, as well as to the public communication networks of foreign states. A dedicated network can be connected to the public network of the ESE with transfer to the category of a public network if it meets its requirements.

Technological communication networks are designed to ensure the production activities of organizations and process control. If there are free resources, these network resources can be connected to the ESE public network with transfer to the category of public networks and used to provide paid services to any user.

Special purpose communication networks are designed to meet the needs of public administration, defense, security and law enforcement. Such networks cannot be used for the provision of paid communications services, unless otherwise provided by law.

It should be noted that the above categories of networks differ from those that were used in the ARIA on the basis of the Law “On Communications” of 1995. Recall that the ARIA included the OP communication network, departmental communication networks and special-purpose communication networks. Thus, a new category of communication networks appeared - dedicated networks, and departmental communication networks were called technological.

On a functional basis, ESE networks are divided into access networks and transport networks.

The transport part is that part of the communication network that performs the functions of transferring (transporting) message flows from their sources from one access network to message recipients of another access network by distributing these flows between access networks.

The access network of a communication network is that part of it that connects the source (receiver) of messages with the access node, which is the boundary between the access network and the transport network.

According to the type of connected subscriber terminals, the ESE networks are divided into:

- fixed communication networks providing connection of stationary subscriber terminals;
- mobile communication networks providing connection of mobile (transportable or portable) subscriber terminals.

Networks are traditionally divided into primary and secondary according to the way channels are organized.

The primary network is a collection of channels and transmission paths formed by the equipment of nodes and transmission lines (or physical circuits) connecting these nodes. The primary network provides transmission channels (physical circuits) to secondary networks to form communication channels.

The secondary network is a set of communication channels formed on the basis of the primary network by switching and routing in switching nodes and organizing communication between user subscriber devices.

According to the territorial division, the networks are divided into:

- the backbone network is a network that connects the nodes of the centers of subjects and the nodes of the centers. The backbone network ensures the transit of message flows between zonal networks and the connectivity of the ESE, is a strategically important component of the ESE;

- zonal (or regional) networks are communication networks formed within the territory of one or several subjects (regions);
- local networks are communication networks formed within an administrative or otherwise defined territory and not related to regional communication networks. Local networks are divided into urban and rural;
- international network is a public network connected to communication networks of foreign countries.

According to the numbering codes, networks are divided into two classes:

- ABC code networks are fixed communication networks covering the territory of the 8-million ABC numbering zone;
- DEF code networks are mobile networks that have been allocated a DEF code.

According to the organizational and technical construction, the backbone networks of the ESE are divided into two classes:

- backbone networks of class I - networks that meet all the organizational and technical requirements of the ESE in terms of ensuring the stability and survivability of the network, protection from information threats and the impact of destabilizing factors;
- backbone networks of class II - networks that do not fully meet these requirements.

According to the number of telecommunication services, networks are:

- monoservice, intended for the organization of one telecommunication service (for example, broadcasting);
- multi-service, designed to organize two or more telecommunication services (for example, telephone, facsimile and several multimedia services).

According to the types of switching, secondary networks are divided into:

- non-switched networks;
- switched networks (with circuit, message, packet switching).

By the nature of the propagation medium, networks are divided into wired, radio and mixed. In turn, radio networks are divided into satellite and terrestrial.

Public networks differ in the volume of the served territory:

• a network of a telecom operator that occupies a significant position (has more than 25% of the installed switching capacity or passes more than 25% of the traffic);

• networks of other operators.

Bearer service is a communication service that transparently transfers user information between network terminations without any analysis or processing of its content.

Service Control Point (SCP) is a specialized communication network node that manages the provision of services in accordance with the concept of an intelligent communication network and belongs to the communication network operator.

Service Node (SN) is a specialized communication network node that provides infocommunication services and belongs to the service provider.

Service Provider (SP) is an individual entrepreneur or legal entity that provides an infocommunication communication service and does not have its own communication infrastructure.

Content Provider (CP) - an individual entrepreneur or legal entity that provides information to a service provider for its distribution or provision to users over the network of a telecom operator[3].

1.3. The concept of network multi-service

A multi-service network is a single network capable of transmitting voice, video, and data. The main stimulus for the emergence and development of multi-service networks is the desire to reduce the cost of ownership, support complex, rich multimedia applications and expand the functionality of network equipment.

The concept of multi-service contains several aspects related to different aspects of building a network.

First, the convergence of network load, which determines the transmission of various types of traffic within a single data presentation format. For example, at present, audio and video traffic is mainly transmitted over circuit-switched networks, while data is transmitted over packet-switched networks. Network load convergence is driving the trend towards using packet-switched networks for the transmission of both audio and video streams and the networks themselves. However, this does not negate the requirement of traffic differentiation in accordance with the quality of service provided.

Secondly, protocol convergence, which determines the transition from many existing network protocols to a common one (usually IP). While existing networks are designed to handle multiple protocols such as IP, IPX, AppleTalk, and a single data type, multi-service networks focus on a single protocol and different services required to support different types of traffic.

Thirdly, physical convergence, which determines the transmission of various types of traffic within a single network infrastructure. Both multimedia and voice traffic can be transmitted using the same equipment, subject to different bandwidth, delay and jitter requirements. Resource reservation, priority queuing and quality of service (QoS) protocols make it possible to differentiate the services provided for different types of traffic.

Fourth, the convergence of devices, which determines the trend of building an architecture of network devices capable of supporting heterogeneous traffic within a single system. For example, the switch supports Ethernet packet switching, IP routing, and ATM connections. Network devices can process data transmitted in accordance with a common network protocol (eg IP) and having different service requirements (eg bandwidth guarantees, latency, etc.). In addition, devices can support both Web-based applications and packet telephony.

Fifth, application convergence, which defines the integration of various functions within a single software tool. For example, a Web browser allows you to combine multimedia data such as audio, video, high-resolution graphics, etc. within one page.

Sixth, the convergence of technologies expresses the desire to create a single common technological base for building communication networks that can meet the requirements of both regional communication networks and local computer networks.

Such a base already exists: for example, an asynchronous transmission system (ATM) can be used to build both regional and local computer networks.

Seventh, organizational convergence, which involves the centralization of network, telecommunications, and information services under the control of top managers, for example, in the person of the vice president. This provides the necessary organizational prerequisites for integrating voice, video and data in a single network.

All of these aspects define different aspects of the problem of building multi-service networks capable of transmitting various types of traffic both in the peripheral part of the network and in its core[4].

1.4. Multi-service network architecture

The complexity of creating a multi-service network lies in the fact that fixed, mobile and Internet networks are built according to different standards and use individual software, which hinders the development of the services market.

The main task of the telecommunications community is to create such a network architecture that the service delivery software does not depend on the type of network or information delivery technology. To build a multi-service network, the following tools are required:

- transport channels and protocols capable of supporting the delivery of information of any type (voice, video, data);
- access equipment to such a network;
- various terminal devices.

It is required to combine the existing networks of different operators (traditional PCN, mobile networks and IP networks) into a single network. This can also be called the convergence of existing networks belonging to different operators and technologies, which is a common solution to the problem.

Today, there are still no technologies that would fully satisfy the needs of a promising multi-service network. However, technological solutions that can become its basis already exist, that is, it is possible to build a prototype of a multi-service network.

At present, the most widespread is the four-level architecture of a multi-service network:

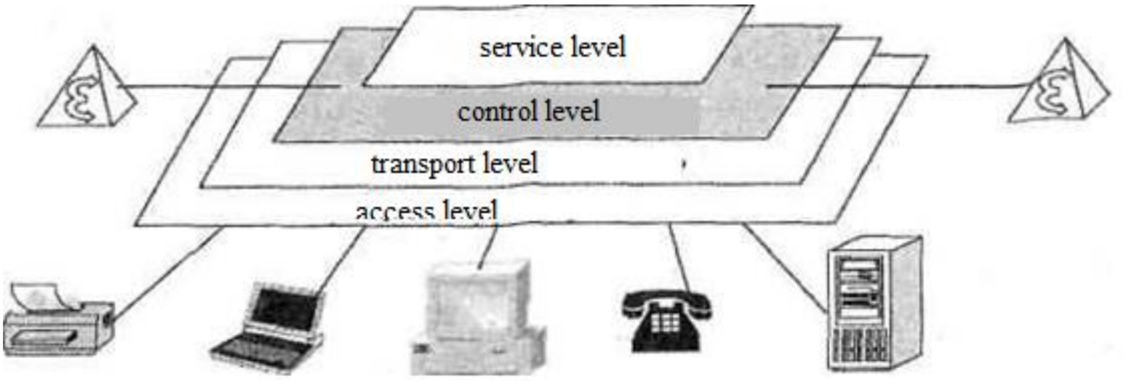


Fig. 1.1. Next generation network architecture

- service management level;
- switching control level;
- transport layer;
- access level.

The service control layer contains the functions of managing the logic of services and applications and is a distributed computing environment that provides:

- provision of infocommunication services;
- service management;
- creation and implementation of new services;
- interaction of various services.

This layer allows you to implement the specifics of services and apply the same service logic program, regardless of the type of transport network and access method. The presence of this layer also allows the introduction of any new services on the telecommunication network without interfering with the functioning of other layers.

The control level may include many independent subsystems ("service networks") based on various technologies, having their own subscribers and using their own internal addressing systems.

Telecom operators require mechanisms that allow them to quickly and flexibly deploy, as well as change services depending on the individual needs of users.

Such mechanisms are provided by the open service architecture OSA (Open Services Access) - the main concept for the future development of telecommunication networks in terms of the introduction and provision of new additional services.

When building systems based on OSA, the following key points should be present:

- an open environment for creating services;

- open service management platform.

Over the years, various organizations have proposed several options for implementing the OSA concept, until in 1998 the Parlay Group consortium was formed, which is developing specifications for an open API (Application Programming Interface), which allows you to manage network resources and access the network ¬how information.

The Parlay architecture is one of the practical implementations of the OSA concept.

As shown in Figure 1.2, different communication networks have different network elements, in particular:

— second generation mobile telecommunication networks include SGSN (Serving GPRS Support Node) and MSC (Mobile Switching Center);

— the public telephone network includes SSP (Service Switching Point) service switch in the PSTN;

— the third generation mobile telecommunication network includes S-CSCF (Serving Call Session Control Function);

— departmental automatic telephone exchanges.

Each of these elements goes to the gateway (Gateway) according to its own protocol, and the task of the gateway according to the OSA / Parlay concept is to reduce all protocols to single APIs. Applications can then be written without taking into account the peculiarities of the underlying networks, and one should only strictly adhere to the APIs.

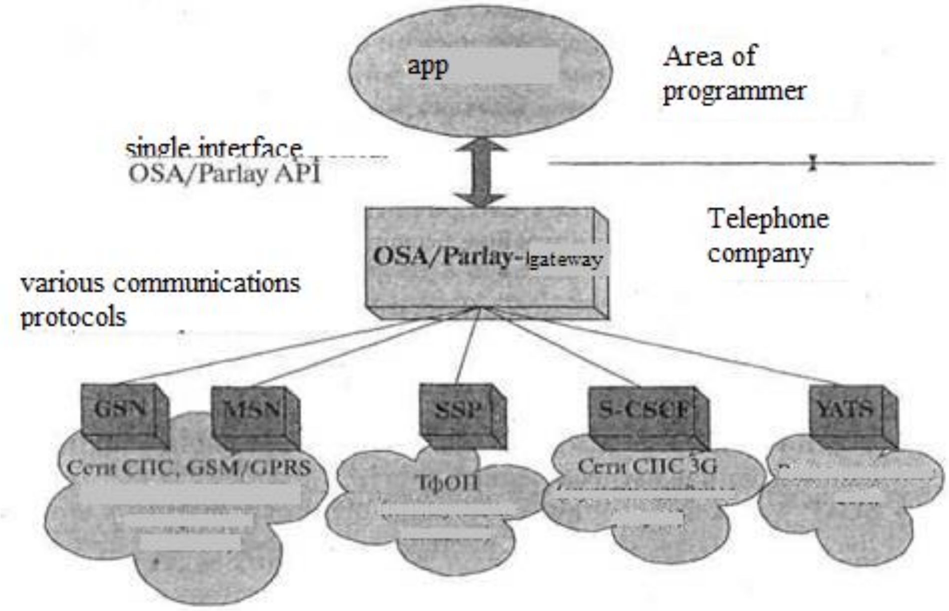


Fig. 1.2. Parlay architecture

It turned out that the concept of Parlay is too complicated for the massive involvement of third-party programmers. It turned out that only 20% of the capabilities of the Parlay gateway are required to provide 80% of the services. Consequently, for the vast majority of programmers, the requirement to master the entire set of Parlay interfaces is excessively high. As the diversity of network capabilities decreases, the number of application developers is growing, which is essential for tapping into the lucrative application market.

Applications can be written in C++, Java, Visual Basic, PHP, etc. The main programming language for developing Parlay X applications is XML. The most commonly used vehicles are:

- CORBA - a universal object-oriented protocol for the interaction of distributed systems;

- SOAP - a simplified protocol for communicating distributed objects, based on the XML language, used in combination with the HTTP protocol.

The most promising object technology today is SOAP/XML, as it is the most versatile, based on international standards and has extensive support from various software vendors. This technology is most often used to create web services and to ensure their interaction with the client process.

The task of the switching control layer is to process signaling information, call routing, and flow control. This layer supports the control logic required to process and route traffic.

The connection establishment function is implemented at the element level of the core network under the external control of the software switch equipment (Softswitch). The exceptions are PBXs with the functions of a gateway controller (MGC - Media Gateway Controller), which themselves perform switching at the element level of the transport network.

Softswitch must implement:

- processing of all types of signaling used in its domain;

- storage and management of subscriber data of users connected to its domain directly or through the equipment of access gateways;

- interaction with application servers to provide an extended list of services to network users.

Softswitch will be discussed in more detail in the next lectures.

The task of the transport layer is switching and transparent transmission of user information.

In the SSP, operators will have the opportunity to increase the volume of services, which in turn will lead to an increase in the requirements for the performance and capacity of transport layer networks. The main requirements for such networks are:

- high reliability of equipment nodes;

- support for traffic management functions;

- good scalability.

Reliability comes to the fore, since SSNs must ensure the transmission of heterogeneous traffic, including delay-sensitive traffic that was previously transmitted using classical time division transmission systems of the SDH or PDH hierarchies.

In some cases, the transport networks being created will replace part of the infrastructure of existing traditional transmission networks. Of course, they must comply with the requirements of technical regulations for the replaced network.

ITU-T defines the following transport layer capability requirements:

- support for real-time and delay-insensitive connections;
- support for various connection models: "point-to-point", "point-to-ellipsis", "ellipsis-dot", "ellipsis-dot";
- guaranteed levels of performance, reliability, availability, scalability.

The transport layer of the SSN is considered as a layer, the constituent parts of which are the access network and the core network.

The access network is understood as a system-network infrastructure, which consists of subscriber lines, access nodes and transmission systems that connect users to the traffic aggregation point (to the SSN network or to traditional telecommunication networks).

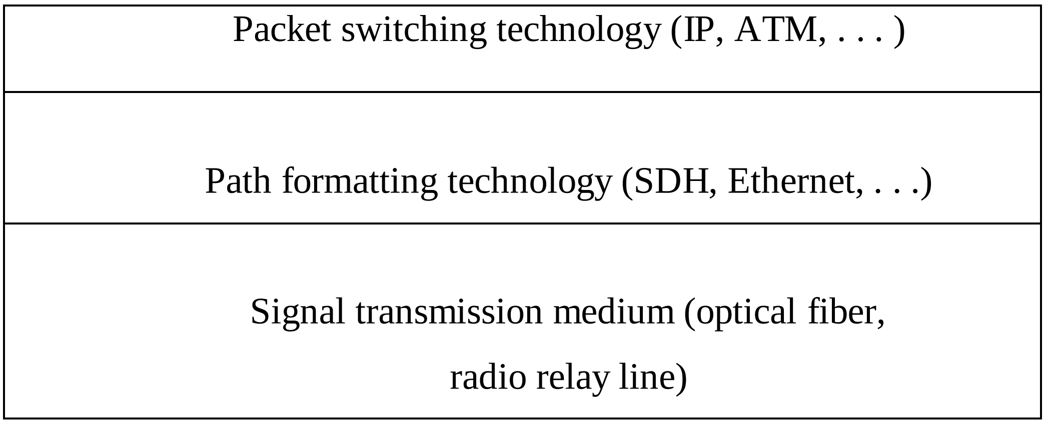
Various transmission media can be used to organize the access layer. This can be a copper pair, coaxial cable, fiber-optic cable, radio channel, satellite channels, or any combination of them.

A feature of the SSN infrastructure is the use of a universal core network based on packet switching technologies.

The core network is a universal network that implements transport and switching functions. In accordance with these functions, the core network is represented as three layers (see Figure 1.3):

- packet switching technology;
- path formation technologies;
- signal transmission medium.

The lower level of the model is the signal transmission medium. This level should be implemented on cables with optical fibers (OF) or on digital radio relay lines (RRL).



Packet switching technology (IP, ATM, . . .)

Path formatting technology (SDH, Ethernet, . . .)

Signal transmission medium (optical fiber,
radio relay line)

Fig. 1.3. Core network model

Access levels include:

- gateways;

- access network (telecommunication network that provides connection of the user's end terminal devices to the end node of the transport network);

- terminal subscriber equipment.

The technologies for building access networks include:

- wireless technologies (Wi-Fi, WiMAX);

- technologies based on cable television systems (DOCSIS, DVB);

- xDSL technologies;

- fiber optic technologies (passive optical networks (PON)).

It can be noted that with the development of telecommunication technologies, it becomes more and more problematic to draw a clear line between the transport layer and the access layer. So, for example, a digital subscriber access multiplexer (DSLAM) can be assigned to both levels [5].

It can be noted that with the development of telecommunication technologies, it becomes more and more problematic to draw a clear line between the transport layer and the access layer. So, for example, a digital subscriber access multiplexer (DSLAM) can be assigned to both levels. The architecture of the telecommunication network, built in accordance with the concept of the MSN, is shown in fig. 1.4 (with some simplifications).

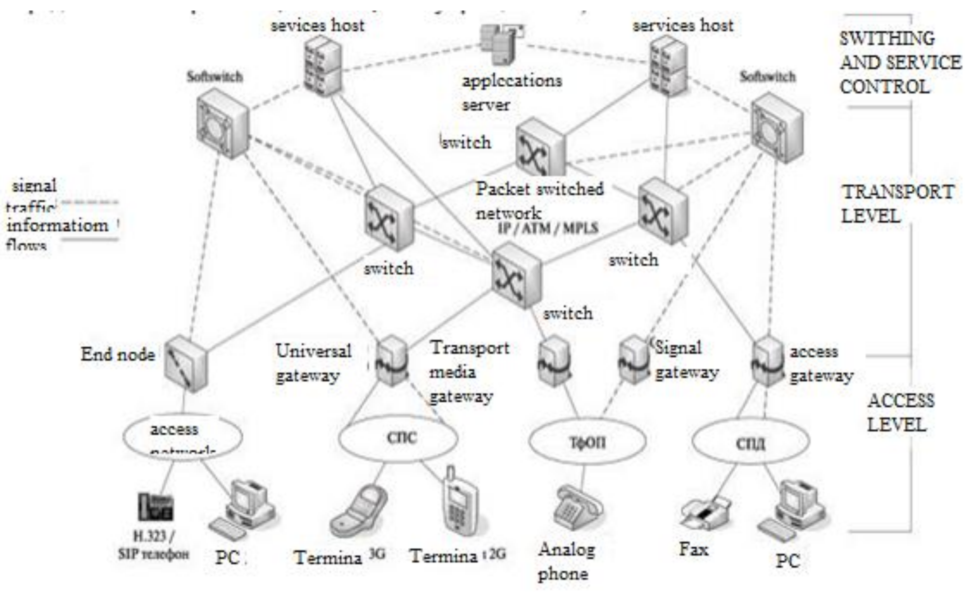


Fig. 1.4. Architecture of a multi-service communication network

Infocommunication services involve the interaction of service providers and telecom operators, which can be provided on the basis of a functional model of distributed (regional) databases implemented in accordance with ITU-T Rec. X.500. Access to databases is organized using the LDAP protocol (Lightweight Directory Access Protocol). The above databases allow solving the following tasks: • creation of subscriber directories; • automation of mutual settlements between telecom operators and service providers; • ensuring interaction between telecom operators in the process of providing intelligent communication services; • ensuring the interaction of terminals with different functionality at different ends of the connection. The above databases can also be used by service providers to organize paid information and reference services. The MSS concept relies heavily on technical solutions already developed by international standardization organizations. Thus, the interaction of servers in the process of providing services is supposed to be based on the protocols specified by IETF (MEGACO), ETSI (TIPHON), 3GPP2 Forum, etc. H.323, SIP and intelligent network approaches will be used for service management. IP/MPLS technology with the possible future use of optical switching is considered as a technological basis for building the transport layer of next generation communication networks [6].

CHAPTER 1 - CONCLUSIONS

So, a multi-service network capable of providing a single platform for voice, video and data transmission, through the use of integrated solutions, can reduce the cost of ownership, support for complex, integrated applications and network equipment.

The concept of multi-service covers many aspects of building a network, allowing you to achieve the required quality of solving user problems, the functioning of both individual parts and the network as a whole.

The architecture of a modern network consists of a core, access infrastructure and periphery (network boundary). Different decisions must be made at different levels of the network.

In building a multi-service network, there may be some stages that allow you to add all the new necessary features as your business develops. However, even today it is important to take into account the multi-service strategy when making a decision on the purchase of network equipment.

The range of the offered equipment and its capabilities make it possible already today to build complex integrated networks that can satisfy the requirements of demanding customers.

CHAPTER 2
FEATURES OF MULTI-SERVICE NETWORKS CONSTRUCTION

2.1. Technologies of multi-service networks

MPLS technology

In the mid-1990s, a multi-tier structure was considered quite suitable, in which ATM and Frame Relay (FR) networks were to be used below the IP level, and SDH / PDH or DWDM at the physical level. The use of such an architecture and with two more levels of packet transmission (on the channel using virtual channels and on the network, mainly in the datagram way) made the global network very complex and expensive. However, it was considered that these shortcomings could be ignored, as the advantages were the transmission of multimedia traffic and the provision of the required quality of service (Quality of Service, QoS).

A new word in the field of IP integration with virtual channel technologies is the technology of multi-protocol label switching. It occupies an intermediate place between the level of IP and the level of technologies such as ATM, FR or Ethernet, integrating them into a single efficient technology.

Multiprotocol Label Switching (MPLS) is a backbone network technology that significantly increases the speed of territorial network traffic. The term "multi-protocol" in the name of the technology means that MPLS technology is applied to any network layer protocol, ie, it is a kind of encapsulation protocol capable of transporting information from many other higher-level protocols of the OSI model. MPLS technology is independent of channel and network layer protocols in IP, ATM, and FR networks, and interacts with existing routing protocols, such as the RSVP resource reservation protocol or the OSPF shortest route preferred network protocol.

The position of MPLS technology relative to the seven-level OSI / ISO model is shown in Figure 2.1.

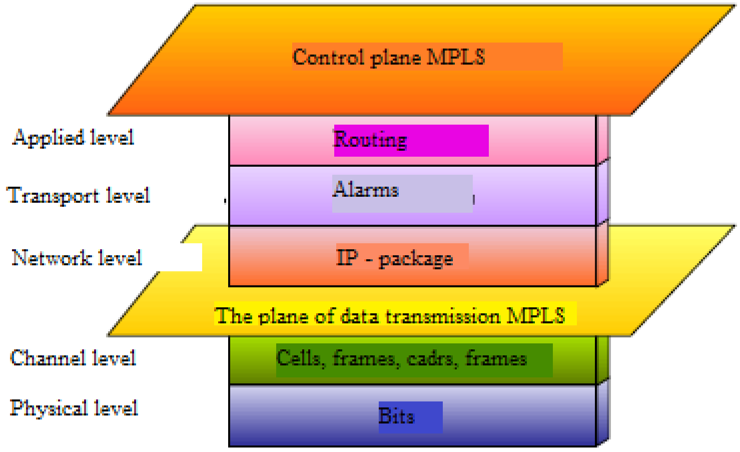


Fig. 2.1. MPLS planes

The MPLS data plane does not form a full layer, it is "wedged" in the IP, ATM or FR network between the 2nd and 3rd layers of the OSI model, while remaining independent of these levels. We can say that the ability to operate MPLS at the network and channel levels leads to the formation of the so-called layer 2.5, where, in fact, is performed by label switching.

MPLS combines the reliability and guaranteed quality of ATM service with convenient and powerful means of IP network delivery. This integration has added value to IP and ATM sharing and can be seen as a hybrid of a virtual channel network and a packet-routed network that implements the TCP / IP stack [7].

Let's take a brief look at how label-based switching technology works in RFC 2547-specific networks. Inbound IP packets are required for the EMOS model level (for example, QoS provisioning or bandwidth management). Depending on these requirements, as well as the destination of the device, IP packets are marked with special labels. Actions that require high processing power (analysis, classification and filtering) are performed only once, at the entry point. MPLS backbones - commonly referred to as Label Switch Router (LSR) or Provider router (P) - promote packet-only packets and do not parse IP packet headers. Labels are deleted at the exit point from the MPLS network.

When moving a packet over a network, the reference devices compile routing tables that associate packets and the specified route with labels. LSRs read the labels of each packet and replace them with new ones according to their routing table. The packets are then passed on. This operation is repeated during each LSR. All packets with the same labels are transmitted on one LSP. At the same time, as already mentioned, depending on the state and load of the LSP network can go on different routes [8].

Technologies for building a physical channel with your own hands

1. Ethernet - twisted pair. Up to 100 meters. Maximum per building or between adjacent buildings. Speed up to 1 Gbps (Strictly speaking, there is a 10GBASE-T standard that allows you to transfer data at a speed of 10 Gbps at the same distance).

2. WiFi. The distance depends on the implementation: it is possible to achieve operability for 40 km using powerful directional antennas. On average, up to 5 km with line of sight. The speed depends on the standard used and on the distance. It is necessary to register in the register, and at high radiation powers, to obtain permission to be included.

3. xDSL - two to four wires. The speed depends on the distance (theoretical maximum 250 Mbps, distance up to 6 km). Although there are rumors about the development of the 1Gb / s standard over two wires.

Or solutions like E1. This does not mean connecting to the Internet via xDSL, namely the link: modemmodem. Yes, such solutions exist. You can call it a bridge.

4. Radio Relay Lines. Distance up to several tens of kilometers. Speed up to 600 Mb/s. But this solution is already an operator level, since it requires a lot of approvals and measures for planning, construction, and commissioning.

5. Optical fiber. 1Gb/s (10 and 100 Gb/s solutions can be prohibitively expensive). The distance depends on many factors: from a few kilometers to hundreds. Approvals for cable laying, qualified personnel for construction and maintenance are required. For small companies, it only makes sense to connect a building not very far from the central hub. In general, of course, each case is individual and requires calculation.

In this case, everything is transparent to you - you use your own physical line, so you can pass anything through it without restrictions.

Provider technologies

1. The most real straight cable. For example, he may lend you one or two dark fibers from his optical beam. You are free to send whatever you want to it. On the part of the provider, this is not controlled in any way, it is not limited, it only provides support. For example, in the event of an accident, you will not have to look for a contractor and a welding machine, but a provider. And he is responsible for downtime. If you do not have it by mutual agreement (read, netting), then perhaps the most expensive way.

2.L2VPN. You can also let anything into the channel, but in this case, your traffic will go through the active equipment of the provider, so it may be limited, for example, in terms of speed.

This term refers to several second-level services at once:

VLAN - in one form or another, a VLAN is provided to you between branches.

Pseudo-cable (PWE3) is a Point-to-Point service where you seem to have a cable between two nodes. All frames transmitted by you are delivered unchanged to the remote point. Likewise in reverse. This is possible due to the fact that your frame arriving at the provider's router is encapsulated in a higher layer PDU, usually an MPLS packet.

VPLS (Virtual Private Network) is a simulation of a local area network. In this case, the entire provider network will be like some kind of abstract giant switch for you. Like the real one, it will store a table of MAC addresses and decide where to send the incoming frame. This is also implemented by encapsulating the frame in an MPLS packet.

3. L3VPN. In this case, the provider's network is like a large router with several interfaces. That is, the joint will occur at the network level. You configure IP addresses on your routers on both sides, but routing in the ISP's network is already a headache for the ISP. IP addresses for junction points can either be determined by you or issued by the provider - it depends on the implementation and on your agreement. It can function on the basis of GRE, IPSec or the same MPLS.

This service looks very simple from the client's point of view - both in terms of configuration and in terms of implementation - but complex - from the operator's point of view [9].

Classes of solutions in the field of OSS/BSS systems

OSS/BSS is an abbreviation of the English Operation Support System/Business Support System. This is a class of software products used by telecom operators, TV companies, energy companies and other organizations that regularly and personally interact with customers: they maintain individual accounts, monitor service consumption and regularly bill their subscribers. A telecommunications company cannot exist without the processes that OSS/BSS provides, this is the core of its business [10].

With the development of the communications industry, the services that they can provide have become a decisive factor in the competition between operators. That is why the efficiency and quality of services take on a new meaning. As a result, the functionality of telecommunications network operational support systems has expanded significantly, and a new class of IT solutions has emerged - OSS / BSS systems.

Recently, OSS / BSS solutions have become widespread in other industries, but the dominant number of implementations of systems of this class falls on telecom companies. Given the role of telecommunications networks in the business of a modern operator, it becomes clear that their efficient operation is one of the most important tasks.

Modern OSS/BSS systems contain many modules (classes) and subsystems aimed at solving various business problems. The combination of various classes with corporate information systems (CRM, HelpDesk, etc.) provides the necessary functionality to solve specific issues [11].

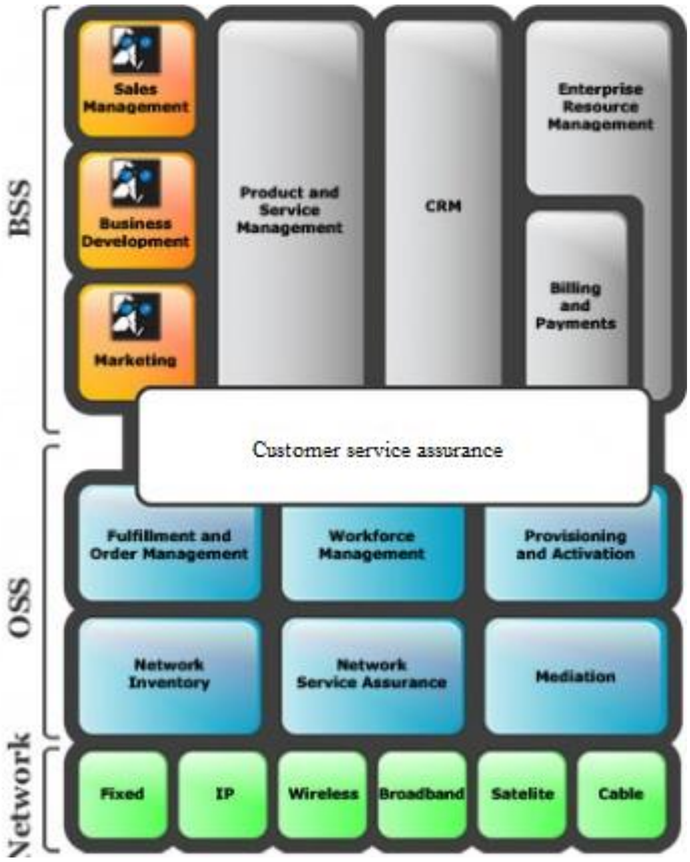

BSS
OSS
Network
Sales Management
Business Development
Marketing
Product and Service Management
CRM
Enterprise Resource Management
Billing and Payments
Customer service assurance
Fulfillment and Order Management
Workforce Management
Provisioning and Activation
Network Inventory
Network Service Assurance
Mediation
Fixed
IP
Wireless
Broadband
Satelite
Cable

Fig. 2.2. OSS / BSS system diagram

2.2. Basic types of protocols

The discipline of information exchange between various network devices in the MCC architecture is determined by a set of standard protocols, which, generally speaking, are modified to solve problems that arise from time to time. These protocols are one of the main elements of multi-service networks (the scheme of protocol interaction is shown in Fig. 2.3).

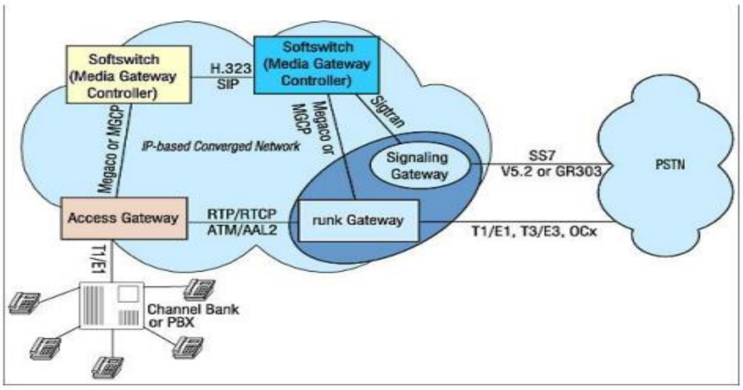


Fig. 2.3. Protocol interaction scheme

H.323 protocol. The ITU-T H.323 standard was developed to enable call setup and transmission of voice and video traffic over packet networks, particularly the Internet and intranets, which do not guarantee quality of service (QoS). It uses the Real-Time Protocol and Real-time Transport Control Protocol (RTP/RTCP) developed by the IETF, as well as standard ITU-T G.xxx codecs.

H.323 was the first implementation of VoIP technology, but under pressure from the industry, it began to lose ground to the IETF-developed SIP protocol, which proved to be simpler and better scalable. However, the ITU has improved the H.323 protocol to improve connection speed and scalability.

Session Initiation Protocol (SIP). The SIP (Session Initiation Protocol) session initiation protocol was developed by the MMUSIC (Multiparty Multimedia Session Control) group and described in RFC 2543 multi-media sessions.

The SIP protocol is designed to organize, modify and terminate multimedia conferences. At the same time, information transfer, quality of service control and other functions are assigned to different protocols included in the protocol stack, which is sometimes called by the name of the main SIP signaling protocol.

Media Gateway Control Protocol. The MGCP protocol is used to control MGs. It is designed for an architecture where all call processing logic resides outside the gateways and is controlled by external devices such as MGCs or Call Agents. 31 The MGCP call model considers MGs as a set of endpoints that can be connected to each other. Endpoints can be either physical (such as an analog telephone line or digital trunk) or virtual (data flow over a UDP/IP connection).

MEGACO/H.248. The Media Gateway Control Protocol (MEGACO) is to replace MGCP as the standard for managing MGs. MEGACO serves as a common platform for gateways, multipoint control devices and interactive voice response devices.

The connection model used by MEGACO is conceptually simpler than for the MGCP protocol. MEGACO considers MGs as a set of end devices that can be related to each other within a specific context. The terminal device is the source or destination of media streams. As with MGCP, endpoints can be either physical or virtual. A connection is established when one end device is placed in the context of another. For example, call forwarding is done by moving an endpoint from one context to another, and a video conference would be initialized by placing multiple endpoints in a common context.

The Signaling Transport protocol is SIGTRAN. is a set of protocols for transmitting signaling information over IP networks. It is the main transport component in the distributed VoIP architecture and is used in devices such as SG, MGC, Gatekeeper (gatekeeper).

In accordance with the SIGTRAN concept, while ensuring the transit of signaling messages, the messages themselves do not change, while the protocols of lower levels (1-3) are replaced by protocols from the IP world. Intermediate protocols appear between the original signaling layers and the IP stack, called adaptation protocols in SIGTRAN. Depending on the layer being replaced, these protocols perform adaptation at the 2nd, 3rd, or higher layers of the OSI model. In addition to adaptation protocols, the SIGTRAN concept uses a special Stream Control Transmission Protocol (SCTP) transport protocol to ensure reliable delivery of signaling message [12].

2.3. Multi-service network equipment

At present, the construction of multi-service networks with the integration of various services is one of the most promising areas for the development of corporate networks. The main task of multi-service networks is to ensure the coexistence and interaction of heterogeneous communication subsystems in a single transport environment, when a single infrastructure is used to transmit normal traffic (data) and real-time traffic (voice and video).

When creating a multi-service network, the following is achieved:

-Reducing the cost of communication channels;

-Reducing the cost of administration and maintenance of the network, reducing the total cost of ownership (TCO);

- Possibility of carrying out a unified administrative and technical policy in the field of information exchange;

- Increasing the competitiveness of the organization by introducing new corporate services and applications into the operating activities and, as a result, increasing the productivity of employees.

When building multi-service networks, a rich integration experience has been accumulated in creating large corporate networks, including for national corporations and government agencies with branches in all regions , united in a single network with service integration. Taking into account all types of traffic in each specific project, and taking into account the specific business requirements of the customer, the specialists of the most modern solutions that meet all the requirements for functionality, expandability, cost-effectiveness and manageability. And in many cases, the most effective enterprise infrastructure solution is a multi-service network that simplifies the deployment of new converged applications and can adapt to ever-changing business requirements through intelligent adaptability and scalability.

The multi-purpose environment allows the transfer of various information through packet switching. This allows you to significantly reduce the cost of equipment for multi-service networks, since everything is of the same type, as well as use common technologies and centralized management, which greatly simplifies the work [13].

Components of a multi-service network:

1. Teleports are a center that performs several tasks at once: managing, receiving, creating, processing and transmitting data. The modular technology on which the teleport is built makes it possible to increase the number of services used and provided over time;

2. Transport networks - provide data transmission, consist of fiber optic cables, they include input, output and data processing nodes, teleports and clusters are connected to them;

3. Clusters are groups of users that can have from 500 to 2000 subscribers located at a small distance from each other, they are all part of an interactive distribution network [14].

When creating multi-service network projects, it is recommended to use active network equipment from the world's leading manufacturers, among which are Cisco Systems and Nortel Networks. The choice of products of these manufacturers is due to the wide range of equipment offered and the support of the most modern technologies, which allows you to create complete solutions with centralized management and solve equipment compatibility problems.

An example of a multi-service network based on Cisco Systems equipment.

The company's multi-service data transmission network ensures the performance of applied corporate tasks and the uninterrupted operation of IT applications, provides intracorporate voice and video conferencing, tools for distance learning, supports an integrated video surveillance system for the security service, and automates the processing of requests from customers, partners and consumers of the company's services.

There are two types of nodes in the network - the central office and regional offices. All nodes are interconnected by a backbone using dedicated channels provided by the service provider under an SLA service level agreement. This central, linking all company facilities, backbone is based on MPLS (Multiprotocol Label Switching) technology.

The network allows you to separate and isolate the information flows of various departments of the company using MPLS VPN technology, thanks to flexible security policies. To ensure the mobility of company employees inside office buildings and to simplify user access to the corporate network when moving between departments, for negotiations, meetings, conferences, presentations and providing guest access to the Internet in each of the offices, access to network resources is possible through Cisco Aironet wireless access points based on Wi-Fi technology.

For communication between network nodes in central offices, routers of the Cisco 7500 or Cisco 7200 series are used - high-performance routers that support redundancy of component modules, power supplies and access ports, the presence of mechanisms for high availability and fault tolerance to minimize possible downtime caused by equipment or link failure connections. Cisco 7200, Cisco 3700 or Cisco 2600 series multi-service routers are used, depending on the number of employees and traffic intensity in each regional office [15].

CHAPTER 2 – CONCLUSIONS

The second chapter discusses different types of technologies. Namely: MPLS, technologies for building a physical channel yourself, provider technologies and classes of solutions in the field of OSS / BSS-systems. Their disadvantages and advantages are considered.

Different types of protocols have been studied, such as H.323 protocol, Session Initiation Protocol (SIP), Media Gateway Control Protocol, MEGACO / H.248, Signaling Transport protocol - SIGTRAN. These protocols are one of the main elements of multiservice networks.

Types of equipment for multiservice networks were also considered. When creating projects of multiservice networks, it is recommended to use active network equipment from the world's leading manufacturers, among which we can single out Cisco Systems.

CHAPTER 3
DEVELOPMENT OF A MULTI-SERVICE NETWORK BASED ON THE EXISTING INFRASTRUCTURE

3.1. Development of a multi-service network for the organization DP "Adidas-Ukraine"

3.1.1. Pre-project survey

The company has two offices located nearby and a warehouse located in another part of the city. The warehouse has one floor. Each of the office buildings has three floors.

On the ground floor of the office is the transport department. On the second floor there is: the marketing department, the advertising department and the management of the commercial service. On the third floor are located: the purchasing department and the sales department.

On the ground floor of the office building is located: administrative and economic part and accounting. On the second floor there is an operational accounting department. On the third floor are located: the financial department and the management of the executive directorate.

Table 3.1

Department name	Number of employees
Warehouse	3
Transport department	7
Marketing Department	12
Advertising Department	12
Commercial Service Manual	7

End of Table 3.1

Purchasing department	11
Sales Department	11
Administrative and economic part	14
Accounting	12
Department of Operational Accounting	21
Financial department	10
Executive Directorate	4

Each department has information that should be accessible only to employees of the department, to which strangers or employees of other departments do not have the right to access. There is also information that all departments should have access to.

3.1.2. Selecting the topology of a multi-service network

All computers in the local network are connected by communication lines. The geometric arrangement of communication lines to network nodes and the physical connection of nodes to the network is called the physical topology. Depending on the topology, networks are distinguished: bus, ring, star, hierarchical and arbitrary structures.

A mixed star-star network topology was chosen, according to how much this topology, in my opinion, is the most reliable and economical price-reliability ratio topology of the canopy of the Adidas-Ukraine offices

If one of the workstations fails, then this is not how it is not displayed on the work of the rest of the network. If one of the floor-by-floor switches fails, then one floor will remain without a network, and all other floors will work normally.

The disadvantages of this topology: a large number of workstations are connected to the switches; the use of expensive high-quality equipment allows you to connect up to 48 workstations to achieve your goals in reliability and transmission speed.

3.1.3. Choice of multi-service network technology

LAN architectures or technologies can be divided into two generations. The first generation includes architectures that provide low and medium data transfer rates: Ethernet 10 Mbps, Token Ring (16 Mbps) and ARC net (2.5 Mbps).

To transfer information, these technologies use cables with a copper core. The second generation of technologies includes more modern high-speed architectures: FDDI (100 Mbps), ATM (155 Mbps) and upgraded versions of the first generation architectures (Ethernet): Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps). With).

Improved versions of the first generation architectures were designed both for the use of cables with copper conductors and for fiber optic data transmission lines.

New technologies such as FDDI and ATM are focused on the use of fiber optic data transmission lines and can be used to simultaneously transmit various types of information (video, voice and data).

Ethernet is a multiple access method with bearer listening and collision resolution. Before starting a transmission, each workstation determines whether the channel is free or busy. If the channel is free, the station starts transmitting information. In reality, conflicts lead to a decrease in network performance only when more than 80–100 stations are operating.

The standard defines four basic media types.

- 10BASE5 (thick coaxial cable);
- 10BASE2 (thin coaxial cable);
- 10BASE-T (twisted pair);
- 10BASE-F (fiber optic cable).

Fast Ethernet - the IEEE 802.3 u specification, officially adopted on October 26, 1995, defines the link layer protocol standards for networks operating using both fiber-optic copper and copper cable at a speed of 100 Mb / s. The basic topology of a Fast Ethernet network is a passive star.

The standard defines three media types for Fast Ethernet:

- 100BASE-T4 (quad twisted pair category 3);
- 100BASE-TX (twin twisted-pair category 5);
- 100BASE-FX (fiber optic cable).

ARCNET is a local area network standard developed in 1977 by Datapoint Corporation. This network is based on the idea of a token bus and can allow multiple topologies at 2.5Mbps: bus, ring, or star. The network is built around passive and active repeaters. Active repeaters (usually 8-channel) can be connected to each other, to passive repeaters and end workstations. The length of such connections, performed by 93-ohm coaxial cable (RG-62, BNC connectors), can be up to 600 m. Use of twisted pairs (RS485) or optical fiber is allowed.

The Token Ring network is the second most famous LAN after Ethernet networks. This is a ring topology network, with a marker access method that takes into account the priorities of different members of the network. It was developed by IBM and became the basis for the IEEE 802/5 standard. A typical implementation of a Token Ring network is characterized by the following initial data: the maximum number of stations is 96; maximum number of hubs 12; maximum length of the closing cable 120 m; maximum cable length between two hubs or between a hub and a station 45 m; two options for data transfer rates on the line 4 or 16 Mbps.

The local area network data transmission standard will use the Fast Ethernet 100BASE-TX standard. This standard uses 8-pin RJ-45 connectors and Category 5 cable, a type of signal cable that consists of 4 twisted pairs, for data transmission. To combat interference, only the properties of a twisted pair are used in the transmission of differential signals [16].

3.1.4. Selection with justification of active equipment

In building a multi-service network, two carved models of routers 48 port and 8 port will be used. 48 port Cisco Catalyst 2960-48 switches will be used as floor switching nodes and connect all workstations on its floor. Cisco Catalyst 3560-8 8-port switches will be used as a chassis switching node, connecting the floor switches of its building with each other and the central switching node.

Features of the Cisco Catalyst 2960-48 Switch:

Switch level: 2 level

Cisco IOS Type: LAN Lite

PoE support: 24 ports 15.4W/48 ports 7.7W

Maximum PoE power: 370W

Versatile Ethernet ports: 2 SFP ports

Ethernet aggregation ports: 2 ports 10/100/1000 Mbps

Ethernet access ports: 48 10/100 Mbps ports

MPPS Switching: 13.3 MPPS

Switching Matrix: 88 Gbps

FLASH memory: 32 MB

DRAM: 64MB

Console ports: 1 CON port RJ-45

Number of active VLANs: 255 VLANs

MAC address table: 8000 MAC addresses

Max VLAN ID: 4096

Height RM UNIT: 1U

Overall dimensions (HxWxD) cm: 4.4x44.5x33.2

Power type: AC 220V

Power consumption nominal / maximum: 50/800 Watts

Features of the Cisco Catalyst 3560-8 Switch:

Dimensions (width x depth x height), cm: 27 x 23 x 4.4

Weight, kg: 2.3

Power Options:

- Power consumption: 204 W
- AC: 100 - 240 V (auto-sensing), 2.5 - 1.3 A, 50 - 60 Hz
- PoE: 124W

Status indicators:

- Per port: link integrity, disconnect, activity, speed, full duplex, PoE functioning, PoE error, PoE disconnect

- System Status: System, Link Status, Duplex, Speed, PoE

Memory specifications:

RAM: 128 MB

Flash memory: 32 MB

Interface ports:

Copper interfaces: 8 x RJ-45 Ethernet 10/100 PoE

Optical interfaces: Only one port can be used at a time:

- 1 x RJ-45 10/100/1000BASE-T
- 1 x SFP 1000BASE-T

Other interfaces: 1 x console port

Network features:

Supported Standards: IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x, IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p Prioritization CoS, IEEE 802.1Q VLAN, IEEE 802.3 10BASE- T, IEEE 802.3u 100BASE-TX Specification, IEEE 802.3ab 1000BASE-T Specification, RMON I and II, SNMPv1, SNMPv2c, and SNMPv3.

Performance:

- Switching Matrix: 32 Gbps
- Non-blocking switching at 2.7 Mpps (packet size 64 bytes)
- Ability to configure up to 12000 MAC addresses
- Ability to configure up to 11,000 unidirectional routes
- Ability to configure up to 1000 IGMP groups
- MTU configurable up to 9000 bytes, with a maximum Ethernet frame of 9018 bytes (Jumbo frames) on Gigabit Ethernet ports, up to 1546 bytes for Multiprotocol Label Switching (MPLS) tagged frames on 10/100 ports

Routers.

The Cisco 2811 router will be used to create the network. Due to the small number of RJ-45 connectors, the selected router will have a 4-port Cisco HWIC-4ESW module inserted into it. An inexpensive TP-LINK TL-R480T router will be placed in the warehouse.

Features of the Cisco 2811 Router:

Physical characteristics of CISCO2811:

Dimensions (width x depth x height), cm: 43.82 x 41.66 x 4.45 1U

Weight, kg: 6.4

Power supply: - AC: 100 - 240 V, 47 - 63 Hz, 2 - 1 A

– DC: 24 – 60 V, 8 – 3 A

Memory specifications:

Flash memory:

– Default: 64 MB

– Maximum: 256 MB

RAM:

– Default: 256 MB

– Maximum: 768 MB

Interface ports:

WAN/LAN interfaces: 2 x 10/100 Fast Ethernet

Other interfaces: 2 x USB 1.1

1 x console port

1 x aux port

Expansion slots: 2 x AIM (internal)

4 x HWIC, WIC, VIC, or VWIC

2 x PVDM (DSP) (internal)

1 x NM or NME

Network features:

Capacity: 120,000 bags/s

Features of the Cisco HWIC-4ESW Module:

dimensions (width x depth x height), cm: 7.82 x 12.03 x 1.93

Weight, kg: 0.079

Interface type: HWIC

Status indicators: One LED on each port to display network status

Interface ports:

Interface ports: 4 x RJ45 10BASE-T/100BASE-TX (automatic detection of speed, transmission mode and cable type)

Transfer rate: 10/100Mbps

Cable types: RJ-45 connector

Network features:

Protocols: Ethernet: IEEE 802.3, 10BASE-T

- Fast Ethernet: IEEE 802.3u, 100BASE-TX
- IEEE 802.1d Spanning Tree Protocol
- IEEE 802.1p CoS for Traffic Prioritization
- IEEE 802.1q VLAN
- IEEE 802.1x Security
- IEEE 802.3x Full Duplex and Flow Control

Management: SNMP, Telnet, CLI, SPAN, TFTP, NTP[17].

Features of the TP-LINK TL-R480T router:

Indicators 10/100 Mbps, Link/ACT, Power

Intel IXP processor up to 266 MHz

Console port Yes, RS-232 cable included

Management Web interface

Fast Ethernet ports 4x 10/100Mbps, 3 of which are WAN switchable

WAN Ports 4 RJ-45 ports (3 of which are LAN switchable)

Power supply From the mains

Power supply Built-in

Port Mirroring Supported

802.1x (User Authentication), 802.3 (Ethernet), 802.3u (Fast Ethernet), 802.3x (Flow Control) Compliant

Secure PPPoE VPN Protocols

Routing Static

Supported: QoS, MAC Address Cloning, VLAN, Port Limiting, Virtual Server, DMZ, NAT, DHCP Server

Dimensions (width x height x depth) 294 x44 x180 mm

Working temperature 0 ~ 40 °C[18].

3.1.5. Selection and justification of SCS passive equipment

Category 5 twisted-pair cable. A type of signal transmission cable that consists of four twisted pairs. This type is used in structured cabling systems for computer networks such as Fast Ethernet. It is also used for telephony and video transmission. The cable is terminated with an RJ45 modular jack or patch panel. Most Category 5 cables are unshielded. To combat interference, only the properties of a twisted pair are used in the transmission of differential signals. Category 5 twisted pair cable is suitable for the implementation of the graduation project, since it can operate at a speed of 100 Mb / s at a distance sufficient for this task. The cable is the best value for money.

The RJ45 connector is a unified connector that is used in telecommunications and has eight pins and a latch. Used to create local area networks using 10BASE-T, 100BASE-T and 1000BASE-TX technologies using 4-pair twisted pair cables, as well as many other areas of technology. This is the most common connector suitable for all used network equipment.

Cable channels 60x40 designed for laying in them in hidden and open ways on combustible and non-combustible surfaces both indoors and outdoors of electrical, telephone, computer and television networks operating at an electrical voltage of direct or alternating current of not more than 1000 volts. The box size 60x40 is suitable for the largest volume of cables to be used.

Wall bracket, 19", 6U, rotation, D=350 mm. Active network equipment will be fixed on them.

3.2. Development and implementation of a network policy, setting up telecommunications equipment of an organization's multi-service network

3.2.1. Network policy requirements

The internal security of the local network will be provided by VLANs. VLAN (Virtual Local Area Network) - a "virtual" local computer network, is a group of workstations with a common set of requirements that interact as if they were connected to the same router, regardless of their physical location. In this local network, we will use 4 VLAN networks:

Table 3.2

Distribution of access rights to internal resources and network services.

No.	VLAN name	Department name	Number of workstations
1	RID	Executive Directorate Guide.	4
2	Adminhoz	Administrative and economic part.	17
3	Finans	Operational accounting department. Accounting. Financial department.	43
4	Kommerh	Transportation Department. Purchasing department. Sales department. Marketing department. Advertising department. Commercial service management.	60

Not all departments will have access to servers due to the fact that they do not need to work from 1s.

Table 3.3

Server name	RID	Adminhoz	Finans	Kommerh
1s Server 1	By FTP	Limited	By FTP	By FTP
1s Server 2	By FTP	Not	By FTP	By FTP

Distribution of access rights to external resources and network services.

Access to external resources will be open to all departments, but some of the departments will not be completely open. It is clear that not all employees of the company require constant access to the Internet. Employees do not always use corporate resources exclusively for work, so the task of accounting for traffic is becoming increasingly important. To keep records of Internet access by user groups and individually for each user, there are Internet traffic accounting systems.

Table 3.4

Name of VLAN	HTTP	Telnet	FTP	DNS
RID	Full	Not	Full	Full
Adminhoz	Limited	Not	Limited	Full
Finans	Limited	Not	Full	Full
Kommerh	Full	Not	Full	Full

Ensuring the security of working with an external network.

To ensure the security of working with the global Internet, the anti-virus program Kaspersky Small Office Security will be installed on the workstations. Kaspersky Small Office Security is a solution that provides the highest level of protection for your company's computers and servers against modern Internet threats: viruses, spyware and other malware, spam and hacker attacks. Excellent protection quality, high performance, ease of installation, configuration and use of the product will allow you not to worry about information threats and focus on solving business problems.

3.2.2. Network Management Technology Requirements

Network management architecture

Almost always, the network management architecture uses the same basic structure and set of relationships. End stations, such as workstations and other network devices, run software that allows them to send alarms when problems occur. Problems are recognized when one or more user-specified points are exceeded. Control objects are programmed so that upon receiving these alarms, they respond by performing one, several, or a group of actions, including:

- Operator notice
- Event registration
- System shutdown
- Automatic attempts to fix the system

Control entities may also poll end stations to check certain variables. Polling can be automatic, or it can be initiated by an administrator. These queries are answered by "agents" at managed points. Agents are software modules that collect information about the managed device in which they are located, store this information in a "management database" and provide it to management entities located within "network management systems" through the local network management protocol. Known network management protocols include "the Simple Network Management Protocol (SPMP)" (Simple Network Management Protocol) and "Common Management Information Protocol (CMIP)" (Common Management Information Protocol). Management proxies are objects that provide management information on behalf of other objects.

3.2.3. ISO Network Management Model

ISO has made a major contribution to the standardization of networks. The organization's network management model is the primary tool for understanding the main functions of network management systems. This model consists of 5 different areas: Performance Management, Configuration Management, Accounting Management, Fault Management, Data Protection Management

Performance management.

The purpose of performance management is to measure and enforce various aspects of network performance so that inter-network performance can be maintained at a satisfactory level. Examples of different efficiencies are:

- Network bandwidth time
- User reactions
- Line utilization factor.

Performance management includes several stages. The first of these is to collect performance information on those variables that are of interest to network administrators. Next comes the analysis of information to determine the normal levels of the network. Determining appropriate performance thresholds for each important variable such that exceeding those thresholds indicates a problem in the network that is worthy of attention.

Managed entities constantly monitor efficiency variables. When the efficiency threshold is exceeded, an alarm is generated and sent to the NMS.

Each of the above items is part of the process of installing a reactive system. If performance becomes unsatisfactory due to exceeding an administrator-set threshold, the system responds by sending a message. For example, when designing the impact of network growth on network performance, a network simulator is sometimes used. These simulators can alert administrators to impending problems in time so that corrective action can be taken.

Configuration management

The purpose of configuration management is to control network and system configuration information specifically so that you can track and manage the impact on network performance of different versions of hardware and software drivers. Since all hardware and software elements have operational deviations, errors, or both, which can affect the operation of the entire network, such information is important to keep the network running smoothly.

Each network device has a variety of version information associated with it. For example, a designer's workstation may have the following configuration:

Operating system, Version 3.4. And the software

- Ethernet, Version 1.4
- TCP/IP, Version 2.3
- NetWare, Version 6.2
- NFS, Version 4.3
- X.25, Version 4.0
- SNMP, Version 2.3

To make it easy to access, configuration management subsystems store this information in a database. When a particular problem occurs, this database will be searched for clues that can help solve the problem.

Resource Accounting Management

The purpose of resource usage accounting is to measure network usage so that individual or group users can modify its interaction accordingly. Such regulation greatly reduces the number of problems in the network and increases the fairness of the network for all users.

As in the case of performance management, the first step to adequate accounting management is to measure the utilization of all the most important network resources. Analysis of the results gives an idea of the current degree of use. Some correction may be used to achieve the best practice for gaining access. From this point forward, further measurements of data usage can yield billing information as well as the information used to evaluate fairness correctness and optimal source utilization.

Fault management

The purpose of fault management is to identify, record, inform the user and, if possible, automatically correct problems in the network in order to efficiently maintain the network. Because faults can result in network downtime or unacceptable degradation, fault management is probably the most widely used element of the ISO network management model.

Fault management involves several steps:

- Determining the symptoms of the problem.
- Isolate the problem.
- Troubleshooting.
- Verify troubleshooting on all critical subsystems.
- Recording the discovery of a problem and its solution.

Data Protection Management

The purpose of data protection management is to control access to network resources in accordance with local guidelines to prevent network disruption and unauthorized access to sensitive information.

Data protection management subsystems work by dividing external sources into authorized and unauthorized areas of the network. For some user groups, access to any network source is prohibited. These users are usually non-members of the company. For other users of this network, it is wrong to access information that comes out of any department. For example, access to files about the presence of debts is inappropriate for any users who do not belong to the financial management department.

Data protection management subsystems control the following set of functions:

- identify sensitive network resources
- Define mappings between sensitive network sources and a set of users
- Control access points to sensitive network resources
- Register inappropriate access to sensitive network resources.

3.2.4. Data archiving

Data archiving will be provided by means of WinRAR. A powerful utility for creating and managing archives, containing a whole range of additional useful features. WinRAR is used daily by millions of people around the world to save PC space and transfer files quickly.

3.2.5. Network Address Allocation Requirements

The local network will use the network 10.8.240.0/26. All active network equipment and servers will occupy the range of ip addresses from 10.8.241.1 to 10.8.241.62. Workstations will have ip addresses ranging from 10.8.242.129 to 10.8.245.255

Table 3.5

Name of active network equipment	Subnet address	Range of addresses used	IP addresses
	10.8.241.0	10.8.241.1-10.8.241.62	
1s Server 1			10.8.241.1
1s Server 2			10.8.241.2
Router			10.8.241.3

Table 3.6

Name VLAN	The address of the subnet	The range of addresses used	Name of the department	IP addresses of departments
RID	10.8.242.0/26	10.8.242.1 – 10.8.242.62	The leadership of the Executive Directorate	10.8.242.1-10.8.242.4
Adminhoz	10.8.243.0/26	10.8.243.1-10.8.243.62	Stock	10.8.243.1-10.8.243.3
			The administrative part	10.8.243.4-10.8.243.17
Finans	10.8.244.0/26	10.8.244.1-10.8.244.62	Accounting	10.8.244.1-10.8.244.12

End of table 3.6

			Department of operational accounting.	10.8.244.13-10.8.244.33
			Financial department.	10.8.244.34-10.8.244.43
Kommerh	10.8.245.0/26	10.8.245.1-10.8.245.62	Transportation Department.	10.8.245.1-10.8.245.7
			Procurement department.	10.8.245.8-10.8.245.18
			Sales department.	10.8.245.19-10.8.245.29
			Marketing department.	10.8.245.30–10.8.245.41
			Advertising department.	10.8.245.42-10.8.245.53
			The leadership of the commercial service.	10.8.245.54-10.8.245.60

3.3. Calculation of economic indicators

In this part of the work, the calculation of one-time costs for the developed local information network will be performed. To find the one-time costs, you need to perform the following calculations:

- calculation of cost estimates for development;
- determination of the cost of technical and software components of the system;
- determination of the cost of installation and adjustment of the system.

3.3.1. Cost of hardware and software

Taking into account the analysis of the hardware already available at the enterprise, the need to purchase the following equipment was revealed

Table 3.7

Name	Unit rev.	Qty	Price per one. UAH
1	2	3	4
Passive network equipment			
Horizontal subsystem			
SCS "Exalan +" UTP cable, 4 pairs, cat 5e, PVC, 305 m	PCS	16	3275.38
SCS "Exalan+" RJ-45 module, Category 5e, type KRONE (IDC 90)	PCS	150	49.00
RJ-45 plug	PCS	340	15.00
Box for external RJ-45 socket	PCS	150	20.00
Main box 60x40 complete with cover	PCS	530	180.00
Inner corner for the box 60x40	PCS	70	61.00
Connecting bracket, 60x40 mm	PCS	480	44.80
Patch panel 19", 2U, 48 RJ45 ports, category 5e	PCS	6	1953.00
Mounting hardware			
Wall bracket, 19", 6U, rotatable, D=350 mm	PCS	6	1134.61
Screw with washer and nut	PCS	24	5.78
Auxiliary materials			
Nylon strap. unopened 200 mm, 100 pcs.	PCS	1	56.00
Screw pad for fastening ties, 19x9 mm 100 pcs.	PCS	1	78.90
Corrugated tube for wiring D40 mm with broach (20 m)	PCS	1	475.44
Dowel-screw 5.0x50 package 10 pcs. x10	PCS	35	9.00
Active network equipment			
Cisco Catalyst 2960–48	PCS	5	79076.00
Cisco Catalyst 3560-8	PCS	3	23546.00
Cisco HWIC-4ESW module	PCS	1	7296.00
Cisco 2811	PCS	1	42114.00
tp-link tl-r480t+	PCS	1	1860.00
Total equipment			153 860

3.3.2. Software

It is required to purchase software and new operating systems, since the old software does not correspond to the work that should be carried out on the company's workstations and servers. The new software was chosen in order to improve the company's work and allow working with licensed and modern products.

Table 3.8

Name	Unit rev.	Qty	Price per one. UAH	Total, UAH
Small Office Security (5 пк. 1 год)	PCS	25	4900	122500
WinRAR 4.x	PCS	122	908	110776
Microsoft Office 2010	PCS	102	7060	720120
Windows 7	PCS	124	2900	359600
Windows Server Standard 2012	PCS	2	47844,3	95688.66
Total				2503184.66

3.3.3. Costs for commissioning, installation and start-up

The costs of the work carried out include: wages of participants in the work carried out; costs for materials and various types of energy; computer operating costs; overheads.

For the installation of passive network equipment, wages are calculated according to the amount of work done

The calculation of the number of performers and the salary fund is presented in Table 3.8.

Table 3.9

Name	Technical and economic indicators		
	Unit rev.	Qty	Unit cost per. UAH

End of table 3.9

1	2	3	4
Installation work		x	
Cabling		x	
Cable tracing for 1 m (reel unwinding, marking, length measurements, stretching, cutting)	м	4700	3.00
Cable laying in boxes (1 m)	M	4500	10.00
Cable laying in boxes (1 m) H>2 m	M	220	14.00
Installation of sockets		x	
Connecting a category 5 outlet per port	PCS	110	81.00
Mounting the socket in the box	PCS	110	75.00
RJ-45 connector crimp	PCS	340	10.00
Installation of cable routes		x	
Fastening thick boxes to concrete and brick walls (1 m)	M	530	135.00
Testing		x	
Certification of network connections for category 5, 15-year warranty (1 port)	PCS	150	255.00
Construction works		x	
Punching concrete and brick walls with a drill with a diameter of 22 mm (wall thickness 10 cm)	PCS	23	135.00
Punching concrete and brick walls with a 22 mm drill (wall thickness >10 cm)	PCS	2	540.00
Punching an interfloor channel (1st floor) using a drill with a diameter of 22 mm (overlapping thickness 10 cm)	PCS	4	540.00
Total for installation work			1805

Setting up and debugging network equipment. As well as setting up servers and workstations, installing software is carried out by technical maintenance engineers.

3.3.4. Salaries

The cost of the basic salary of performers is determined by multiplying the amount of the monthly salary by the amount of time they actually spent. Moreover, the number of working days is considered equal to 22.

Table 3.10

№	Job title	Number of working days	Monthly salary, UAH	Amount of salary	Additional salary, UAH
1	Maintenance Engineer	6	25000	6816	0
2	Maintenance Engineer	6	25000	6816	0
3	Maintenance Engineer	7	25000	7952	0
			Total:	21584	0

3.3.5. Total current expenses

Table 3.11

The cost of equipment will fully pay off in four years and two months

№	Expenditure.	UAH
1	Cost of hardware and software	153 860
2	Software	2503184.66
3	Costs for commissioning, installation and start-up	1805
4	Salaries	21584
Total:		2 679 933

CHAPTER 3 – CONCLUSIONS

During the design were performed:

- Analysis of the company's structure;
- Choice of mixed topology of the star-star network, as far as this topology is the most reliable and economical price-reliability ratio of the topology of the network of offices of Adidas-Ukraine;
- The standard of data transmission of the local computer network is selected, the Fast Ethernet 100BASE-TX standard will be used;
- Identified Cisco equipment for building a multiservice network;
- Developed and implemented a network policy. Configured the telecommunication equipment of the organization's multiservice network;
- Calculated economic indicators.

CONCLUSIONS

This diploma work considers the design of a multiservice network of the company SE "Adidas-Ukraine". The designed corporate multiservice network is geographically distributed and connects the floor switches of its building with each other and with the central switching node.

In the course of choosing equipment for building a network, according to a number of criteria, the choice was made on Cisco equipment, as it most fully meets the criteria defined in the project.

When describing the network being designed, the mechanisms for ensuring the quality of service, as well as some issues of information security, are considered. The main threats to data transmitted in a multiservice network have been identified and measures taken to prevent these threats have been described.

REFERENCES

1. http://ru.wikipedia.org/
2. https://siblec.ru/telekommunikatsii/multiservisnye-seti-svyazi#1
3. https://siblec.ru/telekommunikatsii/multiservisnye-seti-svyazi
4. https://compress.ru/article.aspx?id=9404#begin
5. https://libr.aues.kz/facultet/frts/kaf_aes/40/umm/aes_5.htm
6. https://www.sibsau.ru/sveden/edufiles/126009/
7. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.
8. https://www.bytemag.ru/articles/detail.php?ID=8788
9. https://habr.com/ru/post/170895/
10. https://www.kommersant.ru/doc/2594410
11. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:OSS/BSS_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B
12. https://ozlib.com/1046830/tehnika/protokol_initsiatsii_sessiy#80715
13. https://studbooks.net/2361315/tehnika/rabotosposobnost_oborudovaniya_multiservisnyh_setey
14. https://www.sviaz-expo.ru/ru/articles/2016/oborudovanie-korporativnoj-seti
15. https://studbooks.net/2361315/tehnika/rabotosposobnost_oborudovaniya_multiservisnyh_setey
16. https://www.techtarget.com/searchnetworking/definition/Ethernet#:~:text=Ethernet%20is%20the%20traditional%20technology,rules%20or%20common%20network%20language
17. https://www.cisco.com/
18. https://www.tp-link.com/