

The Ministry of Education and Science, Youth, Sport of Ukraine
A.S. POPOV ODESSA NATIONAL ACADEMY OF TELECOMMUNICATIONS

Chair of Telecommunication Networks

Studying course
TELECOMMUNICATION AND INFORMATION NETWORKS

Part III
THE NETWORK SERVICES.
THE NETWORK APPLICATIONS
(Studying module 4.1)

*Methodical instructions for performance
to the cycle of laboratory works
for training bachelors in Telecommunication*

APPROVED BY
Methodological Council of
Academy of Telecommunications
Protocol number 16
on March 23, 2012

Odessa, 2013

Compilers: Nikityuk L. A., Tikhonov V. I., Sherepa I. V., Bybentsova L. V., Tsaryov R. Y., Shulakova K. S., Borzdych T. O., Ruslyachenko M. S., Nikitchenko V. V., Merenkova M. S., Yavorskaia O. M.

Telecommunication and information networks (Part 3). The network applications: methodical instructions for performance to the cycle of laboratory works for training bachelors/ [Tikhonov V. I., Shulakova K. S., Borzdych T. O. and ect.] – Odessa: ONAT named after O. S. Popov, 2012. – 118 p.

ACCEPTED
After Meeting Chair of
«Telecommunication networks»
Protocol number 7
on February 29, 2012

CONTENT

LABORATORY WORK № 1. Voice system of communication Skype	4
LABORATORY WORK № 2. Organization of videoconference in informational networks	16
LABORATORY WORK № 3. Organization of streaming on a network using RTSP protocol	31
LABORATORY WORK № 4. Investigation of multimedia traffic parameters	43
LABORATORY WORK № 5. HTTP network server: Web – processor HTML.....	56
LABORATORY WORK № 6. Web design and Web hosting.....	67
LABORATORY WORK № 7. Providing Internet – hosting services. Developing and maintenance of websites based on Apache	76
LABORATORY WORK № 8. Configure Proxy Server.....	93
Appendix A	106
Appendix B	115
Literature	118

LABORATORY WORK № 1

THEME: VOICE SYSTEM OF COMMUNICATION SKYPE

1.1 PURPOSE OF THE WORK

Study principles of voice traffic transfer to networks with packet switching. Study basic possibilities of Voice system of communication Skype.

1.2 KEY PRINCIPLES

Not long ago, networks with the channel switching (telephone networks) and networks with the packet switching (IP-networks) existed almost independently from each other and were used for different goals. Telephone networks were used only for voice information transfer, IP-networks – for the data transfer.

Because of increasing of high – speed access usage to the Internet network, the greater quantity of companies and private users start to use Internet and other Ip-networks as means to make telephone calls. Given technology is called «voice over IP-protocol» (Voice over IP, VoIP).

Nowadays to connected worlds – world of telephony and world of Internet allows technology IP-telephony. Technology of IP-telephony combines these networks with a help of device gateway. Gateway is a device, in which from one side connects telephone lines, and from the other side – IP-network (for example, Internet).

Main advantages of IP-telephony, the possibility of providing of many additional services, and also significantly cheaper services, than traditional coaches and international conversations. Let's consider basic variants of connection establishing on base of IP-telephony technology.

Phone- Phone. Lets consider, in which way IP-telephony call performs. For example, that subscriber from the city A calls to subscriber from city B. The call comes from city A telephone network on the gateway of A city, becomes digital, compresses by special algorithm, and as IP-packets transfers to IP-network. In the headers of packets consists information on which gateway of IP-network must these packets come. Packets which come on the gateway in the B-city transform backward into the telephone signal and the subscriber in the city B pick up the handset and talk with the subscriber A.

Final consumers of service do not even have an idea, how this call performs.

As during IP-telephone call international telephone operator is not involved any way, so the price of this call is much less than the traditional telephone connection.

However, the telephone-telephone call is the most evident, but not the single only one service, which operator of IP-telephony can propose.

Decisions of IP-telephony combine voice and data in one network and propose not only cheap international and local calls, but entirely set of modern communication services to each user.

Computer-Telephone. Being in any country, the subscriber of IP-telephony provider can perform a call from any computer, with the Internet access. For this he

must setup the on computer program, that allows to perform this call, and input registration data one time. It must be multimedia computer, it means that it must have the voice board, speakers and a microphone. The call from the computer is usually cheaper than the Telephone call Telephone.

WEB – Telephone. One more service which Ip-telephony providers propose – is the call from the Web-site that allows to perform calling, by choosing link on the name of the necessary subscriber. That decision is directed, first of all, on the expanding of possibilities of electronic commerce. WEB – telephone allows the Internet subscribers users to talk directly, for example, with a market representative or with the specialist of technical support.

Establishing of telephone connection performs by the clicking of the cursor on the link, which represents, for example, a name of a company, the name of necessary subscriber on the Internet page. This way the subscriber do not need the second telephone line or breaking the work in the Internet, everything needed is to download the clients software, which is usually possible to find on the same WEB-page («PC-client») and which establishes automatically. On the other hand, WEB –telephone allows to representatives of companies answer the questions, demonstrate necessary information, and this way improving the quality of the services.

Telephone-Computer. Internet users always have such kind of problems as: busy telephone lines during Dial-up session. IP-telephony allows to solve this problem in a very elegant way. The only thing which subscriber must do is to reserve on his own TS the signal «busy» redirecting on the telephone number of IP-telephony server. During the call to the subscriber's number and the Internet-session simultaneously, the call redirecting in the IP-telephony server, which transforms its into the IP-packets and sends to the subscriber's computer. On the subscriber's computer arises the pictogram «Incoming call», clicking on which he (the subscriber) can speak with a calling person.

There are a lot of different, commonly incompatible voice transfer technologies trough the Internet, based on different standards. International Telecommunication union standard (ITU) provides information voice transfer and videoconference communication. Internet Engineering Task Force (IETF) use the standard, which is called Session Initiation Protocol (SIP). Cisco Company made developed the patented system, which is called Skinny Client Control Protocol (SCCP).

1.2.1 Voice speaking system Skype

Skype is a patented voice system of communications based on VoIP technology, which was developed in 2003 Skype Technologies S. A. –corporation, registered in Luxemburg. Basic functional Skype components are program-client Skype, Skype – server, Skype – protocol. Today, Skype is a very popular program and accessible for all following operating systems: MS Windows, MacOS, PocketPC and Linux.

Skype of system is so popular because of the following factors:

– Skype Usage is free. There are only nominal prices for the calls, made with using of functions «SkypeOut» and «SkypeIn». These functions allow to perform

voice conversation for Internet subscribers with subscribers of telephone network of land phones common usage.

- Usability. Skype-client is easy to be set up/fixed/download. Except subscriber's name choosing, no one else configuration is needed. Unlike programs based on SIP (used, for example by Vonage company), Skype-clients with no difficulties can work with firewall and network address translation systems (NAT).

- Skype proposes high-quality voice codec, what allows to receive characteristics, that are compatible with traditional telephone networks, only if a Skype-client has high-speed Internet access.

- In addition to voice telephony Skype supports exchange of immediate messages, research and file transfer.

- Skype uses cipher. Unlike traditional telephone communication and other VoIP-systems, transferring of voice information ciphers with the help of 128-bites and more cryptographic codes, that makes practically impossible the passive interception of Skype conversations and impossibility to decipher them and to hear them.

Skype system based on technology of connection of equal nodes by Peer-to-Peer method, unlike other popular principle of call transferring through central server (realized, for example on Vonage company). A Skype-client searches and finds other Skype-clients, then from these connections creates a network, which can be used for communication , and also to find other users. Skype system has income because it takes the payment from users for the use of terminal gates, which connect data transfer network with public usage of telephone networks.

1.2.2 Compatible characteristic of Skype system and other Peer-to-Peer systems

Although Skype uses Peer-to-Peer system to determine the location of other Skype clients and transfer text messages, there are many aspects by which Skype differs from other «pure clean» Peer-to-Peer system. Let's consider some of them.

Skype system relies on the central identification server, which identifies users and distributes software. Identification and distribution of software performs is with usage of personal keys RSA with digital signature. Checking of the equality of open RSA key is included into each downloaded Skype module.

Some nodes of Skype have state of special nodes, called as «supernodes». When a Skype – client log in on computer, that has public IP-address and is not situated beyond the internetwork monitor, this computer is going to be a supernode. Supernodes are used as connection points, for the following: computer that placed beyond the internetwork monitors could interact with other users of Skype. Computers placed beyond the internetwork monitors, scan Internet for the supernodes, then form and maintain long-term connection between them. In such way supernodes become real points of connection with computers that placed beyond the internetwork monitors and connection between which is difficult.

When the functions «SkypeIn» or «SkypeOut» of program Skype – client are used, all the information goes through the Skype servers, which placed in different countries and call zones.

1.2.3 Identification of Skype system

Each Skype – user has name and password. Every user's name of is registered on the special electronic address. To enter the system the user must input it's login and password. If the password is lost, Skype system changes password and sends a new registered email to the user. This is called Identification and Authorization based on the email address. Skype-client also has a possibility to Remember names of users and passwords and perform automatically entrance. Skype is the voice communication system, and its users can identify people by voice. However it does not work if the conversation performs only through the text messages and files.

1.2.4 Main features of Skype-system

Safety and security. To estimate safety of Skype, it is necessary to determine definite types of threats and then to solve, if such principle of work can resist the threats.

Safety of conversations in the Skype-system depends on many factors, including safety of computer on which the Skype – client is established, and network that is used for conversation.

Skype protocol is patented and closed, so, as a result, the sources of information can be the applications of company about the safety of program and those information that can be received during the technical analysis of a given software.

Safety of information, that is transferred in the ciphered and compressed view, depends on factors, including the usage of special algorithms of cipher and compressing, choosing of coding keys, procedure of keys exchange, and also performing of algorithms and protocols of ciphering and compressing in the given software.

Analysis of informational packets, transferred between the users, shows that the Skype – client program uses HTTP-version of protocol for connection with the Skype-server **ui.skype.com** (that is situated in Amsterdam), to perform the identification of users and passwords and to register on the Skype-server. Modified version of HTTP-protocol is used for the information transferring to other Skype-clients. While the exchange of information between the Skype-clients may be coded, searching form the Skype users, including searches that are necessary to identify Skype – calls, amenable to observation from the Skype. It means that non-privileged users can perform the traffic analysis and determine that one user calls to another.

Skype system uses algorithm of cipher RSA for the keys exchange and 256-bites AES (key) for coding. However, Skype company, despite look on the constant requests, refuses to open the basic principle of identification system of its certificates, reliable cipler. That is why it is logically to presume that data is coded but not enough.

Conversation through Skype is more confidential than the conversation through traditional analog or ISDN-telephone, which everyone can hear, which has the access to the telephone line in any point between any of conversation sides.

Skype system also is safer than today's VoIP-systems, as ciphering is not a part of the majority of VoIP - applications. Nevertheless, VoIP – conversation is possible to protect, hold VoIP-traffic through virtual private network (VPN). System which uses VoIP through VPN, is safer, than Skype, only if VPN is configured correctly.

It is important to understand that the Skype safety may be destroyed with the presence of spyware (software often called «spyware», because it looks on the web-sites, which are visited by users, and also places there advertisements) or other searching programs, that are downloaded on the user's PC. Forexample, program Netbus allows to strangers switch on pc's microphone and transmit the voice record through the Internet to the other computer. Such program can also hear not only Skype – conversations, but also others, which are going on in the office, in where which the computer is placed with downloaded Skype program.

There are other moments concern safety and reliability of Skype system, about those users must be informed:

- Skype-client does not record and safe Skype – conversations, but it can register history of text messages in the archive file for each user. Skype allows to record conversation by default, other words all text messages recorded, until the user does not perform backward actions. These files can be extracted with the help of spyware, other distance applications, or during non-sanctioned physical access to the computer system.

- As all Skype users loaded in one Skype – «cloud», any other Skype user can find out know, where other user is situated at the moment.

- Skype – client is trying to send packets between participants of conversation directly through the Internet, but if the direct way is not accessible, then it is possible that instead of this packets are send trough the other computers, on which the given program works (supernodes). Representatives of Skype say, that monitoring from the supernode side is impossible because of the ciphering. Logically to suppose, that such monitoring is impossible. Possibly, that workers in the Skype-company think that such monitoring is impossible, but some exist disadvantages in their protocol or in the system organization, that make such monitoring possible. A lot of such disadvantages were founded in other cryptographic protocols, after they were started to use.

- Functions «SkypeIn» and «Skype Out» can use ciphering till the Skype – gateway, but then telephone conversations decode and send through the standard telephone network of common usage, where can undergo by non-legal listening and monitoring.

- It is necessary to say, that most of risks, that appear because of Skype usage, and do not differ from risks of email or other personal programs for the information transmission. Usage of Skype program is less risky for the unity of all the system, only because that Skype initially was intended for the voice communication. But it is necessary to be careful, when Skype is used for the file transfer. With comparison

with KaZaA and other programs for the file exchange, Skype provides less risks, because the exchange is going on only between definite people while when files are downloaded from a potentially unknown source. On the other hand Skype – is more risky program, because the programs similar to KaZaA, have built in antivirus protection, which scans programs when they are download, Skype, is seemed not have such protection.

Accessibility. In many countries telephone network users feel small delays during 5 minutes per each user for a year or less, that is equivalent to 99.99905% of accessibility.

Initially construction of the Internet network supposed that network stand the loss of few critical connections, but it became the task for the developers and producers of Internet – equipment only recently. Quality of Internet service has more advantages compared to the telephone service. So currently telephone calls are not very accessible as so as calls through the networks of common usage.

Additional factors can destroy potential accessibility of Skype. As Skype-client depends on the name identification of the login and password, it is possible that the whole Skype network will stop to function if identification Skype-servers will fail or because of other reasons will stop it to be accessible.

Message integrity. Skype does not guarantee that voice, text messages and files will be delivered in the form in which they were sent.

However, in practice, Skype transmits voice well. Text messages and files are also passed with no distortion. But when using Skype over wireless 802.11 networks, voice quality suffers considerably.

1.2.5 Particular features of work in the Skype system

During the work in the Skype system there are some useful recommendations can be useful:

- It is necessary to be sure ubud that each computer where Skype-client is used, is free from «spyware» and additional «adware» modules, programs of remote control, computer viruses. All computers on which software Windows is used, should have the last version of antivirus programs.

- Name combination of user and password for Skype must not be used for other programs. User's name, that is used in Skype should be difficult to be guessed unravel. It must not be connected with the user name, organization or public facts about user.

- Names of users and passwords must change regularly, especially if the Skype is used for the secret information.

If user names are regularly changed it is more difficult for an attacker to trace the actions of a concrete user, and regularly changed passwords decreases time interval, during which the given password can be used.

- Skype users must take into account that given system at any moment can become non - accessible for not determined time. So it is necessary always to have alternative methods of connection between each other.

– Can not be completely sure that under a known user name hides the type of person that used the same name yesterday. It is not excluded that an unrelated person can sit at a computer of people who you know and use Skype without their permission or their account may be hacked and stolen. Always once again need to independently verify the identity of the person with whom you communicate, especially if you have to exchange secret information.

– Although the company Skype claims that the Skype network can not be used to spread computer viruses, the truth of this assertion is not proved. Particularly, a when buffer overflowed in the voice decoder there is a possibility of another Skype user to execute commands in the system, in which the user works. In addition, files transferred via Skype – client may contain viruses (or) spyware «spyware».

– It must be remembered that the use of coded negotiations can not be a substitute for caution in the content of what is a conversation on Skype about.

1.2.6 Using Skype while connecting by dialing (Dial-Up)

Testing Skype in a Dial-Up Internet dial-up ISP when connecting over analog phone lines at speeds of 26 kbit / s, showed that the quality of sound at such a rate significantly worsens. It loses much compared to analog telephone lines. However, Skype provides acceptable sound quality for a friendly two-way conversation. The advantage of Skype – low cost and safety, resulting from the use of encryption. In situations where international calls are too expensive or play call hocking calling is cause for concern, the use of Skype could be useful.

In order to use the phone lines dial-up, it is prudent expedient to unload all programs that also use the Internet (for example, all web browsers and email programs is desirable to turn off). The conversation in the Skype also will be better if subscribers avoid talking at the same time, as it minimizes the bandwidth requirements.

1.3 CHECK-UP QUESTIONS

1.3.1 What is the essence of the technology VoIP?

1.3.2 Name Enter the main advantages of IP-telephony technology.

1.3.3 Describe the main options for establishing a communication network based on IP-telephony technology. What are they?

1.3.4 Describe the main features of Skype.

1.3.5 Specify the features of Skype software compared to other VoIP-software products.

1.3.6 How is the identification and authorization of users of Skype performed?

1.3.7 Describe the reliability and security of the Skype.

1.3.8 What are availability and integrity of information transfer in Skype?

1.4 HOME ASSIGNMENTS

1.4.1 Study the principles of voice traffic over networks with packet switching, using lecture notes and recommended reading, key principles material.

1.4.2 Prepare answers to check-up questions.

1.4.3 Make a plan for implementation of laboratory work, guided by section

1.5 LABORATORY ASSIGNMENTS

1.5.1 Activate the program Skype – the client by double-clicking the left mouse button on the Skype icon in the window desktop «Student». Learn the basic capabilities provided in the «Start». Here you can quickly get an overview of the number of subscribers of Skype, currently connected to the network, as well as see the status of fee-based services.

This shows all missed calls, chats and calls.

1.5.2 Learn the key features provided in the «Subscribers» program Skype – client (Fig. 1.5.1).

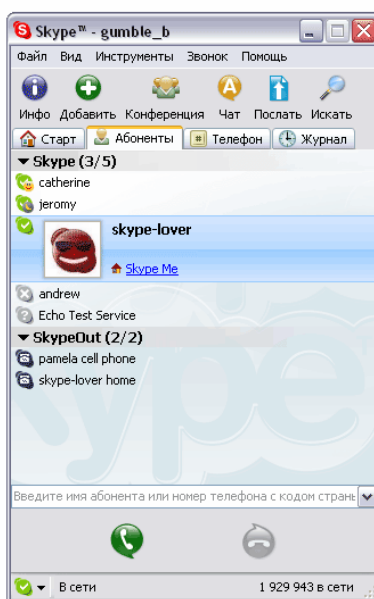


Figure 1.5.1 – Window «Subscribers» program Skype

Skype uses a system of AES (Advanced Encryption Standard), also known as Rijndael, which is used by the U.S. Government. Skype uses 256-bit encryption, which provides $1,1 \times 10^{77}$ possible keys to encrypt given calls and messages. Skype uses 1024 bit RSA signature symmetric AES keys. User's public keys certified by Skype server to connect to the network 1536 or 2048-bit RSA certificates.

1.5.3 Perform a telephone conversation in Skype system.

In order to carry out a telephone conversation with the caller of Skype, we must find a subscriber to the caller list and press the green button to start the call (see Fig. 1.5.2).

There are several ways to call the user from the list of subscribers (Contact – list):

1.5.3.1 The click right on button your username in the contact list or information on search results and select the «Call».

1.5.3.2 Double-click the user's name in the contact – a worklist or on a user name in the list of search results.

1.5.3.3 Choose a user name and press the «Call button» (the bell) at the bottom of the main window.

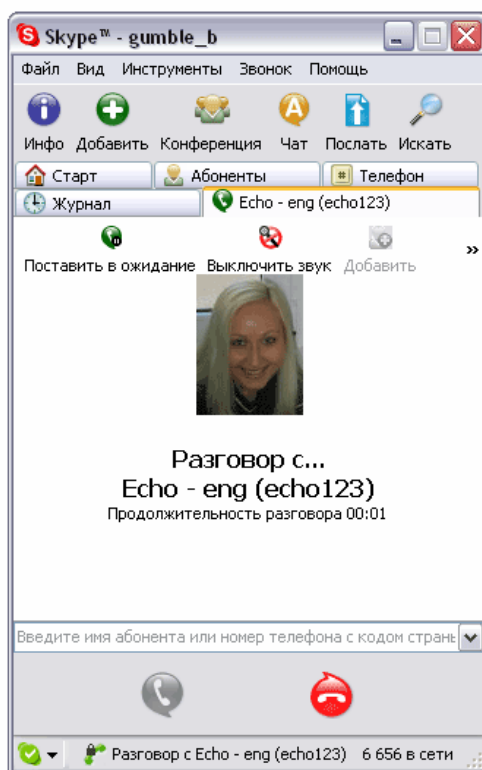


Figure 1.5.2 – Box conversation with the caller «program Skype»

1.5.4 Carry out the answer to the call in the Skype.

When someone calls, you should hear the sound of a phone call and see the flashing icon Skype. We must go to the window «Conversation with the subscriber (if not already displayed) and select the» Answer the call «or» Decline «it on the tab, of the incoming call. If you choose to «Reply the call», a voice connection is established, and the duration of the call will be displayed.

Calls between Skype users are always free. To end the call, press the red button.

1.5.5 Perform the addition of subscriber contact list.

To add a subscriber, click the right mouse button on the Skype Name (name of subscriber party) in the search results window and select the «Add to Contacts» (Add to the list of subscribers). Or select «Tools» -> «Add subscriber», enter your user name or phone number in the window.

1.5.6 Perform blocking unwanted calls.

Skype system can be specified performance receive calls only from people in your contact list. In the «Start» menu, select Tools -> Preferences -> Security.

Select «Only allow calls from people in my Contact List» (Only those who are on my list of subscribers) and save the settings.

1.5.7 Organize Conference Call.

Voice messages in the Skype you can transfer not only between the two callers. You can organize a conference – with the participation of up to five people.

Organize a conference – connection is very simple, and there are several options for doing this. If you want to connect with several people at the same time a conference – the connection, select the speakers from the contact – list, hold down the «Ctrl». Then press the «Conference» button on the toolbar. A window appears the «Conference» with the names of its members (see Fig. 1.5.3). Once you get answers to the request call, they will have access to conferencing services – communication.



Figure 1.5.3 – Window «Conference»

Conference meeting – communication can be accomplished if you are currently talking to someone and want to add other people to the conference. You can choose individuals who want to be add to your contact list and click on «Conference» button on the toolbar or simply press the right mouse button on the subscriber's name and select «Invite to conference» (invite to the conference).

It must be remembered that only the «master of conferences» (a person who initiates the conference) can add new participants. In addition, because the conference is based on technology Peer-to-Peer, it is important that the «boss of the conference» had enough computer power and speed of Internet connection. If you are planning a conference – with the large number of participants, then as a «host of the conference», the participant with the highest rate of Internet access should be chosen.

1.5.8 Make a voice call with PSTN.

The system allows Skype to give calls to ordinary and mobile phones. To do so, in the main window of Skype – the client click «SkypeOut» (see Fig. 1.5.4), then dial the number.

1.5.9 Perform the file transferring.

Skype system can also be used to transfer files. Skype works with files of any size.

By default, the Windows XP operating system to communicate over the Internet using a program Windows Messenger is used.

To transfer a file (see Fig. 1.5.5), press the Send button on the toolbar, the main window, select Add from Contacts – list recipient and press the call button.

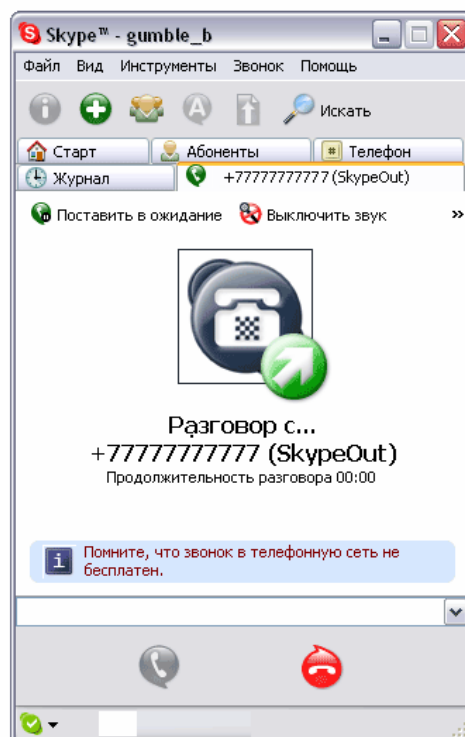


Figure 1.5.4 – Box conversation with the caller «SkypeOut»

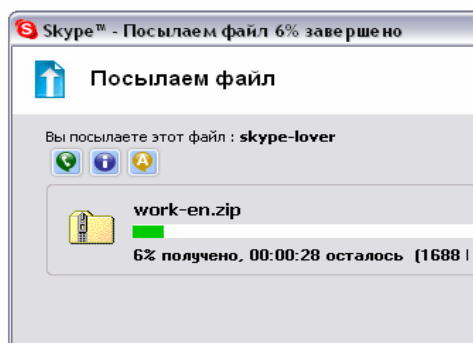


Figure 1.5.5 – Window «Sending a file to the subscriber Skype»

1.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

1.6.1 The name of laboratory work.

1.6.2 Purpose of the work.

1.6.3 Results of home assignments.

1.6.4 Short description of the work done.

1.6.5 Conclusions about the work done.

1.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 2

THEME: ORGANIZATION OF VIDEOCONFERENCE IN INFORMATIONAL NETWORKS

2.1 PURPOSE OF THE WORK

Introduction to methods of exchanging video images, sound and data between two or more points, equipped with hardware and software systems.

2.2 KEY PRINCIPLES

2.2.1 *Systems of videoconferences*

Is used as hardware and hardware-software solutions are used for video conferencing

Currently, three main groups of Videoconferencing the on telecommunication networks are used:

a) Studio video conferencing, requiring special hardware, and designed for large audiences.

b) Group videoconferencing, requiring both hardware, and software and hardware. Organization of this type of videoconferencing requires special equipment and the availability of ISDN lines.

c) Table (personal) video conference should be provided by software and hardware, support a dialogue between the two parties. For the organization of this kind of conferences with multimedia capabilities required personal computers (PCs), as well as the communication channel. As a communication channel can be used mono LAN or ISDN line.

The most available and cheap is desktop system (DS).

DS combines audio and video equipment and communication technology to interact in real time using an ordinary PC.

Application of DS assumes that all the participants are in their jobs and connected to a video conferencing session with a computer as easily as you do a regular phone call.

For the organization of DS it is required: a PC configured for use in a network having means to support audio and video conference codec (compression and decompression of audio and video signals), video camera, microphone, high-speed modem, network connection, or ISDN-line.

Currently, the majority of the most popular NV systems are-used bulletin board systems (White board), which allows you to reserve a separate area of the screen to view and collaborate on documents, in addition to traditional conferencing window, which displays the participants of DS.

Consider their brief characteristics:

Message Board. Usually, the message board means software, allowing co-create and edit documents to all conference participants. The document itself may

consist not only of textual information, but also contain graphics and other design elements. The advantage of message boards over other means of group information processing, available in DS, is compared with the comparative performance of shared applications. When using message boards do not need to use a specialized application, and can be used industry standard software with familiar commands and buttons on the shortcut, providing far more opportunities, message board designed for interactive exchange of text information.

Shared documents. From a technical point of view, the use of shared documents is in greater need for joint processing of specialized documents, such as a piece of a spreadsheet, forms, databases and document layout.

Sharing applications. The difference between shared applications and documents is in that not all applications are designed to work with documents, in distinction from, for example, from a word processor or spreadsheet.

Virtually any application that does not use undocumented calls, can act as a shared application. Advantage, which provides this method of group information processing, is that if a user does not have any application, it can be called from the computer of another user.

The main disadvantages of desktop videoconferencing are: poor video quality and lack of ability to communicate with a large number of participants

Technical capabilities of DS:

1. Affordable audience and the option of communication, usually it is a dialogue of two persons.
2. Quality characteristics of communication: there is no need of broadband.
3. Necessary expenses: only the software and hardware used in the workplace.
4. Equipment needed: computer with support for audio and video, microphone, speakers or headphones, video, LAN, switch (type switched), ISDN-connection.
5. Applications: for joint interactive information exchange, group work with applications, as well as transferring files with little time and financial costs.
6. Typical videoconferencing products and equipment:
 - Intel Proshare (Proshere Personal Video Conferencing System 200);
 - NetMeeting 2.0, NetMeeting 3.0 (the company Microsoft);
 - ISDN-card (Audio / ISDN Board 1.0);
 - Video card (Intel Video Capture Board 1.1);
 - Veb-kamera/ Video camera;
 - Headphones with built-in microphone;
 - Software.
7. Technical capabilities:
 - Implementation of the two-way audio and videoconferencing;
 - Support for switched PBX 5ESS, DMS, EWSD;
 - Videoconferencing in local networks;
 - Enabling protocol (RAS, Q.931, H.245, RTCP, recommendation H.450);
 - Activation of NetMeeting 3.0, telephone lines;
 - The software requires 17 MB of free hard disk space;

- Allows to run and use the shared application to share images;
- Supports standard H.320;
- Partial compliance with Class 1.

2.2.2 System requirements and installing

Microsoft (R) Windows (R) NetMeeting (R) provides a synchronous data transmission, audio and video on the Internet.

In each of those presented on the computer operating systems, application NetMeeting should be installed in a separate folder. When you install a single, common for all operating systems folder, which was listed by default, NetMeeting application will not run properly

In Windows 2000, NetMeeting application is installed in the folder \ net-meeting. This way new files overwrite the previously installed files NetMeeting for Windows 95 or Windows 98. After installing NetMeeting on a computer running Windows 2000 this application should be installed again in Windows 95 or Windows 98, but in to a different folder different from \ net-meeting.

Best work of NetMeeting is provided by fast internet connection (modem speed data transmission of 56 Kbps or higher, or LAN).

Recommended screen resolution – not less than 800 by 600 pixels. It is also possible to use the compression mode.

Using SLIP or other connections, acting like a SLIP / PPP, can prevent the proper execution of the program NetMeeting.

Necessary information on product support, see the file Support.txt. This file can be found in the Windows folder or NetMeeting.

If the OEM-version of Windows 2000 comes with your computer using the window «Add or Remove Programs» in Control Panel application NetMeeting can not be deleted.

General information. NetMeeting supports the H.323 standard for audio and video conferencing, as well as standard T.120 for conferences with the data transferring. With NetMeeting, you can send and receive calls from applications that are supported by these standards. Using the appropriate services and equipment from independent producers, NetMeeting enables telephone calls through the gateway H.323. In addition NetMeeting enables call devices MCU (modules for conferences connecting multiple nodes) that implement the standard H.323, as well as participate in the audio and video conferencing to connect multiple sites.

Common questions. Anyone, ho is holding a meeting in NetMeeting 3.0 (or later versions of this application) may determine a number of limitations (the inability to work together with applications, launched the program «Conversation», etc.). However, these restrictions will not apply to computers with a version of NetMeeting 2.x. Users of NetMeeting 2.x applications can work with these opportunities the same way.

- To determine your network name or IP-address used in NetMeeting, perform the following:

1. Find the shortcut on the desktop «My Network Places, click the right mouse button and pull down the menu, select «Properties».
2. Click the tab «Network Identification».
 - If you are installing Windows settings common to all computers on the network used «user profiles», after changing the computer may need to run the setup wizard of sound.
 - Convert audio and video data can be occurred simultaneously only between two parties.
 - Collaboration in applications Microsoft (R) DirectX (R), OpenGL, MS-DOS (R), the use of games with rich graphics and AVI-files are not supported.
 - General applications, «Bulletin» and «conversation» can not function properly if computers the which participate in the meeting use different installation language and keyboard layout.
 - If Internet Explorer 5.0 (or later version of this application) is running in autonomous mode, when you start NetMeeting automatically connection to the Internet does not occur. To circumvent this problem, install a remote connection protocol RAS for computers running Windows 2000. Or uncheck Work Offline (File menu) in Internet Explorer.
 - If the NetMeeting application has been run, as well as work with the means to access to a table, it is not recommended to change the intensity of color.

After configuring the appropriate settings of the meeting, you can disable to use outside of the NetMeeting software for connected participants («Conversation», «Board», «File Transfer». This, however, does not interfere with continuing to work with these programs, if it has been started before connection to the meeting with these settings.

Sending call (see Fig. 2.2.1). In NetMeeting calls may be send to some people simultaneously.

Thanks to the Internet Directory («Internet Directory Microsoft»), which is organized and conducted by Microsoft, it is possible to find other users of NetMeeting. To view the contents of the address book («Catalogue of Internet Microsoft»), click Search user in the directory and in the «Select» folder, click Directory Internet Microsoft.

***NOTE.** If you use to connect to the Internet connection you use proxy server which does not support the application NetMeeting, then subscribers calling from the web directories (directory server) is impossible. For input connection to connect the input the computer name may not be enough. Try to use the IP-address.*

In some devices of MCU the letters register is taken into consideration. This should be taken into account when entering the name of the conference while sending a call.

When you connect to the porter to call the conference MCU entering an

appropriate nickname may be needed. More details you can find out from your system administrator.

If calls are sent via the gatekeeper, when you connect you can specify the account name as well as the phone number (or both)

Getting call. Maximum number of simultaneous connections is determined by the registry settings for the protocol TCP/IP.

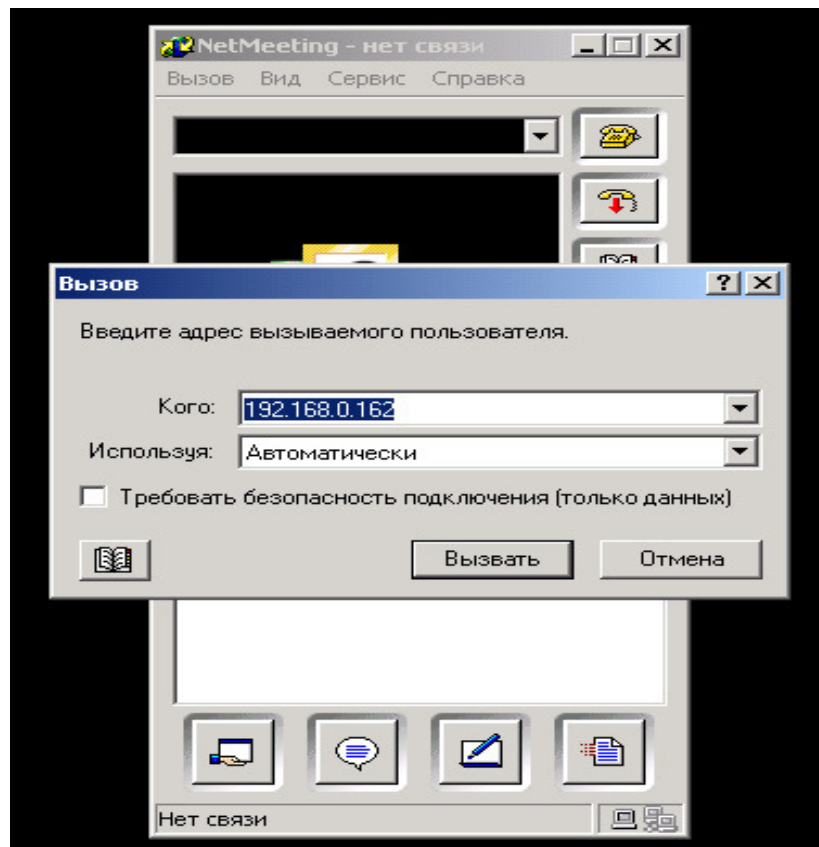


Figure 2.2.1 – Call forming

Working with applications. Any participant of the meeting may give any application to the other parties for the common use of. However, other users can monitor the implementation of general application on their computers. If there is the opportunity to control then other users will be able to work independently with this application.

NetMeeting 2.x users are unable to manage common programs that run on computers with NetMeeting 3.0 (or later).

This version of NetMeeting allows simultaneous work with common applications for many users at the same time. However, access via NetMeeting 2.0 to the application, which has already three or more users, may be impossible. The total number of users who can successfully participate in the meeting depends on network bandwidth and computing capacity of participants.

Microsoft Internet Explorer (version 5 or higher): If you allow shared access with the ability to control the window Explorer Windows, after this window will be

closed by another user, all newly opened windows and programs will also be available for other participants of the meeting. In this case it is possible, to prohibit general access this way: once again, open Windows Explorer, Windows, and then cancel this mode.

If the remote users have the opportunity to manage common programs through the file open dialog and save the file, they simultaneously have access to the file system of the computer or network.

Keyboard shortcuts used in the management of the overall program, seen as the commands in the program, but not in the menu box where the overall program is running. In the general program shortcuts do not work.

Do not leave the computer unattended, if it holds a general application that can be managed by other users.

If from the total application is run another application (for example, when working with Microsoft Word to open the spreadsheet Microsoft Excel), in this case sharing access to the latest may not be possible.

You can not drag objects to the common application, as from well as the general application on to the desktop.

If you change the window size of general application the mouse wheel (if available IntelliMouse) can not work or not work properly.

If in general the application a the Input Method Editor is used (IME), so that others can include it with their mouse, in this case it is necessary to display the status bar at IME.

If the IME does not support the status bar, or other user can not include IME, it can be done manually.

By clicking anywhere on your desktop, update the window IME during the meeting, if this does not happen automatically.

On a computer that is running other applications with the ability to share or a remote control work with general programs in NetMeeting may be impossible.

When the overall management of the program goes to another user interface elements for managing the shared access (frames and dialogs share, as well as a framework created on other computers) on the user's desktop, which provides shared access, are not shown. When you return controlling all these elements of the interface will again be present on the screen.

A computer running Windows 2000 can be configured to work with multiple languages. In this case, when working together with applications, in Unicode format from a computer of organizer of the meeting, the text will not be displayed properly on remote computers running Windows 2000.

If the computer on which the common application are performed, uses hexadecimal color palette (or a palette with fewer bits), the elements of the gray image on the remote computer will be displayed as green. This applies to the menu items, button bar and status bar.

«**Board**». Included with the NetMeeting program «board» allows multiple users to draw simultaneously on the whole window (see Fig. 2.2.2). The contents of this window is available immediately to all participants of the meeting. When one of

the participants of the meeting opens the window of the program the window is displayed on the screens of all other participants.

With the resolution of 1152x864 and more, application «board» can not run in full screen mode.

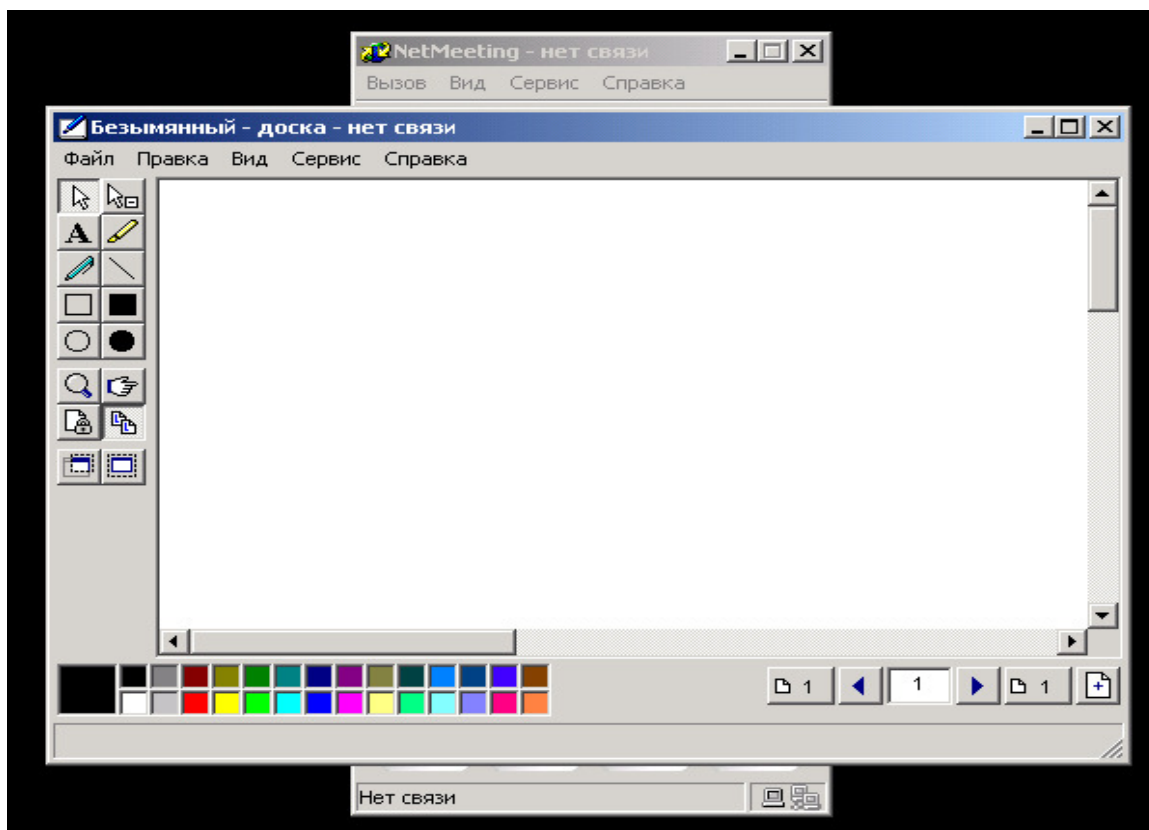


Figure 2.2.2 – Board

When data exchange between participating in the conference computers with Windows 2000 and Windows 95 computers (Windows 98) 15 occurred, recoding two-byte characters (from a set DBCS) may not run correctly.

«**Conversation**». The program «Conversation» allows to enter messages to other members from the keyboard messages to other members (see Fig. 2.2.3). If someone starts an application during the meeting, the corresponding window is displayed on the screens of other participants, who work with NetMeeting 3.0 (or later version of this application).

Users working with the program «Conversation» in NetMeeting 2.11, are not able to close the program, if the other participants in the meeting installed NetMeeting 3.0 (or later).

Which are HTML-files saved by the application can be viewed using a Web browser.

«Conversation» from the NetMeeting 2.x in certain cases can not communicate with the appropriate means in NetMeeting 3.0 (or later).

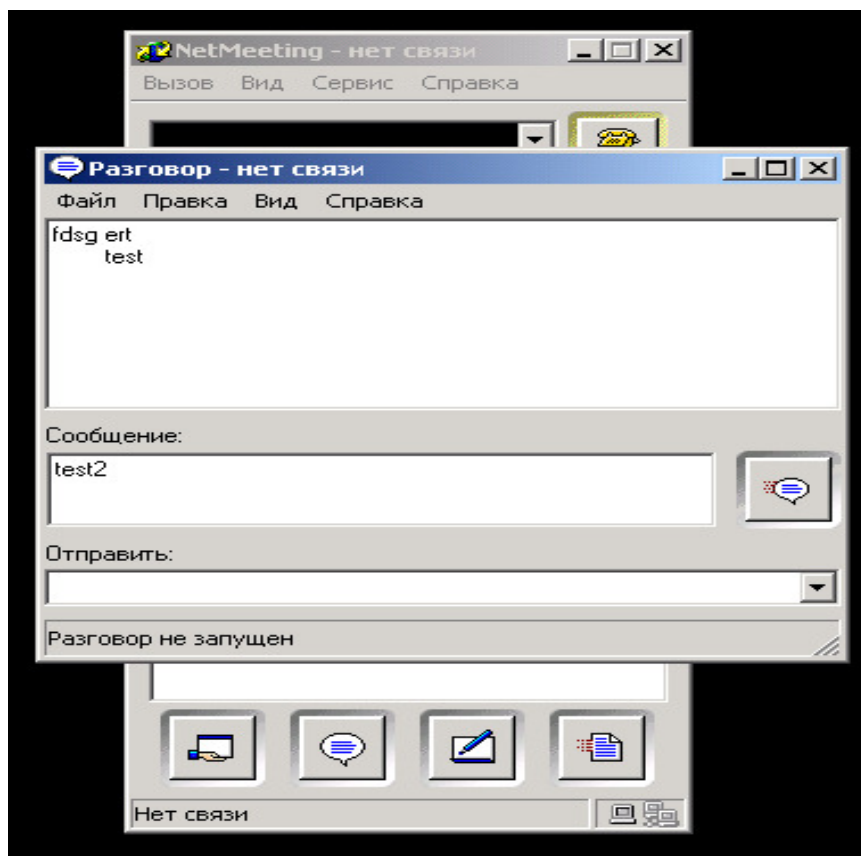


Figure 2.2.3 – Window of message transferring

Sound. For audio connection, a computer that is running the application in NetMeeting, must be equipped with a sound card, speakers and microphone. Communication with audio signal transferring may participate only two users.

The sound quality is highly depend on your sound card and microphone, as well as the quality of the connection.

If you change the sound card driver, for example when you upgrade to a driver that supports full-duplex connection to work properly NetMeeting, wizard sound is required to be set up again (see Fig. 2.2.4).

Restoring audio transmission user by the of NetMeeting 2.0 which had been interrupted during the call, may be impossible. In this case, end the call, and then do it again.

Wizard of sound can give the message that the computer's sound card is not supported. This occurs when the sound card does not offer some features that are required for NetMeeting. Even in this case, the voice link NetMeeting may work, but with the loss of sound quality.

If your sound card is not supported, try to call to the manufacturer, perhaps, for this card new drivers have been issued.

If your computer has motherboard ATI All In Wonder, during the call the microphone may not work and there will not be sound. These problems are eliminated the following way: double-click the location in the state of the speaker icon. In the menu Options, select Properties. Select «Record», then click OK button. Select the microphone as the source of recording.

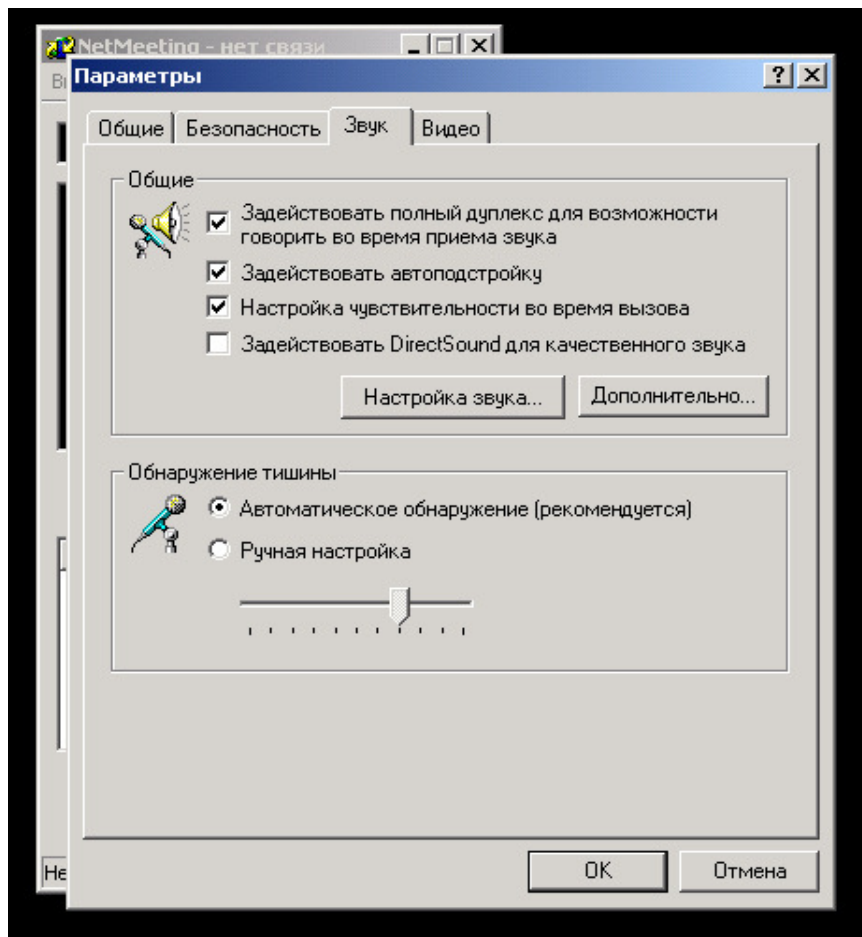


Figure 2.2.4 – Setting of sound parameters

Using the sound card Turtle Beach, Yamaha, SoundBlaster (except the ones based on the types of Ensoniq AudioPCI), Diamond, Crystal, as well as USB speakers Microsoft will harness the power of DirectSound and thus get better quality sound by reducing the signal delay time. By default, this feature is disabled.

The sound quality improve can be achieved by DirectSound activating/switching on.

1. Select Options on the Tools menu.
2. On the Sounds tab, select the Enable DirectSound for quality sound.

If a full duplex sound is intermittent, try switching to half-duplex mode:

1. Make sure that you do not participate in the call of NetMeeting.
2. Select Options on the Tools menu.
3. On the Sounds tab uncheck Enable duplex, allowing to speak when receiving the sound. Do not switch between these two modes during a meeting with a sound bond

Poor sound quality and bad sound card in the annex NetMeeting may be related to hardware configuration or driver installation. To view the latest information about supported software, click the Help menu, click Product Support.

The computer can be equipped with several devices to work with sound. In this

case, you should make sure that the device you selected during sound setup, match the properties of «Multimedia» control panel.

After installing, the new processor, the setup wizard of sound must be re-run.

During the audio conference using NetMeeting, application, in which it is possible to record (eg Microsoft PowerPoint), tries to record. However, since NetMeeting is already using a sound card, in fact, this application sound will not be recorded.

Moving the slider to the right Wave Output Balance (in the appropriate box, Windows) can lead to mute NetMeeting.

If both participants in the call of to the computer are using audio drivers of WDM, at the beginning of a connection signal interference may be heard. In this case, means to disable DirectSound should be switched off/disabled.

1. Select Options on the Tools menu.
2. On the Sounds tab uncheck the Enable DirectSound for quality sound.

Video. To send a video in NetMeeting the computer must be equipped with a video card with a camera or video camera connected to the parallel port (printer port) or to the port USB.

Cameras with video cards are less demanding for computational resources in comparison with cameras that are connected directly to the parallel port.

In the video connection only two users can participate at the same time.

At the speed 28,8 Kbps by default the highest quality of video is used. To change this setting, click the Tools menu, click Options, click the Video tab, and then change the desired parameter in the group Video quality?

Size of the preview window of the video may not match the parameters values that were selected in the dialog «Options».

During a meeting with several participants, video data sending can reduce the performance of all connected computers. So the opening of the video window may interfere with the management of the common application by other users.

If several video devices were installed on your computer was installed, as well as after the improper disposal of such devices from the configuration, the ability to work with video may be absent. If the video device was removed from the configuration in a wrong, way and video in NetMeeting is permitted, the remaining camera software from time to time may issue a warning that the camera was not found (see Fig. 2.2.5).

If working with video applications in NetMeeting the camera is disabled, its software can deliver the message that the camera is not responding. To disable those messages, select the Tools-menu, click Options, click the Video tab, and uncheck Automatically transfer the call.

If you are running other applications that use video tools, video features in NetMeeting may not work.

Violation of color in the video window may be due to poor lighting of the object being sent to the camera. Some video drivers support the filter low light.

When shooting in a dark room, some cameras can significantly slow down computer. Impossibility of preview video with Fig. 5 Setting the video settings

If you are working with video applications in NetMeeting and disable the camera, its software can deliver the message that the camera is not responding. To disable those messages, select the Tools menu, click Options, click the Video tab, and uncheck Automatically transfer the call.

If you are running other applications that use video tools, video features in NetMeeting may not work.

When dealing with the use of video cameras Winnov leads to the automatic switching of input signal. If the video is installed through the connection MXC, a beep will be supplied through the entrance chamber. If the video is set to connect via Composite or S-Video, audio signal will be sent to the line input.

Some cameras through manual adjustment of parameters in dialogs sources and formats (instead of automatic adjustment of the video driver) is to reduce CPU load.

If you use WDM drivers on a computer equipped with a card ATI All In Wonder, means for processing video images in NetMeeting may not work

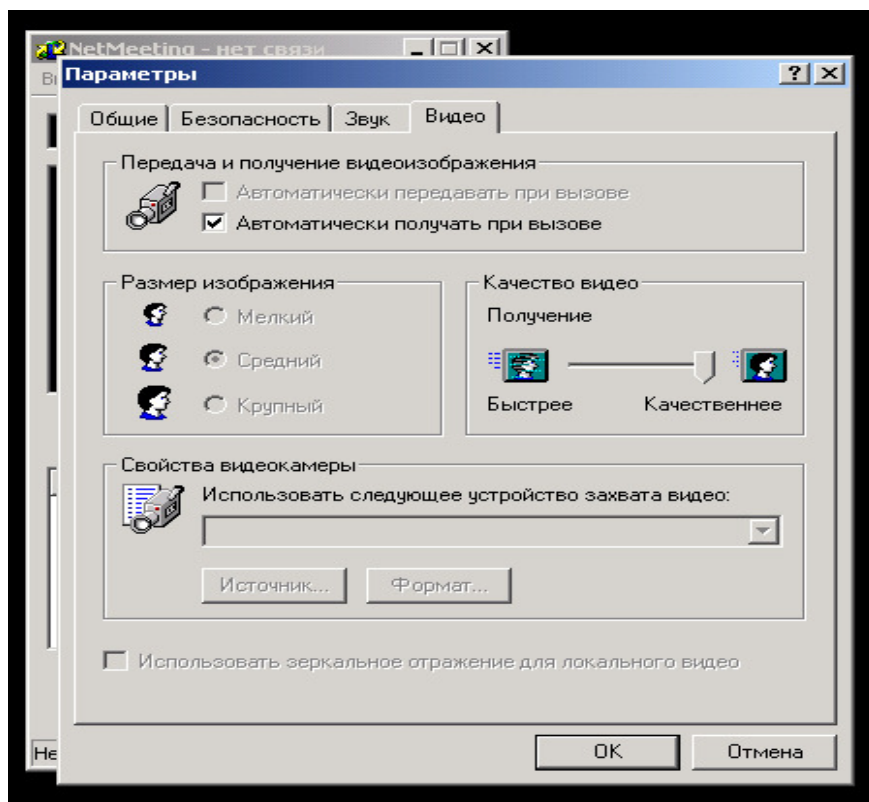


Figure 2.2.5 – Setting of video parameters

Share Desktop. Available in NetMeeting 3.0 (or later) means total access to the desktop allow you to make a call the to call remove the computer that is running the office of public access to the desktop (host computer) and get the access to its programs and folders. After connecting to a remote computer user can handle any file and any applications that are accessible from this computer.

Organization of user's access to the computer through a common desktop does not require the provision of user accounts with administrator privileges. Such access should form a group of users of general desktop NetMeeting «and add the appropriate users.

To remote connection to your computer through the use of general access to the desktop you need to know IP-address of your computer or the name of the called PC. IP-address displayed in the About dialog box (Help menu). When you open the Web page for which NetMeeting is included in the user interface browser, remote access is automatically disabled. They must enabled be manually.

If destination of IP-addresses is done automatically, such as dial-up connection, the remote access server can not continue the session after a temporary disconnection from the network. In this case, you should disable remote access, release and update all the addresses in the setup of IP-addresses in Windows (ipconfig.exe for Windows NT 2000), and then re-enable remote access.

If the application was configured to run automatically at startup of Windows, a general authorization to access the desktop involves the simultaneous disabling automatic start by NetMeeting means. However, the application NetMeeting can not perform this operation correctly. As a result, the next time you start your computer sharing the desktop means will not work. To circumvent this problem, disable the public access to the desktop, switch on automatic start, and then turn it off manually. After this general access to the desktop can be successfully turned on.

If you work with the general access to the desktop to restart the computer running Windows 2000, and then try to log in from a remote computer, the text in dialog boxes, and greeting the login will be displayed incorrectly. The log on to Windows 2000, which includes a facility for general access to the desktop, still possible.

***NOTE.** The text in dialog boxes and greeting logon is displayed correctly if the output of the system was implemented without rebooting.*

If your computer is running Windows 2000, which allowed total access to the desktop, there is support for «standby», this mode is better to off. The «Sleep» transition is performed manually (from the dialog box to completion) or automatically (through the power options in Control Panel).

File Transfer. Transferring files by selecting of corresponding link in Tools menu. Then there is a window to work with receiving and transmitted files (see Fig. 2.2.6).

Security. When the safe call (only for data sending) commands and menu items related to the processing of sound and image, should not be available. In this version however, they remain accessible during the call.

Windows NetMeeting allows you to work only with those certificates, which are represented in the system certificate database Windows. In NetMeeting certificates, received from the personal databases by the browser, can not be used (such as Netscape Communicator 4.5). To work with such a certificate, they should be initially exported from Netscape Communicator, and then imported into Internet Explorer.

At the time of the call security settings dialogs Search of user and 'Call' are unavailable. In addition, if these windows are open during the call, the appropriate

settings in them are unavailable automatically.

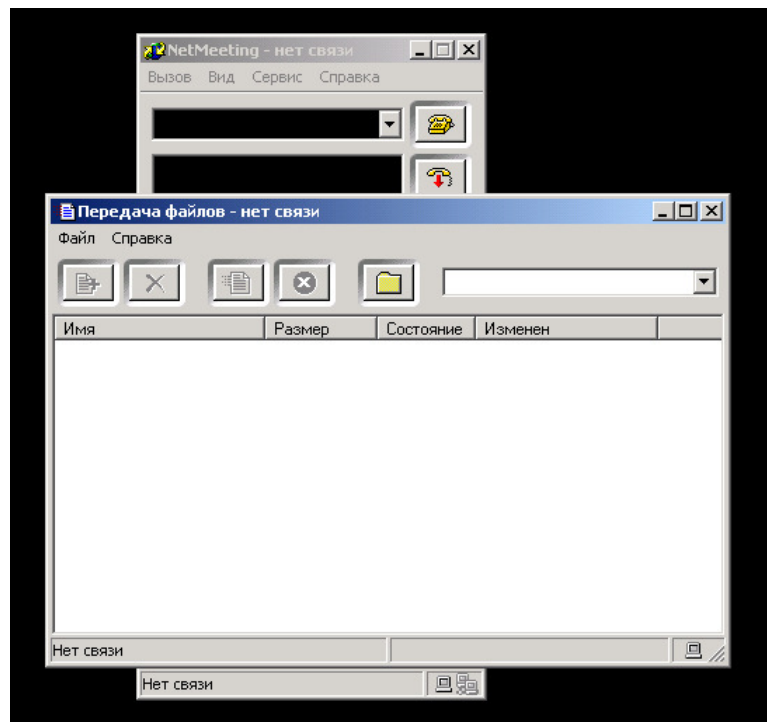


Figure 2.2.6 – Window of files transferring

Special possibilities. Using NetMeeting application, calls can be sent to the system sound-mail the gateway. Keyboard shortcuts for such calls are presented in the following Table 2.2.1.

Table 2.2.1 – Keyboard shortcuts for such calls

To	Use keyboard
Dial the number	CTRL + [number] OR CTRL + [number on digital keyboard]
Press the star button	CTRL + Shift + 8 OR CTRL + [*on digital keyboard]
Press the button with pound	CTRL + Shift + 3

2.3 CHECK-UP QUESTIONS

2.3.1 Give a brief description of existing videoconferences.

2.3.2 The main difference between videoconferencing systems CB, DS, DS.

2.3.3 Describe the software management system DS.

2.3.4 Answer the following questions in written form:

- System requirements.
- Limitations of the system NetMeeting 3.0.
- Sending and receiving calls.
- Share desktop.
- Working with applications.
- Special possibilities.

2.3.5 What is the difference of the videoconferencing «point-to-point» and multipoint conferences.

2.3.6 What are the basic standards used for videoconferencing, and give them a brief description.

2.4 HOME ASSIGNMENTS

2.4.1 To familiarize with key terms and the literature on video conferencing and legacy systems studio, group and desktop (personal) video. Study the Appendix A.

2.4.2 Develop organization chart of personal video conferencing using a local network.

2.4.3 Content of the protocol.

2.4.4 Written reply to the control questions.

2.4.5 Provide wiring.

2.4.6 Bring the algorithm video conferencing point-to-point.

2.4.7 Describe the purpose of windows, buttons and icons.

2.4.8 Draw the algorithm organization conferencing point-to-point using the local network.

2.4.9 Describe the algorithm for video conferencing using the real system NetMeeting 3.0.

2.5 LABORATORY ASSIGNMENTS

2.5.1 Presentation of the video conferencing system laboratory networks. The payload for the organization of a desktop conferencing system includes:

2.5.1.1 Video camera (mounted on a PC).

2.5.1.2 Headphones and a microphone for audio communication.

2.5.1.3 Connectivity to the network.

2.5.1.4 Software for Videoconference.

2.5.1.5 Applied tools to support joint work with data.

2.5.1.6 Personal computer (486 or above).

2.5.1.7 Processing operating system MS Windows (95, NT, 2000).

2.5.1.8 Telecommunication link.

2.5.2 Organization of video window and setting the video.

2.5.3 Organization of videoconferencing in the following modes:

2.5.3.1 Sending call.

2.5.3.2 Board.

2.5.3.3 Conversation.

2.5.3.4 The audio connection for two users.

2.5.3.5 Shared work with applications.

2.5.3.6 Share desktop.

2.5.3.7 Videophone of two users.

2.5.3.8 File transferring.

2.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

2.6.1 The name of laboratory work.

2.6.2 Purpose of the work.

2.6.3 Results of home assignments.

2.6.4 Short description of the work done.

2.6.5 Conclusions about the work done.

2.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 3

THEME: ORGANIZATION OF STREAMING ON A NETWORK USING RTSP PROTOCOL

3.1 PURPOSE OF THE WORK

Investigation the principles of streaming in local networks. Getting practical skills of configuring a multimedia platform Broadcasting RealNetworks.

3.2 KEY PRINCIPLES

RTSP (Real-Time Streaming Protocol) is a protocol of applicable purpose level. Its appointment is to provide possibility for end-users to perform direct control of the flow. RTSP provides an interface that to perform operations such as rewind, scroll, pause and stop. RTSP provides an effective, controlled delivery of queries data in real time applications such as video or audio. Sources of data can be data collection systems of information (for instance cameras) and data storage systems (playing videos). This protocol is appointed for managing the set of sessions in data due of delivery channels (such as UDP, multicast UDP and TCP), and providing choice of delivery mechanism based on the RTP protocol. RTSP is outside strip protocol.

In particular, RTSP-messages are sent separately from the multimedia stream, the packet structure of which is not defined by RTSP protocol. For RTSP-messages a separate port number 554 is used. RTSP service is supported by the set of instructions that the server and client exchange between each other. They are sent in the form of RTSP-packets containing installation parameters for the stream. Here are a few of them:

DESCRIBE. The client requires from the server the presentation or description of the media object, specified in the URL request.

ANNOUNCE. If the instruction is sent from the client to the server, then it describes the presentation or media object specified in the URL request to the server. Submitted in the opposite direction, it updates the session description in real time.

SETUP. Customer requests resources from the server and starts RTSP-session.

PLAY. Client requests the server to start data transmission in the stream, selected by using SETUP.

PAUSE. Client temporarily stops delivery of data without the releasing of the resources.

TEARDOWN. Client requests the server to stop delivering of the specified stream and release related resources.

3.2.1 Principles of streaming organization

Streaming multi media technology first appeared in the mid 90's and was introduced by the products of such companies: as TrueSpeech, VDOnet and Progressive Networks(Now known as RealNetworks). Their first products had very limited capacity, and among all these suppliers only VDOnet company offered streaming video, while the two others were dealing with developing software for

audio broadcasting via the Internet. The main problem at the stage of technology was low quality the offered services. Streaming technology developed quickly enough, and today, producers for streaming media are able to provide image quality comparable to VHS standard with quite reasonable strip of bandwidth (several hundred kilobits per second). Today, for the status of the lead manufacturer of tools for streaming media three companies are competing– Apple Computer, Microsoft and RealNetworks.

You must understand the basic principles of streaming technology multi media to make correct decisions about which products are better to use, how to optimize bandwidth and so on.

The main secret of streaming media technology is buffering player data. A desktop computer with (software) media player provides a connection to the server and requests the stream. The server starts media stream transferring, addressing it to the player. The player, in turn, buffers the information for a few seconds, using the hard drive of the client. With such buffering short delays of streaming are caused by overloading in the network, which do not make discernible effect on the quality of multimedia playback information. And the larger the buffer, the less impact of transmission failures on the quality of network.

Streaming servers can provide continuous access to ready made multi media files. This mode is classified as providing audio or video data on request. Information about the events which are happening at the moment, can be transferred directly by, connected to the computer, microphone or video camera, and then as the media broadcast on the same audience. This mode of transmission of flow is called Web-broadcasting or Webcast technology.

Inside corporation Web-broadcast is often complemented by other features that provide certain types of interactive interaction. For example, you can arrange the issues transferring in real-time for the person whose image is broadcasted by means of streaming video. However, media servers can be also used for emulation of the direct ether. In this case they broadcast reports which have already been saved from the place of events.

More often this streaming media mode – is the transferring of one address flow. It is used in the cases where it is necessary to provide the access to multimedia data for a request. The streaming media server generates separate one address flow for each client, which will request the access to needed resources. Thus, any user can get access to any source of media data any time. Problems arise only when many users simultaneously request access to the same streaming media server, and in this case the total required bandwidth will be needed to calculate based on the sum of all flows. That is, one address speech requires the deployment of the certain bandwidth for each user.

Group broadcasting – an alternative mode of speech, in which a media stream data provides information for many users of this services at the same time. Since the group broadcasting requires much smaller band of bandwidth than the address, it is sometimes used for live broadcast reports from the place of event. Group streaming broadcasting is very effective for the numerous access providing to popular static

multimedia files (for instance, via streaming technology can provide opportunity for all our employees to see the performance of the main director).

Another popular alternative of broad speech technology is called the splitting of the media (splitting). It can be useful, in terms of saving bandwidth, on slow channels. Except that, on public servers it is actively used by internet companies that specialized in content management. The technology of splitting of the media includes two key components: they are a server-source media stream, flow from which the broadcast «Signal» comes out, and the server of splitting, which up was set in a remote area network.

Splitting of the media stream, which is sent from the server source, is happening on the splitting of servers, which retransmits the signal to all their customers. In corporate network it usually looks like this: the server, which is a source of streaming, speech located in one of the divisions which is responsible for the formation of broadcast stream and the transmission through channels of territorial network to remote branches. The servers of splitting receive media stream there, and retransmits it to local customers. So, the territorial network bandwidth is saved because through its channels a limited number of the media transferred to remote servers of splitting.

The software component, that prepares media data for further transmission on the network, is called the Encoder. It converts files with the multi media data or delivers them in real-time format with high factor of compression, which is suitable for streaming speech. For organization of the direct speech from the Webcast server, the encoder sends media stream directly to the media server where it is retransmitted for a group or one address streaming speech. In the stream broadcasting, for a to request, the encoder creates a compressed file, which is copied to a corresponding catalog on the server.

Data compression is the main function of the encoder. Compression formats that previously were used to transfer audio or video information, could only work with delivered files, this is not suitable for streaming absolutely in the conditions of limits on network bandwidth channels. At the beginning of formation of flow technology every manufacturer used their own compression algorithm, as suitable standards for compressing audio and video data did not exist, which would work acceptably for connections with low bandwidth.

Private technologies of data compression appeared in the concurrent competition, despite the fact, that there were already such standards as MPEG and others, developed by the International Union (ITU) and counting the reality of modern packet networks. Today H.263 compression algorithm, adopted by ITU and MPEG-4, is used along with many other methods available in the products of streaming multimedia. However, the manufacturers continue to offer private technologies, which, in their view, provide the best quality and productivity.

In addition to data, transferring it is also important to provide interaction between the client and server and the synchronization of multimedia data. For these purposes the RTSP protocol is used. RTSP (Real-Time Streaming Protocol) – is a protocol of application level of engineering problem group of IETF, which allows to ensure the interaction between the player and server, including the start functions,

temporary stop (pause) and transmission of official transport information, such as, the name of the media stream. RTP specification (Real-Time Transport Protocol) – also IETF- standard are used to transfer multimedia data in real-time UDP protocol. One more record from this set – RTCP (Real-Time Transport Control Protocol) synchronizes the multi media data on the client server and reported to the server about the loss of certain packets.

3.2.2 Software platform for organization of streaming multimedia

For organization of broadcasting of the streaming multi media the special Software is needed. From known systems, such as RealNetworks, Apple Quick Time and Microsoft NetShow, the first one was the easiest to be installed and used, and also it provides the best quality of broadcasting.

The RealSystem complex consists of:

- *RealOne Player* – the program of viewing and listening of RealAudio / Video streams.
- *RealProducer Basic* – the program to convert multimedia files into format of Real Systems, and also on-fly coding and transmission of live audio and video to the server.
- *HelixServer* – actually a server, which distributes the streams of RealAudio/Video.

RealOne Player. Initially at first, the program video for supporting was created for work with audio files. The program for video performing the fourth version was developed. On Fig. 3.2.1 the interface of RealOne Player is submitted. In addition to the usual media-player buttons start /pause /stop there is a for switch compact /normal display, mute and zoom buttons.

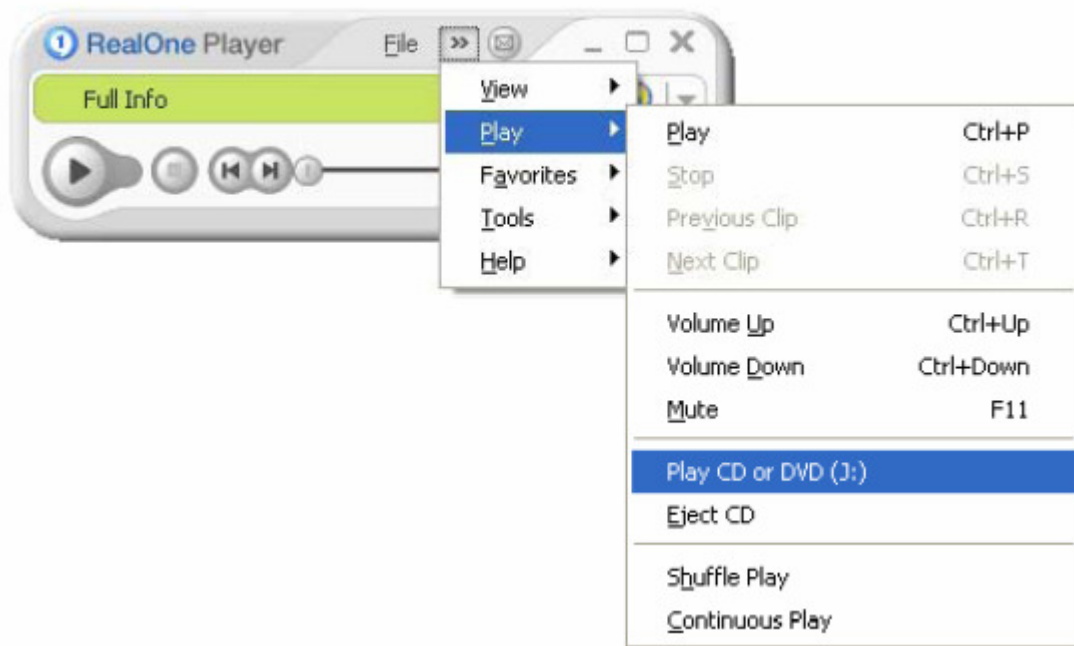


Figure 3.2.1 – Interface of RealOne Player Program

Also through the menu the window of the current connection statistics, can be called cause on which the number of /recovered /lost /later staff, the current bandwidth to the server and so on are depicted/shown.

Undisputed plus of the program is the availability of links to popular sites RealAudio /Video File, so, after the installation of the program one does not have to perform a long search for checking the site work. A menu customize the program: network connection (modem, ISND, LAN), work through proxies, transport TCP / UDP / HTTP, automatic updates and so on.

RealProducer Basic. This program is designed to prepare RealAudio (. ra) and RealVideo (. rm) files and streams. Source input files can be of WAV, AU, AVI and MOV type. You can also encode streams from any audio / video sources (second are needed MS Video for Windows compatibility) and transfer them to HelixServer. The program runs under Windows 95/NT/2000/XP. The Sample of the program is shown in Fig. 3.2.2. Recommended hardware requirements (at least): iP120, 16Mb RAM, 1G disk free space, TrueColor video, 16 bit sound.

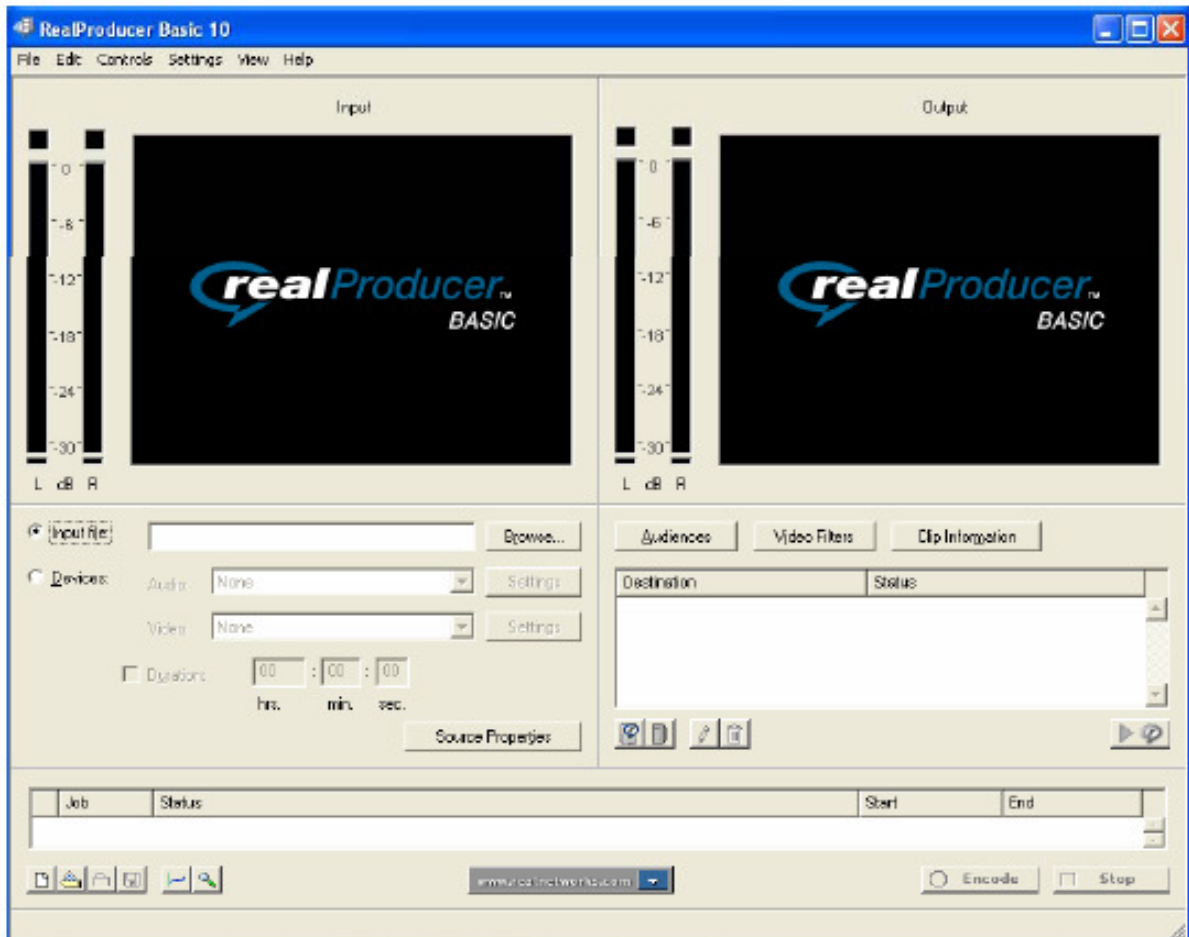


Figure 3.2.2 – The interface RealProducer Basic program

There are three variants of work: encoding from file to file, encoding from media-source into a file, encoding from the media-source and transferring to RealSystem server for online communication.

During the video encoding, you can watch and compare the results with the original. For correct perception is advisable to use quite a fast PC. When encoding live video it is better to ban displaying of these windows. To simplify the creation of media files, several templates (Recording Templates) are offered. You can correct ready or ones add. They indicate encoding settings - speed, codec, settings of quality.

HelixServer. This is the main part of the software RealSystem. There are different versions of this software. They differ by the price and number of simultaneous connections, and service capabilities. HelixServer Basicb is free (but requires Registration by e-mail) and supports up to 25 simultaneous connections. By external signs HelixServer is different from the WWW little or from FTP servers. Run under a Win 9x/NT/2000/XP/BSD/Linux/Solaris. To administer the server functional web-interface that given on Fig. 3.2.3 is used.

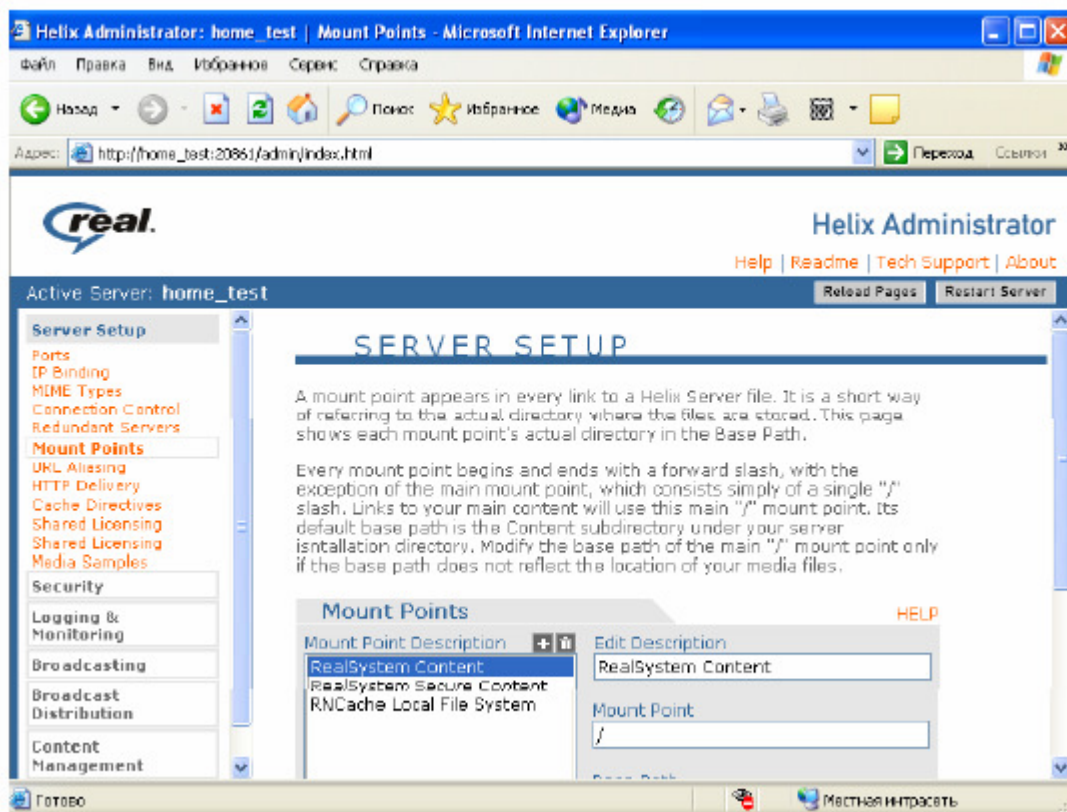


Figure 3.2.3 – Interface of administrative server HelixServer

With it you can also check the server work by playing the test examples (This requires a PC RealPlayer). To check the server work log files can be used and which the server maintains, noticing that that who, what and watched and how well it was performed. Server configuration defined in the text file. Setting features are very wide, however, to start the server a standard configuration file that is included in delivery can be used. Later you can add a user identification, sources of live-streams, setting IP-addresses and ports, to allow or deny entry recoding of broadcasts to user is disk, include message delivery by e-mail about the server work, setting configure performance and etc.

3.2.3 Practical organization of multimedia communication – based on RealNetworks platform

Multimedia on demand. For example service «media on demand» will use two PCs, one as a server and another as a client. And HelixServer and RealProducer Basic software, is installed on the server to client - RealPlayer. Setup is performed by standard ways for Windows-systems, and does not contain any «pitfalls», so let's move directly to the organization of language regime. Initially to get the file format *.**ra** *.**rm**, for that one should use RealProducer Basic, one should do file coding of **test1.avi**. For this we should load this file **test1.avi** into the program RealProducer Basic using menu items **file> open input file> test1.avi**, then we should do the recoding: **controls> encode**. Converted file on default, is stored in the same directory, where the original file was.

In Windows systems server 'HelixServer' is installed in the directory: '**C:\Program Files\Real\Helix Server**'. The directory **C:\Program Files\Real\Helix Server\Content** is the root location for documents. That is, if the multimedia file is located at **C:\Program Files\Real\Helix Server\Content\video\file1.rm**, it is needed to indicate the following address bar: RealPlayer way **rtsp://name_server:554/video/file1.rm**.

No additional settings on the server this mode is required that is why we Just move the file **test1.rm** in the directory **C:\Program Files\Real\Helix Server\Content**, and then on the client computer, RealPlayer is launched. We can get Access to file **test1.rm**. when in the a field 'location Open dialogue' the address enter is entered.

Imitation of live broadcast. To simulate a live broadcast the SLTA utility (Simulated Live Transfer Agent), is served which allows you to broadcast pre-recorded video clips or audio tracks. On Fig 3.2.4 the operation of using the SLTA utilities is shown.

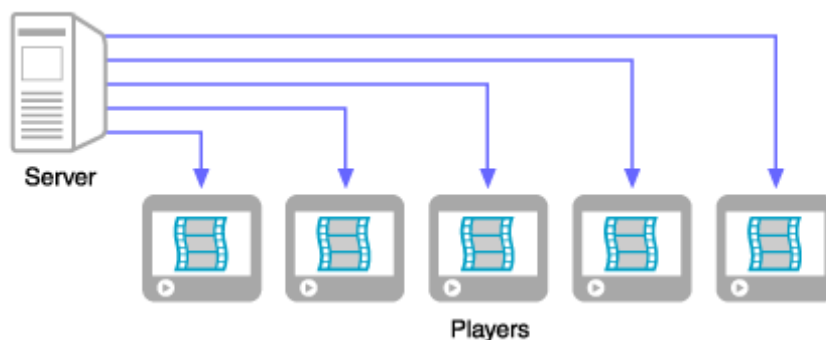


Figure 3.2.4 – The SLTA utility

SLTA is a command line utility, that is included in standard distribution HelixServer. Bellow we consider the simulation procedure.

Receive file **test2.rm**, using methods mentioned above.

Create a directory **Simulation**, in which the files should be copied:

- **C:\Program Files\Real\Helix Server\Bin\slta.exe.**
- **C:\Program Files\Real\Helix Server\Bin\slta.bat.**
- **~\test2.rm****Rysunok 2.4 - Using the SLTA utility.**

The Word Processor Create a file **transmit.cfg** in a text editor:

```
<List Name="BroadcastDistribution">>
  <Var SourceName="Simulation"/>
  <List Name="Destinations">>
<List Name="TestReceiver">>
  <Var PathPrefix="*/>
  <Var PortRange="30001-30020"/>
  <Var Address="127.0.0.1"/>
  <Var Protocol="udp/unicast"/>
  <List Name="Security">>
<Var Type="None"/>
  </List>
</List>
</List>
</List>
</List>
```

NOTE. *That IP-address and port numbers depend on the settings of your system, and having used the names of sources of transmitting stream and others, can be chosen arbitrarily.*

Do the simple server setup. To make this operation, use the interface of administration HelixServer Administrator. On the tab ‘the Broadcast Distribution’ in the Receiver submenu, insert the parameters.

*Transmitter Name Simulation
Transmitter Address 127.0.0.1
Transmitter Netmask 32bit
Security Type None*

Configuration of your server to simulate a live broadcast is shown Fig. 3.2.5:

After that, then open a command line window and move into the emulation directory. Now you need to do the command:

slta.bat -c transmit.cfg live.rm test2.rm

Here **live.rm** is the name of the broadcasting stream.

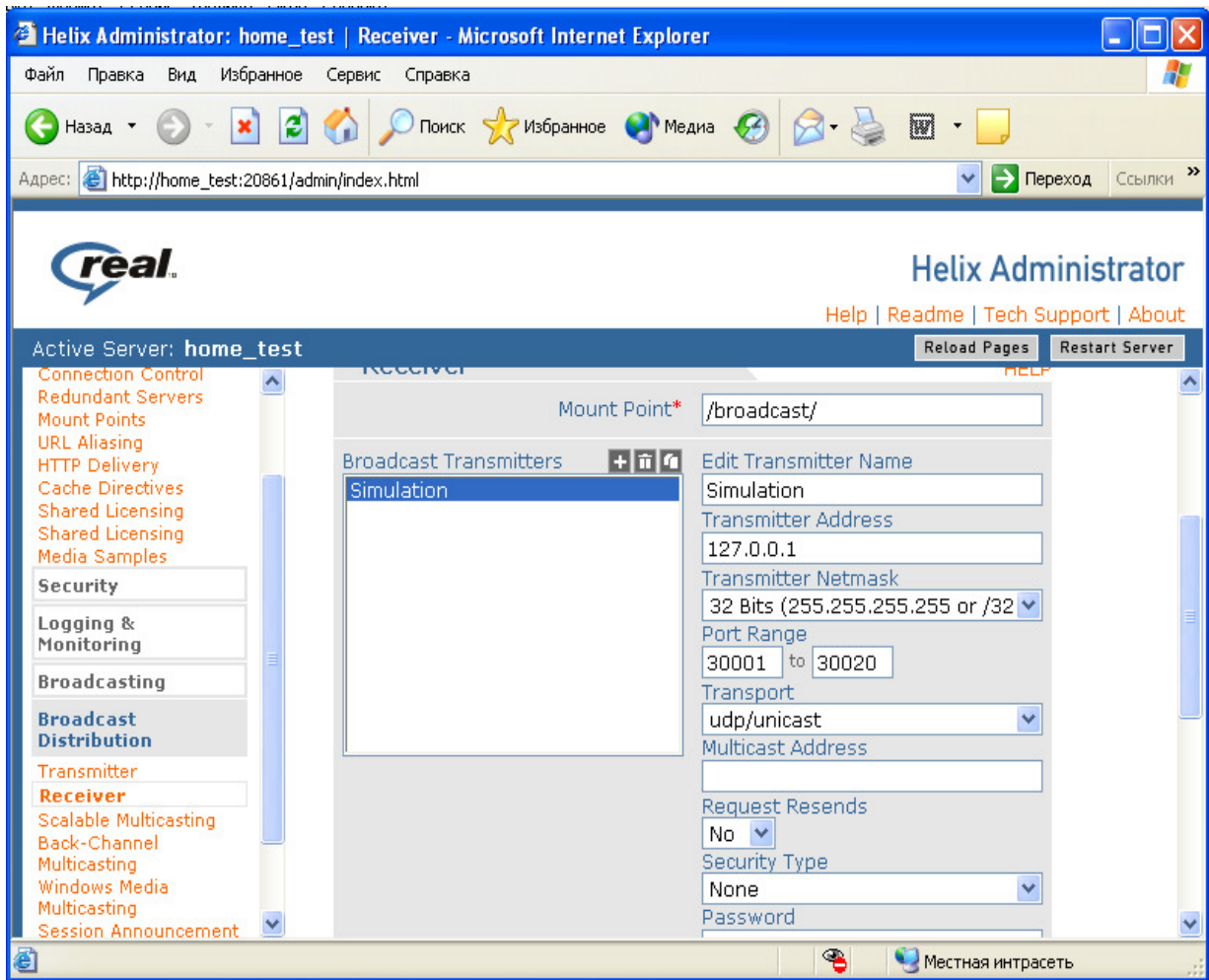


Figure 3.2.5 – Setting up a server to simulate a live broadcast

After that we can get the access to multimedia broadcasting stream, typing the address directly in to RealPlayer on your PC client:

rtsp://127.0.0.1/broadcast/Simulation/live.rm.

Instead of 127.0.0.1, use the network IP- address of the server.

Transmission in real time. To perform broadcasting directly from RealProducer Basic it is needed to establish a connection between it and HelixServer, which is shown in Fig. 3.2.6.

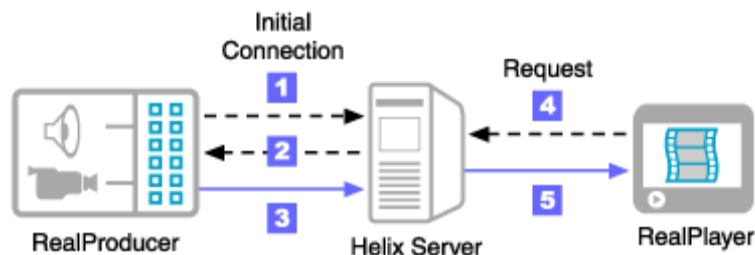


Figure 3.2.6 – Live broadcasting

RealProducer establishes a control connection to HelixServer. At this stage the server provides authentication, connection, checking the correctness of the user's password, on whose behalf the connection is established.

After the user has initialized, the server notifies the client (in this case, RealProducer) the connection options, such as ports, used in connection. After that RealProducer establishes data connection and starts broadcasting.

RealPlayer requests the Media stream on the Server, after that the server sends encoded stream to the client. Consider the settings to be completed for RealProducer Basic (see. Fig. 3.2.7).

It is needed to specify the server parameters to which connection will be established, and namely:

- User name.
- Name of directed speech stream. Usig extension *. rm for constant bit rate, and *. rmvb to variable speed.
- IP-address of the server or it is domain name.
- Port number HTTP on the Server.
- User name and password.

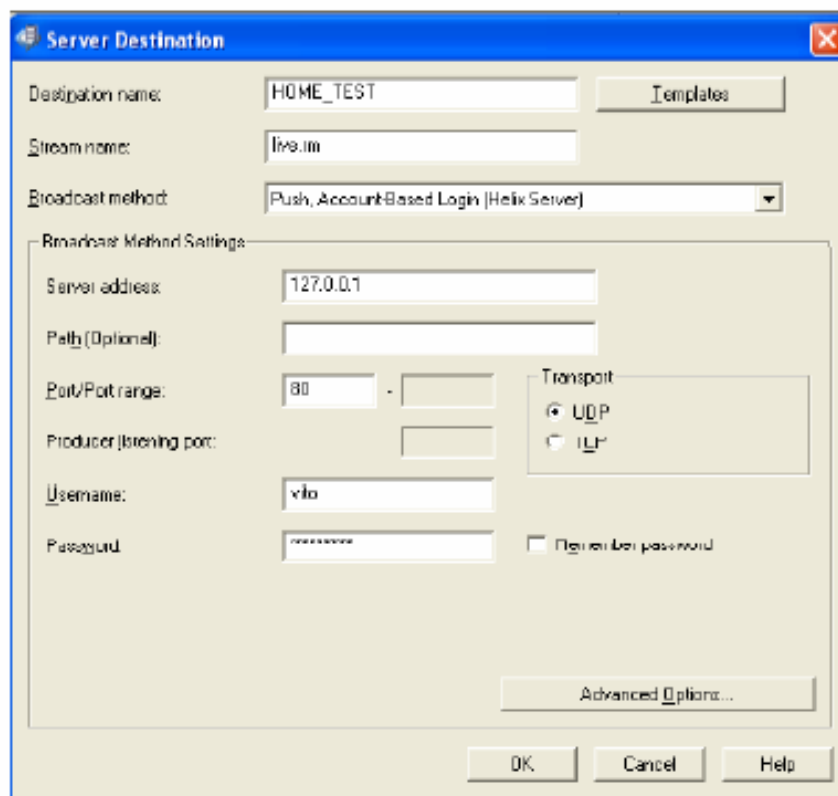


Figure 3.2.7 – Connection setting to HelixServer

It is not required any additional configuration. After that the connection of the Media stream will be held. For example, consider the broadcast voice, which

subtracted from the microphone. For this we activate option 'Devices', and select the device which is connected (Fig. 3.2.8).

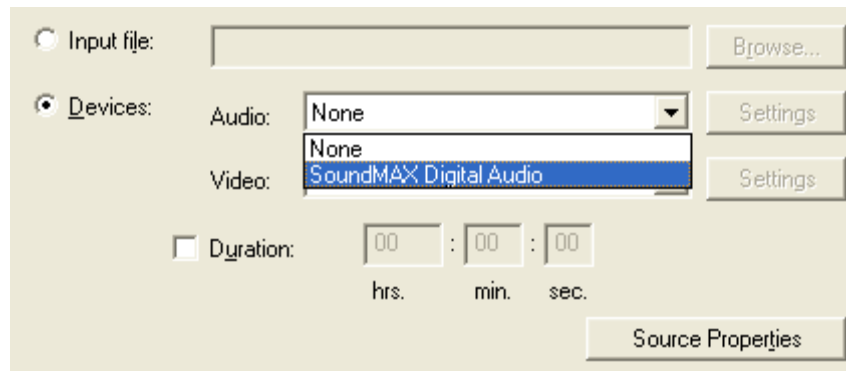


Figure 3.2.8 – Connection setting of outside device

On the Settings tab, you can specify additional connection options. After, that you can perform encode the stream and it is farther broadcasting to the server. At the request of the client, the online stream will be passed to be played on RealPlayer.

3.3 CHECK-UP QUESTIONS

- 3.3.1 Explain the function of RTSP protocol.
- 3.3.2 What are the main instructions which are used for communication between the stream server and clients.
- 3.3.3 Characterize streaming technology.
- 3.3.4 What reason for the broadcasting stream the data buffering is performed?
- 3.3.5 What are the commonly used modes of streaming?
- 3.3.6 What are the differences between on address transmitting and group broadcasting?
- 3.3.7 When is it appropriate to use splitting the media stream?
- 3.3.8 What software components are needed to have streaming communication?
- 3.3.9 What are the function of encoder?

3.4 HOME ASSIGNMENTS

- 3.4.1 Learn the key principles.
- 3.4.2 Prepare answers to check-up questions.

3.5 LABORATORY ASSIGNMENTS

- 3.5.1 Install the software and RealProducer Basic HelixServer onto the server.
- 3.5.2 Install software RealPlayer on client computer.
- 3.5.3 Start HelixServer.
- 3.5.4 Recode test1.avi file in *.rm format using RealProducer.
- 3.5.5 Place the received file in the directory on the server.
- 3.5.6 Get access to that file using program RealPlayer on the client computer.

- 3.5.7 Recode test2.avi file to format *. rm.
- 3.5.8 Run the configuration utility SLTA for HelixServer.
- 3.5.9 Run simulation streaming.
- 3.5.10 Get access to the flow of transmitting using RealPlayer program on the client computer.
- 3.5.11 Connect the signal source specified as an input stream to RealProducer.
- 3.5.12 Set up settings of output stream from RealProducer to enter HelixServer input/entence.
- 3.5.13 Start streaming in the interactive mode.
- 3.5.14 Get access to the broadcasting stream through the transferable Program RealPlayer on the client machines.

3.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

- 3.6.1 The name of laboratory work.
- 3.6.2 Purpose of the work.
- 3.6.3 Results of home assignments.
- 3.6.4 Short description of the work done.
- 3.6.5 Conclusions about the work done.
- 3.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 4

THEME: INVESTIGATION OF MULTIMEDIA TRAFFIC PARAMETERS

4.1 PURPOSE OF THE WORK

Study and run video broadcast on the local network by different protocols and of transmission modes of Unicast and Multicast.

Configure WEB interface media player VLC and start broadcasting by different protocols and transmission modes of Unicast and Multicast, using the WEB interface.

Analysis of packet transmission in a network with different modes and protocols, using software Wireshark.

4.2 KEY PRINCIPLES

New network multimedia applications (applications with continuous data flow) – video, IP-telephony, Internet-radio, teleconferencing, interactive games, distance learning and so on others has been developing rapidly. The requirements for network services in these applications differ significantly from the requirements of elastic applications (such as email, web, remote terminal, sharing files). In particular, many multimedia applications are very sensitive to the duration transit delays and to the delay changes, but allow some amount of data loss.

For networked multimedia applications are especially important some synchronization aspects and stability to data loss.

Aspects, related to the synchronized are important, because many multimedia applications are very sensitive to delay. In such applications packages that are late more than a few milliseconds hundredth practically in vain. However, the network multimedia applications mostly admit the loss of data - these random packet loss causing small crashes when audio-, video- playing and often can be partially or completely masked. These characteristics of multimedia applications, clearly contrasted with the characteristics of elastic applications, such as web, email, FTP and Telnet. For elastic applications long delay does not cause is not causing substantial damage, they are just bad for the user, but the critical importance is completeness and integrity of transmitted data.

4.2.1 Particular features of the multimedia traffic

IP-networks created for the transmission of data traffic, the particular feature of which, is irregularity and the transfer requirement for integrity of transmitted data. For example, the archive file should be transferred with maximum speed and without errors. Data traffic is insensitive to the time-frame. When viewing content of web-site, delay in displaying of the web-page within a few seconds is unimportant.

Multimedia traffic has different character. At transferring multimedia traffic the data must be transmitted at uniform stream. At this, important parameters are the packet delay and delay variance (jitter), while is partial loss of data allowed. It because of, the transmitted information should be played immediately. If at transmitting of audio traffic one packet per second was faded, the user will not notice.

If the packages have a high delay or high delay dispersion, then at the receiving side sound is broken and the quality will be unsatisfactory.

4.2.2 Multimedia traffic types

The set of multimedia applications are transmitted through the Internet (data). There are three classes of multimedia applications: recorded streaming audio and video, streaming audio and real time video, also interactive audio and video in real time.

Recorded streaming audio and video. For this class of applications are related the applications in which the client sends a request to review, that stored on the audio- or video-file server, and its request is transmitted to him, usually, in summary form and is reproduced at once. These files may contain, for instance, audio- and video-recordings of lectures, music, famous radio archives, historical records, full-screen movies, TV shows record, documentaries, video archives of historical events, movies or music videos. This class of applications has three key characteristics.

Storing multimedia data on the device, which stores. Audio or video data is previously written and stored on the server as files . As a result, the user can stop, fast forward or rewind the movie and start playing from the beginning of any part of a film. Time of the system response to such commands must be less than ten seconds.

Stream. In applications recorded streaming audio / video the client can play audio and video in a few seconds after the data begins to come from server. This means, that the client plays are part of the file, while taking over the network its next/other parts. This method of reproduction is called streaming, and allows not to wait for downloading of the entire file (for this a lot of time may be needed) before playing it. There are many streaming multimedia products, including RealPlayer by company RealNetworks, QuickTime of Apple, Windows Media Player of Microsoft Corporation and VLC media player.

Continuous reproduction. Once having begun, multimedia playback should continue as long as the original recording is continuing. This requirement imposes strict limitation on the delay value in data delivery. Data from the server should arrive on time. Although, applications of the recorded media streaming present rather high requirements for data delivery services, limitations, imposed by them, to different delay are not as strict as for interactive real-time applications, such as Internet-telephony or video conferencing.

This class of applications is similar to traditional broadcast radio and television with the difference that the channel is not broadcasted and without a special cable, but via the Internet. These applications allow the users to receive TV or radio programs from anywhere in the world.

As «live» streaming audio and video is not stored on devices that store, the client may not replay forward. However, some applications allow the user to store locally the received data and perform actions such as stop and rewind. There is often a very big broad audience of such radio or television. Data delivery to many clients at once, which accepting the transfer at this point in the same station, can be effectively

done by group IP-routing. As in the case of recorded streaming media, it requires continuous reproduction, but temporarily limitations are not as strict as for interactive real-time applications. Assumed delays are in ten seconds after the moment of the user's request to start playing.

Interactive audio and video real-time. This class of applications enables users to communicate with each other in real time mode. Interactive audio service with real time data transmission via the Internet is often called Internet-telephony, as from a user's view, it reminds a traditional telephone service with switched channels. Internet-telephony can be used for local and long distance telephone service at a very low price. In addition, Internet-telephony allow to ask the deployment of a new services, that are poorly supported by traditional circuit switched networks, such as telephony integration services in web, video conferencing, directory services, subscribers filtering services, and so on. At this moment, hundreds of programs to support Internet-telephony are created. For instance, users of Microsoft's Instant Messenger can make calls from personal computer to a normal phone or from one PC to another. Interactive video connection in real time allows users not only to hear, but also see each other. Today the market offers many software products, that provide interactive video via the Internet in real time, including a program NetMeeting from Microsoft. Note, that in interactive audio and video real-time applications the user can move and speak. For such applications the delay in the delivery data must not exceed a few tenths of a second fate. At voice transmitting which are delays less than 150 ms are not perceived for audience, delays ranging from 150 ms to 400 ms are considered acceptable, and delays exceeding 400 ms, can be perceived as a distortion and lead to indiscriminate speech.

Live streaming audio and video application.

Applications of this class are identical to traditional radio and television, programs difference is the only in the information transfer way.

4.2.3 The concept of quality of service (QoS)

Quality of service is defined as a value of performance of the transmission system that reflects the transmission quality and availability of services. Quality of Service determined by the following factors:

1. *Access service* is a range of time, during which the service is available between certain input and output points with the parameters, specified in service level agreements (Service Level Agreement – SLA). Final goal of high availability corresponds the level 99,999%.

2. *Losses* are expressed as a percentage of rejected packets, that were not delivered to the destination. Without any overload, loss will be zero. During overloads QoS mechanisms determine which packets can be dropped.

3. *Delay* – this is the time the package needs to arrive after the transfer to the destination. If the voice delay is defined as the time of the signal passing from the user what says to the listener.

4. *Delay variation (jitter)*-this is the difference between differ time delay, that occurs during transmission across a network of different packages. For instance, if for

one packet transmission over the network it is needed 100 msec, while to transmit the next packet – 125 msec, then the oscillation in the delay is 25 ms.

Each terminal VOIP (voice over IP) or «Video over IP» has the buffer oscillation delay (jitter buffer), used to smooth oscillation in packet delay. If the oscillation exceed the possibilities of buffer delay, it will work with under downloading (under-run) or overload (over-run). Both of them make negative influence on the quality.

Capacity – available to the user tract of bandwidth, between two points of the operator presence.

4.2.4 Transmission protocol of the multimedia traffic

Appointment of all basic algorithms and protocols is traffic control.

Protocols are a set of rules or procedures that define the discipline for transmission data in packet networks. They provide, in particular, such functions as initialization and the session ends, addressing and packets routing, authentication and / or encryption, perform error correction.

RTP. In IP-networks loss of packets is possible and their order change during delivery. To harmonize the requirements of multimedia applications with features IP-networks, application layer RTP (Real-Time Protocol) has been developed, which designed to data delivering in real time. RTP usually uses UDP, as transport protocol. RTP supports multicasting if multicasting is supported by network level.

RTP itself does not provide timely delivery and does not provide any QoS guarantees. This protocol can not guarantee the correct order delivery data. Recovering data stream may be achieved by the receiving side with the help of sequence numbers of the packets.

In practice, the RTP protocol is used in conjunction with the protocol RTCP (RTP control protocol). RTCP is used for QoS monitoring and transferring of the information about exchange participants during the session.

At organization of audio-conference, each participant must have the address and two ports, one for audio data and one for RTCP-packets, which manage. If necessary, confidentiality of information and packages can be encrypted. At audio conferences each participant sends encoded small sounds fragment duration of 20 milliseconds, each placed in a data field of RTP-packet, which is invested in UDP-datagram.

RTP packet header determines which kind of audio encoding is used, which allows to the sender, if necessary, to change the encoding method. At sound transmission is very important mutual position encoded fragments in time. To solve the task correctly play RTP packet headers contain temporary data and serial numbers. Serial numbers allow not only to restore the correct order of fragments, but also set the number of lost packets, fragments.

As participants can come and go out, it is useful to know which of them is present in the network at the moment, and how they receive the transmitted data. For this purpose, each participant periodically broadcasts via RTCP multicasting

messages, containing the name of the participant and diagnostic data. Also a participant of conference reports through RTCP, if he leaves the session.

If, not only sound is passed but also images, are they are transmitted as two independent streams. RTCP-packets are sent independently for each of these two sessions.

If one of the participants is connected via narrowband channel, then for rate adoption the converter can be installed, called the mixer, close to the narrow area. The mixer converts stream of audio packages in sequence of packets, appropriate opportunities narrowband channel. These packages can be addressed to one recipient or can be multicasted.

Some participants of the conference are not available for IP-multicasting (for instance, are based out of Firewall). For these units use RTP- broadcasting is used. Two translators are installed individually with each sides of Firewall. The external translator sends multicast-package to the internal translator, and the internal translator sends them to the internal network by the normal way.

RTCP. RTP control protocol (RTCP), which manages, is used to manage the RTP-session and based on periodically packet transferring, which manage, to all participants in the session. This protocol has no independent meaning and is used only in conjunction with RTP. RTCP provides control of service quality and feedback in case of overload, as well as identification of the sender.

RTSP application-level protocol allows the user to control media stream. With the help of RTSP protocol, such functions as pause, fast forward / backward, and so on may be implemented. RTSP does not transport data. RTSP is much like HTTP. Each media file is identified by its URL form «rtsp ://...».

UDP. User Datagram Protocol (UDP)– Protocol is for the datagram user) – a transport protocol for data IP networks. Unlike TCP, UDP does not guarantee delivery of the package, so sometimes the abbreviation is decoded as Unreliable Datagram Protocol (Protocol of unreliable datagrams). It allows it to deliver data to applications which are required high bandwidth communication lines more quickly and efficiently, or needed a small time data delivery.

UDP protocol is a major protocol located directly over IP. It provides transportation services for application process, and not much different from services of IP protocol. UDP protocol delivers datagram, but does not require confirmation of its receipting. UDP protocol does not require connection to the module removed UDP («incoherent» protocol). Before the heading of IP-packet, UDP port adds field to the port of the sender address and to the port receiver, that provides multiplexing of information between application processes as well as fields with length and udp-datagram, and checksum which will allow to maintain the data integrity. Thus, if the ip level determine where the package is used address, at UDP level – port number.

TCP. Transmission Control Protocol (TCP) - one of the main Internet network protocols, designed for data communication control networks and subnets TCP / IP. Execute the functions of protocol transport layer of OSI model.

TCP is a transport mechanism, that allows the data stream, from the previous installation of the connection, that gives confidence in the reliability of receiving data, makes a second data request in the event of data loss and eliminates duplication in receiving of two copies of one package (see also T / TCP). Unlike UDP, TCP ensures that the application exactly receives data in the same sequence in which they were sent, without any.

The implementation of TCP, is usually built into the system core, although there is implementation of TCP in the context of application.

TCP is often denoted «TCP / IP». When doing the transmission from computer to computer through the Internet, TCP operates on the top level between two end systems, such as the Internet browser and the Internet server. Also, TCP provides the reliable transmission of byte stream from one program on same computer to a program on another computer. Applications using TCP for e-mail and file sharing. TCP controls the message length, speed of messaging traffic, net traffic.

4.2.5 Streaming

Streaming – is a way to data transfer by small portions (packets), each transferred portion may be used without waiting for the end of the transfer of the entire file.

Streaming allows you to send multimedia information and at the same time provides its reception by user groups, geographically remoted from one another.

Description of streaming is in the following. Transmitted media files are compressed and divided into pieces (packets) and then successively transferred to the user. Packet size is determined by capacity on the network or communication channel between the client and the server, transmitting video signal channel. Having enough saved packets in the buffer, the client program starts playing one of them and simultaneously receives and executes the decompression of next files. The main task, given to the buffer, is to provide a smooth and continuous video playback. In practice, the results of such applications are still very heavily depend on computer speed and the speed of network connection, so the quality of sound / video – it is always a compromise. Stream (bitrate) directly influences to the quality of reproduction; in can we watch video over the network is also mainly depend on it. Stream size can be found in the file properties, but many codecs use dynamic variable bitrate, so, sometimes, even specified value can be false. Worth of this file transferring method is the ability to play the file almost instantly, quickly scrolling forward, start playback from anywhere , terminate or suspend it without consuming time and network resources to fully download the file. The main problem of streaming broadcasts is the quality of reproductive product. Manufacturers are searching for the algorithms that allows you to make intelligent analysis for approximation of (replacement) lost data, hoping thereby to improve the quality of transferring information. This substantiates the absence of common standards among existing programs receiving if a streaming broadcast.

There are two ways to play removed media files:

- Use a PC or other device, capable of working with local and network files.

In this case, it is enough to find in a network file and start playing it. It

plays through the network file system used by your OS. In most cases it will be SMB (Server Message Block), which operates at the upper levels of the TCP / IP stack.

- Use for playing media server and streaming broadcasting protocol, which deliver the media stream from the server to the player. For transfer the stream protocols such as RTP and RTCP used, are used running over UDP.

The difference between them is that TCP / IP provides reliable carriage, but the UDP – not, because TCP has built-in mechanisms to control the carriage and data integrity. However, TCP can not be called the better solution for multimedia transmission, since this protocol adds a large number of service information to the data packets. For TCP, it is important to transmit data accurately, while time delivery is secondary.

On the other hand, UDP uses less overhead than TCP, so it is better suited for applications that work with streaming data, where at first is important the time delivery of information. As for the omissions and distortions of packages, that solving of this problem relies on the receiving side.

4.2.6 VLC media player

VLC media player (Video LAN Client) – is a free mediaplayer. The program works on most modern operating systems.

VLC player can be used as a server to stream broadcast audio / video over a network (support protocols IPv4 and IPv6). To play media files it is not required installing additional codecs, they are «build-in» in the program. VLC can play DVD and streaming unencrypted (free) video (IPTV) and Internet-radio. The program also can record streaming audio / video to your computer.

VLC plays the spoiled or damaged files, such as with damaged indexes.

4.2.7 Transmission Modes

There are three main methods of transmission of traffic in IP-network it – Unicast, Broadcast and Multicast.

Understanding the difference between these methods is very important to understand the benefits of IP-TV and for the practical organization of broadcast video in the IP-network.

Each of the three transfer methods using different types of destination IP-addresses according to their tasks and is a big difference in the degree of their influence on the volume of consumed traffic.

Unicast traffic (single sending packets) is used primarily for services «personal» character. Each subscriber may request a personal video content in arbitrary time convenient to him.

Unicast traffic tends from one source to one destination IP-address. This address belongs to one single computer or subscriber in the network.

The subscriber numbers, that can receive unicast traffic simultaneously, is limited by accessible in trunk part of zone of flow width (flow velocity). For the case of Gigabit Ethernet network, theoretical maximum width of the data stream may be

closer to 1 GBps less bands, necessary for transmission of service information and inventory equipment technology. Suppose that in the main part of the network we can, for example, select no more than half of the band for services, which need unicast traffic. An easy to calculate for the case of the TV channel 5Mb/sec MPEG2, that subscriber numbers of simultaneously receiving unicast traffic does not exceed 100.

Broadcast traffic (broadcast packets transmitting) uses a special IP-addresses to send the same data stream to all subscribers of this IP-network. For example, this IP-address can end in 255, for instance 192.0.2.255, or have 255 in all four fields (255.255.255.255).

It is important to know, that broadcast traffic is accepted by all switched computer which are switched on (or STB) in the network regardless of the user. For this reason this type of transmission is mainly used for service information network level or the other exclusively for the transmission of narrowband information. Clearly, for the transmission of video-data broadcast traffic is not used.

Multicast traffic (multicast packet transmission) is used for streaming video, when it is necessary to deliver video content to unlimited number of subscribers, not overloading the network. This is the most frequently used type of data in IPTV networks, when the same program is watched by a large number of subscribers.

Multicast traffic uses a special class of IP-addresses assignment, such as addresses in the range 224.0.0.0 ... 239.255.255.255. It can be IP-address of D class.

Unlike unicast traffic, multicast addresses can not be assigned to individual computers (or STB). When the data is sent to one of the multicast IP-addresses, the potential receiver of data may decide to accept or ignore them, that subscriber will watch this channel or not. This method of transmission means that most equipment of IPTV operator transmits a single stream of data on many destination. Unlike the case of broadcast transmission, the subscriber has thr choice – accept data or not.

It is important to know that to implement multicast transmission, routers should be in the IP-networ, which support multicast. Routers use IGMP protocol to monitor the current state of distribution groups (namely, membership in a particular group of one or other end-node).

Basic rules of operation of IGMP are the following:

- the end network node sends an IGMP packet type report for starting the process of connecting to the group distribution;
- the node does not send any additional packets at disconnect from the distribution group;
- multicast router, at regular time intervals in the network, sends IGMP requests. This requests allow to determine the current status of distribution groups;
- the node sends a response packet for each IGMP to the distribution group until there is, at least, one client of this group.

Download multicast backbone of the network traffic depends on the number of broadcast channels in the network. In a situation with Gigabit Ethernet network,

assuming that half of the main traffic we can provide for multicast transmission, we get about 100 television channels MPEG-2, each data stream has a speed 5 Mb/sec.

Clearly, in the IPTV network at the same time there are 3 types of traffic all broadcast, multicast and unicast. The operator, planning the optimal bandwidth value, should take into account different mechanisms of influence of various technologies for addressing to IP-traffic. For example, the operator needs to make clear about that services to provide «video on demand», for the large number of customers, are required very high capacity of backbone network. One of the solutions to this problem is the decentralization of the network video servers. In this case the central video server is replaced with several local servers distributed among themselves and close to the peripheral segments of the multilevel hierarchical architecture of IP-network.

4.2.8 Packet analyzer Wireshark

Wireshark (previously – *Ethereal*) – program for the analysis of the Ethernet packet and some other networks (sniffer). It has a graphical interface intended for the user.

Functionality, provided by Wireshark, a very similar to the program of features tcpdump, but Wireshark has a graphical interface intended for the user and many more opportunities for sorting and filtering of information. The program allows the user to view all traffic, passing through the network in real time, moving the network card in cramped mode (promiscuous mode).

The program is distributed under the free GNU GPL license and it uses library GTK+ for the GUI cross platform. There are versions for most types of UNIX, including GNU / Linux, Solaris, FREEBSD, NETBSD, OPENBSD, Mac OS X, and also for Windows.

Wireshark – is the application that «knows» the structure of various network protocols, and therefore allows to parse packets, reflecting the value of each field in the protocol at any level. As for packet capture using pcap, it is possible to capture data only from those networks that are supported by this library. However, Wireshark can work with multiple formats of the initial data, respectively, can open data files captured by other programs that enhances the grip.

4.3 CHECK-UP QUESTIONS

- 4.3.1 Give the definition to multimedia traffic.
- 4.3.2 Name of protocols of multimedia traffic.
- 4.3.3 What is the broadcasting Multicast mode?
- 4.3.4 What special class of IP-addresses is used by Multicast traffic?
- 4.3.5 What is broadcasting Unicast mode?
- 4.3.6 What is the difference between multimedia traffic and data traffic?
- 4.3.7 Name the types of multimedia traffic.
- 4.3.8 What is the difference between an interactive audio and video real-time, and live streaming audio and video?
- 4.3.9 What is QoS?
- 4.3.10 What is the difference between UDP and TCP protocol?

4.4 HOME ASSIGNMENTS

4.4.1 Learn the key principles.

4.4.2 Prepare answers to check-up questions.

4.4.3 Prepare the Table 4.4.1 to fill in.

Table 4.4.1 – Broadcasting Protocol

Time	Source	Appointment	Protocol	Information

4.5 LABORATORY ASSIGNMENTS

4.5.1 Broadcast start (see Fig. 4.5.1).

4.5.1.1 Broadcast starting in Unicast mode.

- Review the VLC player. Start several windows with it.
- Brigade № 1 broadcasts to computer № 2, in this case, the computer server will be № 1 and № 2 computer – the client.
- Start transmission from computer № 1 to computer № 2 over HTTP protocol.
- Open running broadcast on another computer (client). 1.5 Repeat starting broadcast by RTP, UDP and RTSP protocols.
- Execute the same problem, but the machine № 2 will be a service now, and half the team № 1 are the client.

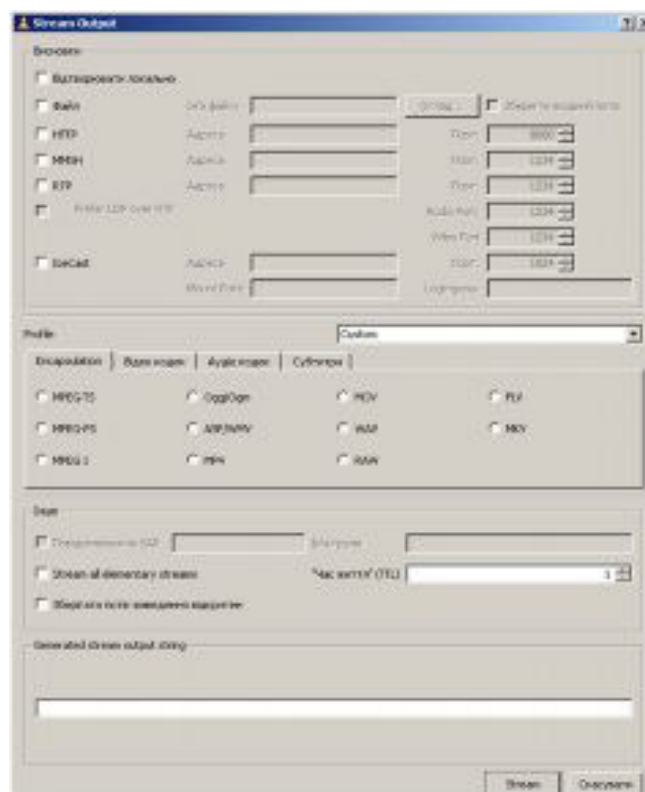


Figure 4.5.1 – Broadcast starting in Unicast and multicast mode by HTTP, RTP, UDP and RTSP protocols

4.5.1.2 Start Broadcast Multicast mode.

- Start broadcasting to another computer over HTTP protocol.
- Media / Open network resources.
- Open bookmark «Network». Choose a network protocol and prescribe IP-address multicast (224.0.0.10).
- Open tab «File» and select the desired file. Click «Play» button.
- Open running broadcast from another computer. Open the tab «Network». Choose a network protocol and prescribe the necessary IP- address (224.0.0.10).
- Repeat start by broadcast RTP, UDP and RTSP protocols.

4.5.2 Management Interface.

Customize VLC server.

- Start VLC player on the server.
- Customize WEB interface VLC media player, in order to be able to manage the server from any machine via WEB interface (see Fig. 4.5.2).
- Start Internet browser (see Fig. 4.5.3).

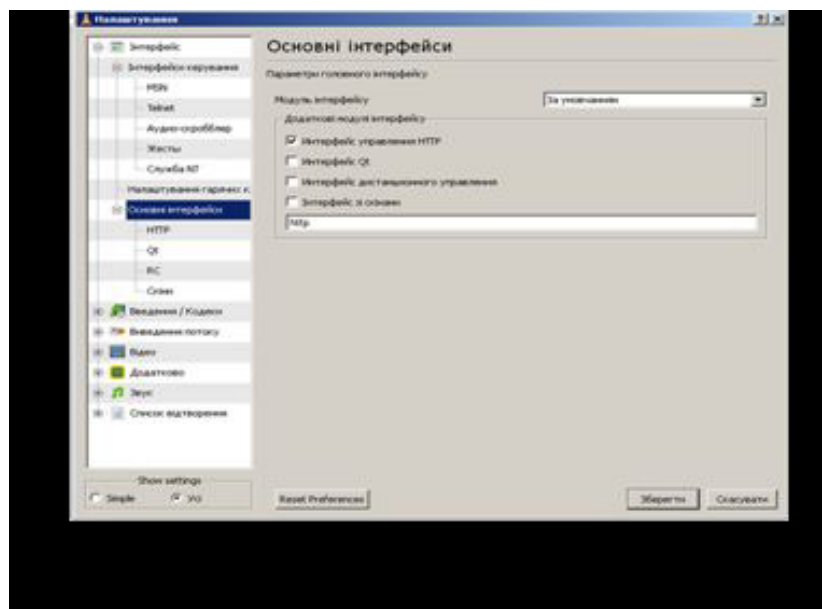


Figure 4.5.2 – Customize WEB interface VLC media player

- Enter the WEB interface of VLC media player (see Fig. 4.5.4).
- Choose stream output menu (output stream) the necessary parameters to adjust.
- Choose the file for review.
- Play the file.
- Repeat setting from the RTP, RTSP and HTTP protocols in Unicast mode.

4.5.3 Analysis of the transmission mechanism by Wireshark (see Fig. 4.5.5).

After completing the previous items, you are familiar with the launch of broadcast video stream to other computers on different network protocols.

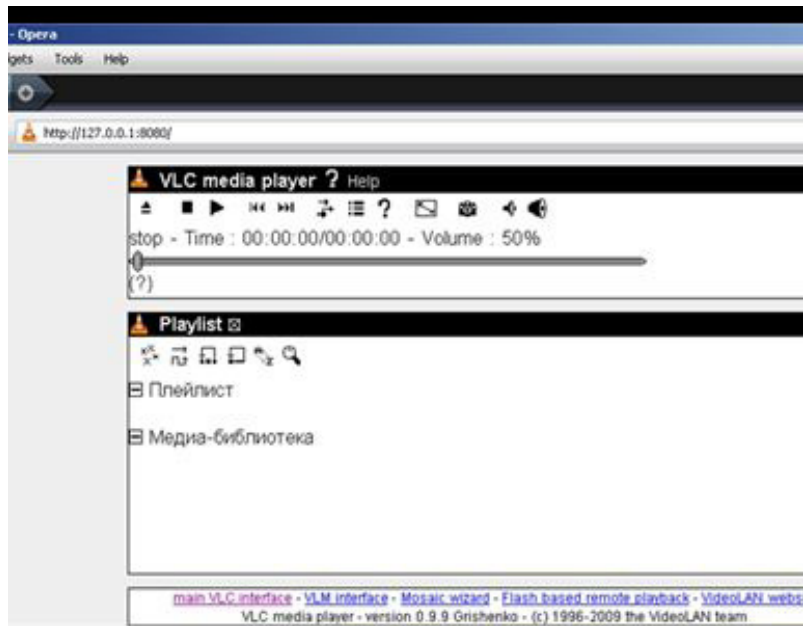


Figure 4.5.3 – Start Internet browser



Figure 4.5.4 – Enter the WEB interface of VLC media player

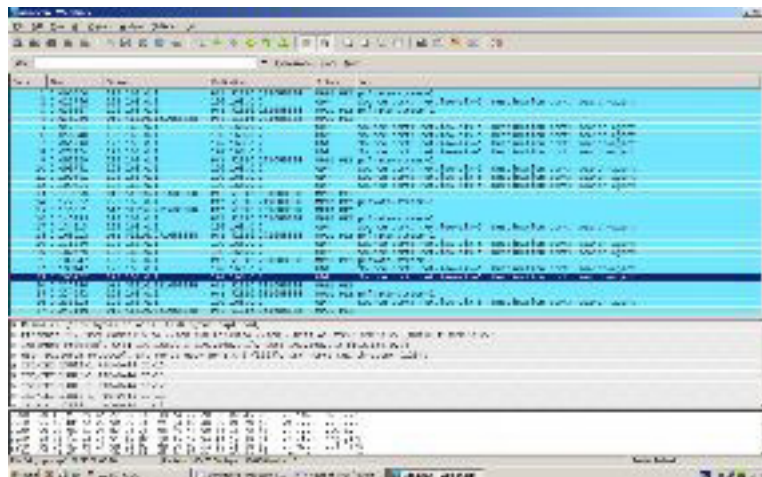


Figure 4.5.5 – Analysis of the transmission mechanism by Wireshark

- Review with Wireshark program. Start it.
- Start broadcasting to another computer by the UDP protocol.
- Once started broadcasting on your computer, start a packet capture

CAPTURE / START.

- Receive a few packages. Press stop.
- Store on record the image of receiving packets.
- Repeat packet capture at startup broadcast RTP, HTTP and RTSP protocols.
- Store on record the packet image in a table form.
- Make a conclusion about differences of receiving package on the basis information, stored in the protocol record.

4.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

4.6.1 The name of laboratory work.

4.6.2 Purpose of the work.

4.6.3 Results of home assignments.

4.6.4 Short description of the work done.

4.6.5 Conclusions about the work done.

4.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 5

THEME: HTTP NETWORK SERVER: WEB – PROCESSOR HTML

5.1 PURPOSE OF THE WORK

Familiarization with the structure of the extended HyperText Markup Language (HTML). Practical skills for working with HTML by creating a web-page.

5.2 KEY PRINCIPLES

HTML (HyperText Markup Language is a «markup language of hypertext») is the standard language of formatting of documents in the World spider web. All of web pages are created through the language of HTML (or his expansions of XHTML).

The language of HTML is interpreted a browser and represented as a document, comfortable for a man.

HTML is *the appendix of SGML* (standard generalized forming language) and corresponds the international standard of ISO 8879.

The language of HTML was developed by British scientist Tim Berners-Lee approximately in 1991–1992 in the walls of the European council of nuclear researches in Geneva (Switzerland). HTML was created as a language for an exchange of scientific and technical documents, suitable for the use of people, who are not specialists in area of make-up. HTML successfully got along at the problem of complication of SGML by determination of a small set of structural and semantic elements (marked out «tags»), which were developed for creation quite simple, but beautifully designed documents.

Besides simplification of the structure of the document, support of hypertext is borne in HTML. Multimedia possibilities were added later. Initially the language of HTML was planned and created as a mean of structuring and formatting of documents without their attachment to facilities of reproducing (reflections). Ideally, a text with markup of HTML has to be without stylistic and structural distortions and be reproduced on an equipment with different technical equipped (coloured screen of a modern computer, a monochrome screen of an organizer, screen of a mobile telephone or a device and a program of the voice reproducing of texts limited on sizes). However, much modern application of HTML is very much far from its primordial task.

For example, tag <TABLE> is intended for creation in the documents of the most ordinary tables, but, as a rule, it will not avail for this purpose. In time, the basic idea of platform independence of language of HTML was given in an original victim modern requirements in multimedia and graphic registration. Text documents, containing a code in language of HTML (such documents have expansion of «html» or «htm», traditionally), are processed by the special applications which represent a document in its formatted kind. Such applications, called as urgent browsers or internetcommentators, usually give a user a comfortable interface for the query of web pages, their viewing (and conclusion on other peripheral devices) and, if necessary, dispatch entered the user of information on a server. Today the most

popular browsers are the Internet Explorer, Firefox, Opera, Safari and Google Chrome.

The official specification of HTML 1.0 does not exist. Before 1995 there was a great number of unofficial standards of HTML. That a standard version differed from them, at once, the second number was appropriated it.

Version 3 was offered by Consortium of the World spider web (W3C) in March, 1995 and provide a lot of new possibilities, such as creation of table, «flowing» around of text images and reflection of difficult mathematical formulas. Even that way, this standard was corresponded with the second version, realization of it was difficult for the browsers of that time.

Version 3.1 was never offered officially, and the next version of standard of HTML was 3.2, in which many innovations of 3.0 version were dropped, but non-standard elements, supported the browsers of «Netscape» and «Mosaic», are added. HTML of version 4.0 contains many elements, specific for separate browsers, but some «cleaning» of standard happened at the same time. Many elements were marked as out-of-date and not recommended (deprecated). In particular, the element of font, utilized for the change of properties of font, was noted as out-of-date (instead of it, it is recommended to use the tables of styles of CSS).

Now Consortium of the World spider web (W3C) develops the fifth version of language of HTML5. The draft variant of specification of the language appeared in the Internet in November, 20 in 2007. Simultaneously, the work is conducted on further development of HTML under the name of XHTML (Extensible Hypertext Markup Language is a «extensible language of markup of hypertext»). While XHTML on the possibilities will confront with HTML, however, produces more strict requirements to the syntax. As well as HTML, XHTML is subset of the language of SGML, however, based XHTML, unlike a predecessor, is on XML.

The variant of XHTML 1.0 was approved as Recommendation of Consortium of the World spider web (W3C) in January, 26 in 2000.

The planned specification of XHTML 2.0 tears compatibility with the old versions of HTML and XHTML, that does not meet arranges some web-developers and producers of browsers heeds and interests. The group of WHATWG (Web Hypertext Application Technology Working Group) is being developed the specification of Web Applications 1.0, often unofficially called as urgent «HTML5», which extends HTML (however, having and consonant with XHTML 1.0 XML-syntax) for the better presentation of semantics of different typical pages, for example, forums, sites of auctions, searching systems, online-shops and ect., which are not successfully very much written into a model of XHTML 2.

In the middle of 1990s there was the next phenomenon. Basic producers of browsers – the companies Netscape and Microsoft – began to inculcate their own sets of elements in HTML-formatting. A mess was created from different constructions for work in the World spider web, accessible for viewing in both browsers. Especially large difficulties were at creation of the cross-browser programs in language of JavaScript. Web- masters had to create few variants of pages or try other devices. For some time the problem lost actuality for two reasons:

a) Because of the Microsoft Internet Explorer browser of ousted all the other browsers. Soy, the problem of web-masters became the problem of users of alternative browsers.

b) Due to efforts of producers of other browsers, which either followed the standards of W3C (as Mozilla and Opera) or tried to create maximal compatibility with Internet Explorer.

On the modern stage it is possible to establish growth of popularity of browsers, followings recommendations of W3C (it Mozilla Firefox and other browsers on the rendering-engine of Gecko; Konqueror, Safari and other browsers on the rendering-of KHTML; Opera with the unique rendering-engine of Presto). Thus Internet Explorer still keeps leading positions.

5.2.1 HTML-document structure

HTML – tag language for documents markup. Every document in HTML language represents an set of elements, where beginning and ending of every element assigns using special sign – *tag*. Elements can be empty, without any text or data (for example, line feed tag `
`). In this case not necessary to use closing tag. In addition, elements can have some attributes, which determine element features (for example, font size for element *font*). Attributes are marked in the beginning tag. Examples of HTML-documents fragments:

- ` text between two tags which are – opening a closing ones. `
- ` Here the element contains the attribute href. `
- `Here the example of an empty element:
`

Register, where the name of element is set as well as and attributes names, HTML has not meaning. Elements can be inserted.

For example, the following code:

```
<b>  
This text will be in bold and this one is bold and in italic type,  
<i>and this - italic type </i_>  
</b>
```

It will give the following result:

This text will be in bold and this one is bold and in italic type

Any HTML-document (that is, Web-Page) is a plain text file, which in addition to the text there are special codes, the text is describing, that is privnosyaschie the document structure.

These codes – tags – are used to break up text on information pieces – **elements** that clearly reflect the structure of information and the relationship between its parts.

Tags for an element recorded as follows:

```
<-name> element content </ element-name>
```

That is, first there is the opening tag – element name in angle brackets, then - the contents of the – any combination of the other elements and text comments, and all ends with a closing tag – the name of the element with the usual oblique angle brackets.

Elements, you can specify any characteristics – *attributes*.

Attributes recorded in the opening tag of the element in the form of pairs of *attribute-name = "attribute value"*. The attribute value can be taken in double quotes «or apostrophes».

In quotes for HTML attribute values can be omitted. In HTML attribute values are always taken in quotes.

Pairing of opening and closing tags is a prerequisite for correct HTML-document.

In HTML elements can not cross. Tag, open the first, closed last, and vice versa. For example, this record is wrong:

In the previous example, we can not say which of the elements – a child, and what - parents – Tel sky. Code should be amended to read:

```
<element-1> <element-2> </ element-2> </ element-1>.
```

It is important to always observe the nesting of elements and prevent them from crossing

Except the elements, in HTML – documents we have entities – «special symbols». The Entities begin from ampersand (&) and has «&name» structure; or &#NNNN; where NNNN – symbols code in Unicode in decimal system.

For example, © – author's rights sign (©). As a rule, entities are used for symbols which are missed in the document code, or for using «special symbols»: < – (<) symbol; > – (>) symbol and so on... symbols which impossible to write in a standard way, because of special meaning in HTML doc.

The list of main tags and special symbols you can find using following link: *HTML elements*. More comprehensive special symbols list is in *Special Symbols*.

Every high end HTML document, must begin from version announcement of HTML <!DOCTYPE...>, as which usually looks like this:

```
<!DOCTYPE HTML PUBLIC «-//W3C// DTD HTML 4.01//EN»  
«http://www.w3.org/TR/html4/strict.dtd»>
```

If this line is not indicated, then it is hard to achieve correct document representation in the browser. After that begin/end of document is marked using tags <html> and </html>

Inside of this tags (<head> </head>) there must be tags of header and (<body> </body>) tags of document body.

5.2.2 Variants of DOCTYPE for HTML 4.01

Strict: does not contain elements, which assign as «deprecated» or «outdated».

```
<!DOCTYPE HTML PUBLIC «-//W3C//DTD HTML 4.01//EN» «http://www. w3.  
org/TR/html4/strict dtd»>
```

Transitional: contains outdated elements for matching and easy transition from old HTML.

```
<!DOCTYPE HTML PUBLIC «-//W3C//DTD HTML 4.01 Transitional//EN» «http://www.w3.org/TR/html4/loose.dtd»>
```

With Frameset: the same as transition it, in addition contains tags frame creation.

```
<!DOCTYPE HTML PUBLIC «-//W3C//DTD HTML 4.01 Frameset//EN» «http://www.w3.org/TR/html4/frameset.dtd»>
```

Table starts with and ends with tags <TABLE> label </TABLE>. Label may include several attributes:

Align. Sets the location of the table in relation to the fields of a document. Valid values are: ALIGN = LEFT (left-justified), ALIGN = CENTER (center alignment), ALIGN = RIGHT (right justified).

Width. The width of the table. It can be specified in pixels (eg, WIDTH = 400) or a percentage of the width of the page (for example, WIDTH = 80%).

Border. Sets the width of the outer frame table and cell in pixels (eg, BORDER = 4). If the attribute is not set, the table is displayed without a frame.

Cellspacing. Sets the distance between the borders of table cells in pixels (eg, CELLSPACING = 2).

A table can have a title (<CAPTION> ... </CAPTION>), although the title is not mandatory. The label can include <CAPTION> attribute ALIGN. Valid values: <CAPTION ALIGN=TOP> (title is placed above the table) and <CAPTION ALIGN=BOTTOM> (header is placed under the table).

Each row begins with a label and ends <TR> label </TR>. <TR> Label can include the following attributes:

Valign. Sets the vertical alignment of the text in the cells of the line. Valid values: VALIGN = TOP (aligns the top edge), VALIGN = MIDDLE (center alignment), VALIGN = BOTTOM (aligns the bottom edge).

Each cell in the table starts with and ends with tags <TD> label </TD>. <TD> Label can include the following attributes:

Nowrap. The presence of this attribute means that the contents of the cell to be shown on one line.

Colspan. Sets The «Spread» Of The Cells Horizontally. For example, COLSPAN = 3 Means that the cell extends to three columns.

Rowspan. Sets the «spread» of the cells vertically. For example, ROWSPAN = 2 means that the cell spans two rows.

Height. Sets the height of the cell in pixels (eg, HEIGHT = 40).

If a table cell is empty, it is drawn around the frame. If the cell is empty, and the frame is needed, you can enter the cell character object (non-breaking space – non-splittable space). The cell will remain empty, and the frame around it will.

5.2.3 Execution template of HTML documents

Template of HTML document with its browser interpretation you can see below (see Fig. 5.2.1).

```

<HTML>
<title>HTML-Table-pattern </title>
<BODY bgcolor='#FFFFCC' >
    <CENTER>
    <TABLE BORDER=5 WIDTH=700 BGCOLOR='#DDDDFF'>
        <TD ALIGN=CENTER> <FONT COLOR=BLUE SIZE='5'> <B> TABLE OF
DATA </TD>
    </TABLE>

    <TABLE BORDER=5 WIDTH=700 BGCOLOR=WHITE>
        <TR bgcolor='#CCCCCC'>
            <TD WIDTH=150 ALIGN=CENTER> <FONT FACE=ARIAL> <B> COLUMN1
</TD>
            <TD ALIGN=CENTER> <FONT FACE=ARIAL> <B> COLUMN2 </TD>
            <TD ALIGN=CENTER> <FONT FACE=ARIAL> <B> COLUMN3 </TD>
        </TR>
        <tr> <td bgcolor='#CCCCCC' ALIGN=CENTER><B> Cell (1,1) </td>
            <td bgcolor='#FFDDDD' ALIGN=CENTER>
                <A HREF=http://chlg-2000.ucoz.ru> Visit our site </A>
                </td>
            <td bgcolor='#DDFFDD' ALIGN=CENTER>
                <LINK> visit our <A HREF=http://chlg-2000.ucoz.ru> site </A>
                </td>
        </tr>
        <tr> <td bgcolor='#CCCCCC' ALIGN=CENTER> Cell (2,1) </td>
            <td bgcolor='#FFDDDD' ALIGN=CENTER> Cell(2,2) </td>
            <td bgcolor='#DDFFDD' ALIGN=CENTER> Cell (2,3) </td>
        </tr>
        <tr> <td bgcolor='#CCCCCC' ALIGN=CENTER> Cell (3,1) </td>
            <td bgcolor='#FFDDDD' ALIGN=CENTER> Cell(3,2) </td>
            <td bgcolor='#DDFFDD' ALIGN=CENTER> Cell(3,3) </td>
        </tr>
    </TABLE>
</BODY>
</HTML>

```

TABLE OF DATA		
COLUMN1	COLUMN2	COLUMN3
Cell(1,1)	Visit our site	Visit our site
Cell(2,1)	Cell(2,2)	Cell(2,3)
Cell(3,1)	Cell(3,2)	Cell(3,3)

Figure 5.2.1 – Template variant view

5.2.4 Template of HTML hyperlink

1). <A - **anchor** (якорь, привязка)

`Visit Our Site` **Results:**

- [Visit Our Site](http://chlg-2000.ucoz.ru/)

2). <LINK> - ссылка

<LINK> Visit our `site` - Visit our [site](http://chlg-2000.ucoz.ru/)

5.2.5 Base colors template

HTML COLOR CODE CHART		
Blue	#0000FF	
Black	#000000	
Red	#FF0000	
White	#FFFFFF	
Green	#008000	
Purple	#800080	
Yellow	#FFFF00	
Orange	#FFA500	
Violet	#EE82EE	
Silver	#C0C0C0	
Gold	#FFD700	
Gray	#808080	
Pink	#FFC0CB	
Fuscia	#FF00FF	
Light Blue	#ADD8E6	
Sky Blue	#87CEEB	
Aqua	#00FFFF	
Khaki	#F0E68C	

5.2.6 Individual tasks variants:

MD2 of Name Surname (variant 1)		
COLUMN1	COLUMN2	COLUMN3
Row 1	Year	2007
Row 2	Date	November 29
Row 3	Time 15.30	Visit our site

MD2 of Name Surname (variant 2)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Visit our
Row 2	Date of birth	site
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 3)

COLUMN1	COLUMN2	COLUMN3
Row 1	Date of birth	?????
Row 2	Address	??????
Row 3	Tel. Number	Visit our site

MD2 of Name Surname (variant 4)

COLUMN1	COLUMN2	COLUMN3
Row 1	Address	?????
Row 2	Tel. Number	Visit our
Row 3	Hobby	site

MD2 of Name Surname (variant 5)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Our Web pages:
Row 2	Date of birth	E-Business
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 6)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	?????
Row 2	Date of birth	Our page
Row 3	Tel. Number	E-Business

MD2 of Name Surname (variant 7)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	See E-Business
Row 2	Date of birth	??????
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 8)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	???????
Row 2	Date of birth	See E-Business
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 9)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Go to the web page
Row 2	Date of birth	Personal computers
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 10)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	See Personal computers
Row 2	Date of birth	??????
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 11)

COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Visit our site
Row 2	Date of birth	Personal computers
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 12)		
COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Refer to E-Commerce site
Row 2	Date of birth	??????
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 13)		
COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	??????
Row 2	Date of birth	Link our site
Row 3	Tel. Number	E-Business

MD2 of Name Surname (variant 14)		
COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	Search in Google
Row 2	Date of birth	??????
Row 3	Tel. Number	???????

MD2 of Name Surname (variant 15)		
COLUMN1	COLUMN2	COLUMN3
Row 1	Year of birth	?????
Row 2	Date of birth	Ask Microsoft
Row 3	Tel. Number	???????

5.3 CHECK-UP QUESTIONS

- 5.3.1 What is a tag language HTML?
- 5.3.2 How to create links to documents and bookmarks?
- 5.3.3 How to change the page background?
- 5.3.4 What is a symbol?
- 5.3.5 What are the protocol headers HTTP?
- 5.3.6 You know what the attributes for text formatting?
- 5.3.7 What are the effects of setting the font?
- 5.3.8 How to insert an image? You know what image formats?
- 5.3.9 How important is the layout? Give an example.
- 5.3.10 How to create a table? Describe the structure and design of the tables.

5.4 HOME ASSIGNMENTS

5.4.1 Learn the key principles.

5.4.2 Prepare answers to check-up questions.

5.4.3 Make protocol of general provisions: Web-document technology with HTML using.

5.5 LABORATORY ASSIGNMENTS

5.5.1 Create on the desktop text document named as *Ivanov.txt*

5.5.2 Write the following in your document:

```
<HTML>
```

```
Ivanov - My first html document
```

```
</HTML>
```

5.5.3 Save your file using *.html* extension: *Ivanov.html*. Delete *Ivanov.txt*

5.5.4 Open your file using *MS Internet Explorer*.

5.5.5 Using the example (scripts and visual image of the document which is given on p. 5.2.3.) create your document (according to your individual task variant). Show to your results teacher.

5.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

5.6.1 The name of laboratory work.

5.6.2 Purpose of the work.

5.6.3 Results of home assignments.

5.6.4 Short description of the work done.

5.6.5 Conclusions about the work done.

5.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 6

THEME: WEB DESIGN AND WEB HOSTING

6.1 PURPOSE OF THE WORK

Practical skills for working with HTML by creating a web-site on the server UcoZ.

6.2 KEY PRINCIPLES

Computer, which shows web-page on subscribers demand, and also makes many another functions, is called an Internet server (also called a server, web-server, http-server). When your computer communicates with server and the computer receives all needed data, when communicate with server, for example web-page code. In this situation your computer called «client» while whole system «client-server».

NOTE. Mechanism of information transmission between remote computers, which share resources and subscribers PCs which use it resources, called «client-server» system. Servers can be variable, the main difference is in OS which used for server administration. To data in main part of internet nodes two types of server software are used: Internet Information Server for Windows NT or Apache for UNIX standard. As a rule, server works on line with high throughput. In addition the server must have its own DNS (Domain Name System). Server administrator can change options, accept or prohibit access to resources, connect, tune up and starts some addition programs and functions, such as CGI scripts or SSI applications, this means whole configuration control.

Thematic content of the servers can vary widely depending on the purposes for which they were created, opportunities or fantasy of the owner, and many other conditions. What unites them all, perhaps, is only one thing: a true server must be a fact that among Internet users called the term «information portal» that is, ideally, it is big enough virtual space consisting of a wide variety of topics of smaller size or a certain number of independent projects.

The site, as opposed to server, it does not possess server software. As a rule, it is an integral part of the server, directory on the server computer, despite the fact that most sites have their own domain name.

Another aspect, in which the server and the site varies considerably, – it is their content. The site is a section of the server is fully dedicated to any one topic. Of course, virtually all of the sites include many subsections, each of which can be split up into even smaller components. But in any case, all parts of the site bring together some general idea, semantic orientation, the general style of performance. There are no universal decisions about what topics the site should include, everything depends on the goals set before co-author, and chosen the methods to achieve them. Some semblance of «standard» is probably formed on the official website of the business - here is the mandatory page «about us», which tells the history of the company, its profile about the projects and development plans; page «products / services, providing the visitors with information about what the organization is

engaged, and containing an offer to buy or order any of the goods produced by it, to use its services, but also «Job» with information about specialists required at this time and a list of employment conditions. But in practice there are many perfectly executed sites that contain no above-mentioned thematic headings. Homepage, in most cases, does not even have its own domain.

6.2.1 Server Structure

As mentioned above, one of the key concepts in Internet resources realization is organization of data transmission using «client-server» scheme.

For web-page downloads, client browser sends query to the http-server, after that browser operates with receiving data. In the following case, browser work is to send a query for data from server, download data and image web-page on the screen. Server receives the query, look for needed document data and send the document or information about error (if this file was not found or it with limited access) to client. It is very important that server does not analyse transmitted file contain. Searching of queried page can be performed only in specified directory, which reserved only for this site – the link for this directory is a part of site address. In the case when a query is directed not on the exact document, but on the whole site, http-server automatically redirects on to start pages, which has name index.html. This document is stored in the root directory. All the other files can be stored in same directory or in attached directories.

Besides the subfolders, which you have created and in which you are free to put almost any content you need, server directory usually contains a few directories that should be mentioned separately.

At first, this is CGI-BIN, where CGI-scripts and other launched from your site interactive applications, as well as several service directories required for the proper operation of the server. At the initial stage, they simply should be ignored. Sometimes in the same directory that stores index.html, there are a number of additional files: not_found.html – a document that appears when the http-server can not find the requested by user file, forbidden.html – appears as an error message, if access to the requested document is denied, and finally, robots.txt – a file that describes the rules in a special way of indexing your site by search engines.

In most cases, especially when publishing home page on the servers that provide free hosting, for service directories and the CGI-BIN directory, access to users is locked, changing the contents not_found.html and forbidden.html files also is not possible. It should be noticed that if you plan to include in your resource an interactive content that requires at least the possibility to put the files in a service folder. In some cases you may not be allowed to create subdirectories on the server, then the user would have to settle for only one directory, allotted to your needs.

From the foregoing it is clear that the client browser can only receive and process information from the server, and place and change it – only if file uploads is implemented on the basis of the HTTP protocol with special CGI-scripts that are included in the web server interface. In other cases we have to use so-called ftp-server, which by special software (its description will be in lesson 4) may transfer

required files, automatically downloading them in a designated directory on your site. In both cases you need to know your login and password to access the system.

You should also remember that most server programs (in particular, Apache for UNIX-compatible platforms) are case sensitive, so all the file names and extensions should be written in lowercase letters, and always in Latin in order to avoid errors. This is due to differences in the encoding process of the Russian language for various servers.

UcoZ – a modern free website management system that operates on the principles of Web 2.0 and allows you to create fairly sophisticated projects for programmers and non-professional users. The control panel allows you to customize the site for different needs. Material Management Site is done directly through the site, making it easier to work with the site. Full access to the code patterns allows to realize various design ideas. System modules can be optimized and customized for a specific project, which allows you to create different types of sites: a simple online business card, a large Internet-representation of the company, a big information portal, etc.

UcoZ System does not need to be downloaded and installed, simply sign up, and the system is at your disposal. For certain skills, you can create websites in 10 minutes. UcoZ Company provides large enough disk space for free. There are a large number of professionally customized designs to choose from. You can have the domain in any zone, for example: `mysite.ru`. If you do not have a domain, you can use the domain, provided by the UcoZ system. You can have a email in domain of your site (`mail@mysite.ru`). Company service provides a file upload via either FTP or the Web-interface. Data backup is provided.

The system has the following pre-configured modules: Users, Page Editor, Site News, Forum, Blog, Gallery, Catalogue of articles, Files,directory, Sites directory, Classified ads, Guest Book, Tests, Questions and Answers,Shoutbox, Polls, E-mail Forms, site statistics.

Assistance in the form of the Forum and FAQ (frequently asked questions) is provided. There are many functions for quick setup of different levels of design complexity, the ability to go into the control panel directly through the site (for example: `http://mysite.ru/admin/`). The client may not know that his site is on UcoZ. There are nocopyrights UcoZ in the control panel, it is possible to disable the copyright and bannerson the site.

6.2.2 Mailbox creation

For creation and registration your own site on Ucoz server its necessary to have mailbox(E-mail) on any server. At this address client receives administrator rights in the creation and registration process. You can see how to create mailbox bellow. Now we use server mail.ru.

Дополнительная информация о пользователе

Ваш пол * Мужской Женский

Ваша страна

Регион

Другие сервисы

Создать персональную страницу на проекте Мой Мир

Защита от автоматических регистраций



Код на картинке * [Не вижу код](#)

Нажимая эту кнопку, Вы принимаете [условия пользовательского соглашения](#).

6.2.3 Registration in Ucoz system

Click on



РЕЕСТРАЦІЯ КОРИСТУВАЧА

Адреса сайту (логін) *: .

Логін може складатися лише з латинських літер, цифр і дефіса [a-zA-Z0-9-]. Мінімальна довжина логіна 2 символи, максимальна - 15 символів.
Увага! Персональний домен, наприклад, **mysite.com**, Ви зможете прикріпити після реєстрації.

Пароль *:

Пароль (підтвердження) *:

Пароль має бути складним, щоб його не можна було підібрати (приклад: "k0i3p9S7"). Пароль може складатися лише з латинських літер, цифр, знаку підкреслення і дефіса [a-zA-Z0-9-_]. Мінімальна довжина пароля 6 символів, максимальна - 15 символів. **Реєстр** букв враховується системою.

Ваша e-mail адреса *:

Ви повинні ввести **робочу** e-mail адресу, оскільки Вам доведеться її **підтвердити**, щоб мати можливість повноцінно працювати з Вашим проектом.

Ваше повне ім'я *:

Країна мешкання *: ✓

Дата народження *: Рік Місяць День ✗

Ваша стать *: ✗

Секретне питання *: ✓

Відповідь на секретне питання *:

Мінімальна довжина відповіді 3 символи, максимальна - 20 символів.
Увага! Не забудьте свою відповідь, вона Вам знадобиться для цілкового управління проектом.

Код безпеки *:


Введіть цифри зображені на картинці в полі зліва від неї.

Згоден з [правилами](#) системи *: ✗

Увага! Сайти, що містять порнографію, зображення сцен насильства або розпусти, пропаганду расової ненависті і нацизму, а також інші сайти, що суперечать законодавству РФ, видалятимуться без попередження.

Fill in a form

РЕЄСТРАЦІЯ КОРИСТУВАЧА

Адреса сайту (логін) *:	<input type="text" value="http://mblack"/> . <input type="text" value="ucoz.ua"/> ✓
<small>Логін може складатися лише з латинських літер, цифр і дефіса [a-zA-Z0-9-]. Мінімальна довжина логіна 2 символи, максимальна - 15 символів. Увага! Персональний домен, наприклад, mysite.com, Ви зможете прикріпити після реєстрації.</small>	
Пароль *:	<input type="password" value="*****"/> ✓
Пароль (підтвердження) *:	<input type="password" value="*****"/> ✓
<small>Пароль має бути складним, щоб його не можна було підібрати (приклад: "kD13p9S7"). Пароль може складатися лише з латинських літер, цифр, знаку підкреслення і дефіса [a-zA-Z0-9_]. Мінімальна довжина пароля 6 символів, максимальна - 15 символів. Рєєстр букв враховується системою.</small>	
Ваша e-mail адреса *:	<input type="text"/> ✓
<small>Ви повинні ввести робочу e-mail адресу, оскільки Вам доведеться її підтвердити, щоб мати можливість повноцінно працювати з Вашим проектом.</small>	
Ваше повне ім'я *:	<input type="text"/> ✓
Країна мешкання *:	<input type="text" value="Україна"/> ✓
Дата народження *:	<input type="text" value="1988"/> - <input type="text" value="Грудень"/> - <input type="text" value="14"/> ✓
Ваша стать *:	<input type="text" value="Чоловічий"/> ✓
Секретне питання *:	<input type="text" value="Кличка домашньої тварини"/> ✓
Відповідь на секретне питання *:	<input type="text"/> ✓
<small>Мінімальна довжина відповіді 3 символи, максимальна - 20 символів. Увага! Не забудьте свою відповідь, вона Вам знадобиться для цілкового управління проектом.</small>	
Код безпеки *:	<input type="text" value="437578"/>  ✓
<small>Введіть цифри зображені на картинці в полі зліва від неї.</small>	
Згоден з правилами системи *:	<input checked="" type="checkbox"/> ✓
<small>Увага! Сайти, що містять порнографію, зображення сцен насильства або розпусти, пропаганду расової ненависті і нацизму, а також інші сайти, що суперечать законодавству РФ, видалятимуться без попередження.</small>	
<input type="button" value="Зареєструватися"/>	

Registration complited

ВХІД У ПАНЕЛЬ КЕРУВАННЯ

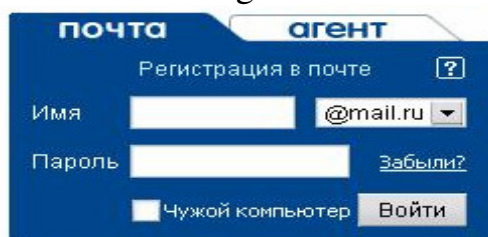
Спасибі

Реєстрація в системі UcoZ була успішно завершена.

Скористайтеся формою знизу для входу в Адмін центр.

Don't close page for control panel enter.
After this necessary to confirm e-mail address.

For mail viewing:



почта агент

Регистрация в почте ?

Имя @mail.ru

Пароль [Забыли?](#)

Чужой компьютер

Fill the fields name and password.

Dear, Косня.

Somebody used this e-mail to register at UcoZ Web Services. If it were you then continue reading. our apologies.

This letter has been sent to this e-mail address (crazycom@icn.od.ua) for its verification.

To verify e-mail click on the link: <http://s15.ucoz.net/panel/?a=cem&t=491d1a18ed0032112b6f7727112397e22807dcl274d86d04d1a7a790edd24be018bcc7ee33>

or enter the following code in "Confirm e-mail" section of the Control Panel:

Verification code: 609956313

Click on «To verify e-mail click on the link «

[Thank you. Your e-mail has been confirmed.](#)

Enter in the control panel

[ВХІД У ПАНЕЛЬ КЕРУВАННЯ](#)


Спасибі

Реєстрація в системі UcoZ була успішно завершена.

Скористайтеся формою знизу для входу в Адмін центр.

Логін *:

Пароль *:

Код безпеки *: 

Введіть цифри зображені на картинці в полі зліва від неї.

[Забув пароль](#) [Реєстрація](#)

6.3 CHECK-UP QUESTIONS

6.3.1 What are features of the system Ucoz?

6.3.2 On what programming language is written system Ucoz?

6.3.3 What are you still know of a free system to create website?

6.3.4 Is it possible to create an online store in the system Ucoz?

6.3.5 What is the maximum size of an uploaded file to the server FTP in the system Ucoz?

6.3.6 How many megabytes of disk space allocated in system Ucoz?

6.3.7 Can we set own PHP or Perl scripts and to use MySQL?

6.3.8 Where you can change the data generated site – for example time zone or name of the website?

6.4 HOME ASSIGNMENTS

6.4.1 Learn the key principles.

6.4.2 Prepare answers to check-up questions.

6.5 LABORATORY ASSIGNMENTS

6.5.1 Create mailbox in mail.ru (if haven't own mailbox).

6.5.2 To make registration in Ucoz .

Save whole site authors data, because this will be inaccessible in future:

Login Control Panel

Password panel

FTP host name

Login Host FTP

Host FTP password

The answer to the security question

Moreover, from Ucoz mail, save the following links:

– *To enter the control panel;*

– *To enter the administrator*

One more save:

– *name and password to access your mailbox*

The fullest rights have access to the control panel. Administrator rights lower compared with control panel rights. For example, *administrator cannot delete site pages or whole site module.*

6.5.3 Every student should create his own website with domain name like Alexander_Ivanov. The site logo (on any page) should be the name of the type Alexander Ivanov Site .

6.5.3.1 Home page should contain a brief appeal to its readers (briefly about yourself, your interests, hobbies). Specify the details of communication (email or phone, your photo if you want).

6.5.3.2 Create 5 pages of your website:

1. *Academic background*

2. *Discussion*

2.1 *Part 1 (My thoughts on the subject of TIN)*

2.2 *Part 2 (My check-up questions and answers on TIN)*

3. *Facts and events*

On each of these pages make correspondent header in the middle of page field. Use blue, size 4, italic for Main Pages and size 3 for Part without italic.

Create page it can be in administration mode:

«Add» – «Page Editor» – enter page name, enter header text indicate font parameters.

«Save» – «Go to page» – be sure that page created, and header entered.

Page editing in admiration mode possible to activate «*Control block*» mode (little triangle icon on the page field); its works in two edit modes:

- a) visual editor (same as WORD)
- б) using codes (scripts) of HTML language.

Manu editing: it has to be look like:

1. *Academic background*
 - 1.2 *Part 1 (My thoughts on the subject of TIN)*
2. *Discussion*
 - 2.2. *Part 2 (My check-up questions and answers on TIN)*
3. *Facts and events*

To do this, enter the edit mode of any created page (ex, main), then «*Save*», then use the item «*Edit menu*». Choose a visual editor («*eyes*»); in this editor copy the necessary row of page menu to buffer memory (using the keyboard shortcut CTRL + C). Next, insert a row from the buffer to the desired location of the text menu bar, remove an unnecessary string.

«*Save*», Close the window, «*Go to page*» and to make sure the changes are correct.

Remove one page (2.2. Part 2). For this update the home page, «*General*» – «*Manage your account*», enter the password in Control Panel, «*Page Editor*» – «*Manage Pages Site*», in the page table remove the desired page.

NOTE. *This lab can be performed in advance, e.g. from your home PC, and defend the lab during the lab class (you should be able to explain, how everything was performed). After receiving estimates for this work personal site can be closed at the request of the student.*

6.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

- 6.6.1 The name of laboratory work.
- 6.6.2 Purpose of the work.
- 6.6.3 Results of home assignments.
- 6.6.4 Short description of the work done.
- 6.6.5 Conclusions about the work done.
- 6.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 7

THEME: PROVIDING INTERNET – HOSTING SERVICES. DEVELOPING AND MAINTENANCE OF WEB – SITES BASED ON APACHE

7.1 PURPOSE OF THE WORK

Research of the process to install and configure web-server Apache. Getting practical skills in the creation of html-documents.

7.2 KEY PRINCIPLES

Apache Web-server was developed in 1995 by a group of American Centre for Computer NCSA, and is designed for creating Web- nodes. Web-server Apache is the most popular software product for creation of Web-sites. Today, over 65% of all web-sites of the world powered by Apache. The main advantages of Apache, which brought it popularity, are easy to be installed and configured, as well as that it is a freely distributable software product.

7.2.1 Installing the Apache server

To install the Apache server on a computer running Windows 2000/XP, you must run the file **apache_2.0.47-win32-x86-no-ssl.msi**. While starting the screen shown in Fig. 7.2.1 is appeared:

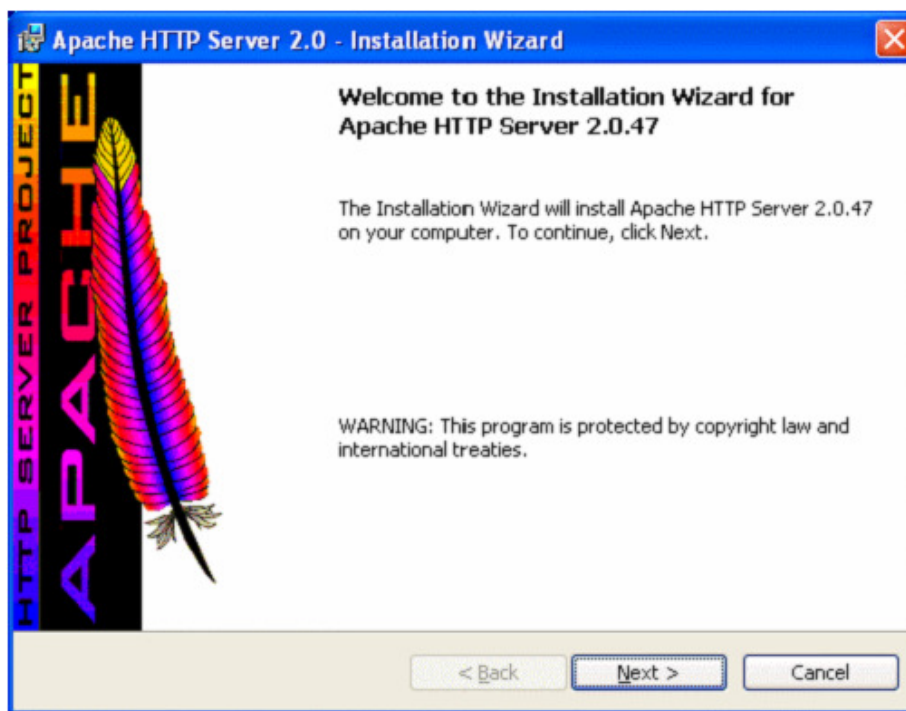


Figure 7.2.1 – The initial window setting of the Apache server

After clicking the 'Next' button the following window appears (see Fig. 7.2.2), in which the license terms of this software will be shown, they are needed to be

agreed – **I accept the terms in the license agreement.** Otherwise, the installation of Apache will be interrupted.

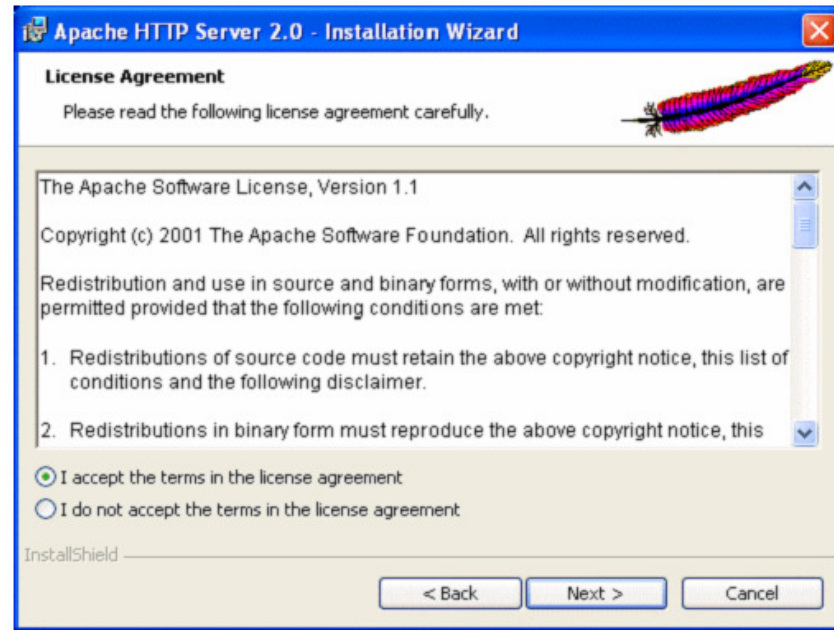


Figure 7.2.2 – License Terms Apache server

In the next window a short information of the Apache display is displayed (see Fig. 7.2.3).

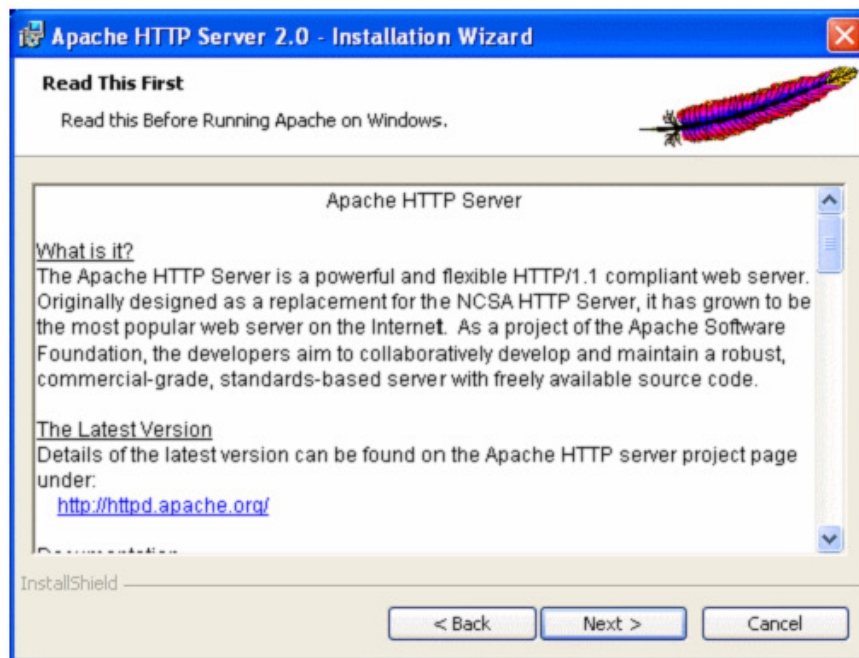


Figure 7.2.3 – Summary of the Apache server

The initial server configuration options are indicated after that (see Fig. 7.2.4).

In the Network Domain the domain name, is specifies providing hosting, for example localhost. In the Server name is the name of the server: localhost.

In the Administrator `s Email Address email address Server Administrator is specified, such as localhost @ localhost or master @ localhost.

Since Apache is the web-server, it uses port 80 Protocol TCP, so when you install the server, you must select the option **For All Users, on 1980 port, as a Service – Recommended.**



Figure 7.2.4 – Initial server settings

In the next window the type of installation web-server will be selected: usual or typical installation (Typical), or Manual Installation (Custom). Select the type of Custom type installation.

Further, in Custom Setup window, you must select **Build Headers and Libraries**, and in the dropdown menu, select **This feature will be installed on local hard drive** (see Fig. 7.2.5). To change the installation directory, press the **Change**, button and select the appropriate directory (the default setting server is carried out in the directory **C:\Program Files\Apache Group\Apache2**).

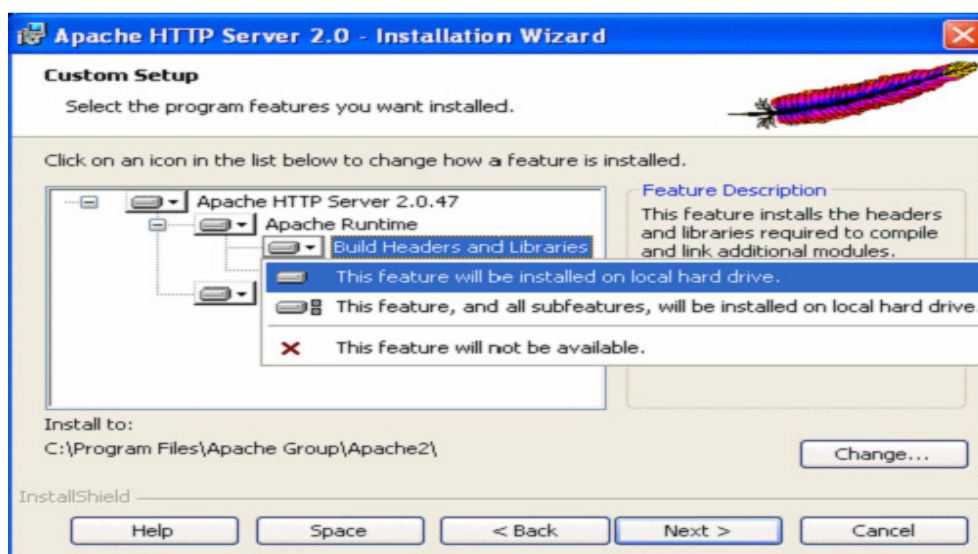


Figure 7.2.5 – Selecting Installation Components

After selecting the installation directory, the window of beginning the installation will be opened, for start click **'Install'**. Upon completion of the installation process you must click **Finish**. After installing the web-server, in the lower right corner of the taskbar, the Apache icon will be shown- the white circle with a triangle inside and a pen (see Fig. 7.2.6).



Figure 7.2.6 – Apache Server icon on the taskbar

Double-click on the icon to open the monitor server, Apache (see Fig. 7.2.7). Apache Server Monitor shows which version of the system is installed, as well as displays control of the operation of the server. After installation is completed, the server must verify the installation and correctness of its work. To test the work a browser must be run to run, and in the address bar to specify **http://localhost**. If the browser displays a window that shown in Fig. 7.2.8, the installation process server is executed without errors, and your server is working correctly.

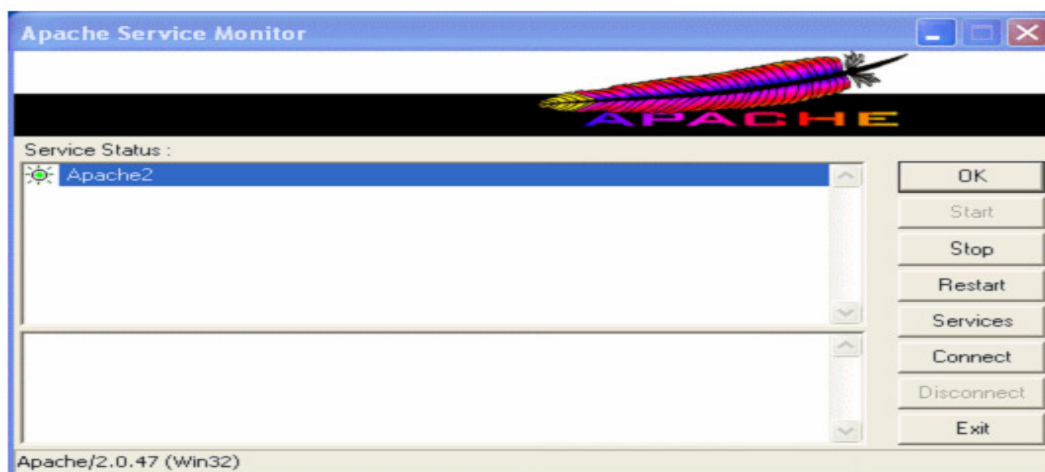


Figure 7.2.7 – Monitor of the Apache server

Если Вы это видите, это значит, что установка ПО веб-сервера Apache на этой системе завершилась успешно. Вы можете теперь добавлять содержимое в эту директорию и заменить эту страницу.

Вы видите это вместо ожидаемой страницы?

Эта страница находится здесь потому, что администратор системы изменил конфигурацию этого веб-сервера. Пожалуйста, свяжитесь с лицом, ответственным за поддержку этого сервера для выяснения ваших вопросов. Apache Software Foundation, автор ПО веб-сервера, которым пользуется администратор этой системы, не связан с поддержкой этой системы и не может помочь Вам разрешить проблемы конфигурации.

Figure 7.2.8 – Test page of Apache server

7.2.2 *Configuring the server configuration file httpd.conf*

To ensure proper operation of the server after installation, you must make changes to the configuration file Apache2. If the server was installed in directory proposed by default (when installing), then, as a rule, no change in the configuration file httpd.conf is necessary. If the server is installed in any other directory, the configuration file httpd.conf must be corrected. Where are the most important pieces of configuration file. It is assumed that the server is installed in a directory **K: \ home \ server **.

```
#
# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See for detailed information about
# the directives.
-----
#### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#
# configuration, error, and log files are kept.
#
# NOTE! If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the LockFile documentation (available
# at );
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
ServerRoot «K:/home/server/Apache2»

#
# ScoreBoardFile: File used to store internal server process information.
# If unspecified (the default), the scoreboard will be stored in an
# anonymous shared memory segment, and will be unavailable to third-party
# applications.
# If specified, ensure that no two invocations of Apache share the same
# scoreboard file. The scoreboard file MUST BE STORED ON A LOCAL DISK.
#
#ScoreBoardFile logs/apache_runtime_status

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
#
PidFile logs/httpd.pid

#
```



```

# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than>
# one request per connection). Set to «Off» to deactivate.
#

KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 15

##
## Server-Pool Size Regulation (MPM specific)
##

# WinNT MPM
# ThreadsPerChild: constant number of worker threads in the server process
# MaxRequestsPerChild: maximum number of requests a server process serves

ThreadsPerChild 250
MaxRequestsPerChild 0

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#

```

```
# ExtendedStatus controls whether Apache will generate «full» status
# information (ExtendedStatus On) or just basic information (ExtendedStatus
# Off) when the «server-status» handler is called. The default is Off.
#
#ExtendedStatus On
```

```
### Section 2: 'Main' server configuration
```

```
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# definition. These values also provide defaults for
# any containers you may define later in the file.
#
# All of these directives may appear inside containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#
```

```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin localhost@localhost
```

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work. See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName localhost
```

```
#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set «Off», Apache will use the Hostname and Port supplied
# by the client. When set «On», Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off
```

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
```

```

# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot «K:/home/server/www»

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the «default» to be a very restrictive set of
# features.
#

Options Indexes Includes
AllowOverride All

Allow from all

#
# Note that from this point forward you must specifically allow
-----
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents. The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.htm index.html index.php

#
# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives. See also the AllowOverride
# directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#

Order allow,deny
Deny from all

#
# TypesConfig describes where the mime.types file (or equivalent) is
# to be found.
#
TypesConfig conf/mime.types

#
# DefaultType is the default MIME type the server will use for a document

```

```

# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, «text/plain» is
# a good value. If most of your content is binary, such as applications
# or images, you may want to use «application/octet-stream» instead to
# keep browsers from trying to display binary files as though they are
# text.
#
DefaultType text/plain

#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#

MIMEMagicFile conf/magic

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off

#
# EnableMMAP: Control whether memory-mapping is used to deliver
-----
# Set to one of: Full | OS | Minor | Minimal | Major | Prod
# where Full conveys the most information, and Prod the least.
#
ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to «EMail» to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#
ServerSignature On

#
# Aliases: Add here as many aliases as you need (with no limit). The format is
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL. So «/icons» isn't aliased in this
# example, only «/icons/». If the fakename is slash-terminated, then the

```

```

# realname must also be slash terminated, and if the fakename omits the
# trailing slash, the realname must also omit it.
#
# We include the /icons/ alias for FancyIndexed directory listings. If you
# do not use FancyIndexing, you may comment this out.
#
Alias /icons/ «K:/home/server/Apache2/icons/»

Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all

#
# This should be changed to the ServerRoot/manual/. The alias provides
# the manual, even if you choose to move your DocumentRoot. You may comment
# this out if you do not care for the documentation.
#
AliasMatch ^/manual(?:/(?:(?:de|en|fr|ja|ko|ru)))?(/.*)?$ «K:/home/server/Apache2/manual$1»

Options Indexes
AllowOverride None
Order allow,deny
Allow from all

SetHandler type-map

SetEnvIf Request_URI ^/manual/de/ prefer-language=de
SetEnvIf Request_URI ^/manual/en/ prefer-language=en
SetEnvIf Request_URI ^/manual/fr/ prefer-language=fr
SetEnvIf Request_URI ^/manual/ja/ prefer-language=ja
SetEnvIf Request_URI ^/manual/ko/ prefer-language=ko
SetEnvIf Request_URI ^/manual/ru/ prefer-language=ru
RedirectMatch 301 ^/manual(?:/(?:(?:de|en|fr|ja|ko|ru)))?{2,}(/.*)?$ /manual/$1$2

#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the client.
# The same rules about trailing «/» apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ «K:/home/server/cgi/»
ScriptAlias /cgi/ «K:/home/server/cgi/»
#
# «K:/home/server/Apache2/cgi-bin» should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
#
# Redirect allows you to tell clients about documents which used to exist in

```

```

# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Example:
# Redirect permanent /foo http://www.example.com/bar

#
# Directives controlling the display of server-generated directory listings.
#

#
# IndexOptions: Controls the appearance of server-generated directory>
# listings.
#
IndexOptions FancyIndexing VersionSort

#
# AddIcon* directives tell the server which icon to show for different
-----
# AddType allows you to add to or override the MIME configuration
# file mime.types for specific file types.
#
AddType application/x-tar .tgz
AddType image/x-icon .ico

#
# AddHandler allows you to map certain file extensions to «handlers»:
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add «ExecCGI» to the «Options» directive.)
#
AddHandler cgi-script .bat .exe .cgi

#
# For files that include their own HTTP headers:
-----
#
# Bring in additional module-specific configurations
#

-----
Include conf/ssl.conf
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at

```

```

#
# for further details before you try to setup virtual hosts.
# You may use the command line option '-S' to verify your virtual host
# configuration.
#
# Use name-based virtual hosting.
#
NameVirtualHost 127.0.0.1
#---localhost

ServerAdmin localhost@localhost
ServerName localhost
DocumentRoot «k:/home/server/www»
ScriptAlias /cgi/ «k:/home/server/cgi/»
ErrorLog k:/home/server/error.log
CustomLog k:/home/server/access.log common

```

7.2.3 *Setting up virtual hosts*

The concept of virtual hosts allows web-server Apache to support several web-sites. As a result, a single server replaces several, ones and external users can see the individual web-sites.

Hosts are called virtual if they use for work one common IP-address or one general physical server, but have different domain names. In order the set server can support virtual hosts it is needed to add these hosts in the server configuration file, in the section Use name-based virtual hosting, which has already registered the main host - localhost. The following example shows two blocks to set up virtual hosts based on the same IP-address, one host uses for this the IP-address and another – the domain name corresponding to the IP-address.

```

<VirtualHost 192.168.0.147>
ServerAdmin  webmaster@newdomain
DocumentRoot k:/home/server/newdomain/www
ServerName   newdomain
ErrorLog     k:/home/server/newdomain/logs/error_log
.....
</VirtualHost>

<VirtualHost mydomain>
ServerAdmin  hostmaster@mydomain
DocumentRoot k:/home/server/my/www
ServerName   mydomain
ErrorLog     k:/home/server/mydomain/logs/error_log
.....
</VirtualHost>

```

After you create the virtual hosts, it is needed to make changes to operating system of the files to perform the matching domain name host with its IP-address. You must correct the file hosts, which located in the directory C: \ WINDOWS \ SYSTEM32 \ DRIVERS \ ect \ host.txt. Example of the configuration of this file is shown below.

```

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com      # source server
# 38.25.63.10  x.acme.com         # x client host

127.0.0.1    localhost hacker
127.0.0.1    cracker

```

7.2.4 Authentication

Web-server can manage user's access and group's-access to the specific catalog web-site. You can set different levels of authentication for this. Access to some facilities may be permitted only to certain users or members of certain groups of users who provided the password. But you can also enable the anonymous access. To apply the directives of authentication to a specific directory put them in a block <Directory> of this catalog. The directive **Require** is used to specify the names of the users who can access the directory. **AuthName** directive sets the name with which the access to a specific set of resources can be got. With the directive **AuthType** the form of authentication can be specified- basic or enhanced. **AuthUserFile** directive sets the location of the password file. An example of the block to configure the authentication procedure is given bellow.

```

<Directory «K:/home/server/mysrv/www»>
  AuthType Basic
  AuthName mysrv
  AuthUserFile «J:/home/server/mysrv/.htpasswd»
  require valid-user
  Allow from All
</Directory>

```

To generate the password file, you can use the htpasswd.exe, for example:
htpasswd -c /var/www/host2/.htpasswd admin

Key-c suggests that we create a new password file. When you add users, this key is not used.

7.2.5 Testing the server

After setting up the configuration file, it is necessary to test work of the server. This testing will verify the correct operation of the Apache html-files.

To test the server with the html-files you need to create arbitrary html – the file named as **index.html** and place it in the **www** directory of the corresponding virtual host, then you should launch a browser and the address **http://localhost**, must be specified in the address line, if you are testing the main host.

7.2.6 Creating HTML-documents

7.2.6.1 General information about the structure of HTML documents

HTML - Hypertext Markup Language, is the primary language of a web-pages. HTML like any other language, consists of operators which is called **tags**. Most operators of the HTML have opening and closing tags. The opening tag is the `<>` and closing tag is the `</>`, symbols for example: `<html>` – the opening tag and `</html>` – closing tag. HTML document is sequence of Tags, and the data concluded between them.

Every HTML document consists of two parts - the «head» of the document and body document and contains 4 mandatory tag. The general structure of an HTML document shown in Example 1.

Example 1. The general structure of an HTML document

```
<html>
<head>
<title> </titl
</head>
<body>
</body>
</html>
```

where `<html>` and `</html>` – tags of the beginning and end of the HTML document, `<head>` and `</head>` – Tags of the beginning and end of the «head» HTML document, `<body>` and `</body>` - tags of beginning and end of the document body, `<title>` and `</title>` – tags of the beginning and end of the header of the document are always located inside the tag «head» of the document and `<head>` and `</Head>`.

The above tags are required and are found in all HTML documents.

7.2.6.2 Tags for creating HTML documents

Here we consider the basic tags that are used to create HTML documents. Some tags have additional parameters that extend the capabilities of a particular tag, such parameters are called as **tag attributes**. The attributes are specified only in the opening tag. The `` and `` tag – allows you to manage the fonts, and has *three Attributes*:

- **Attribute of color** – sets the color of your text, such as color = «# 000003» (all colors of HTML documents use RGB color specter and written in hexadecimal form. In appendix 1 the codes of the primary colors are shown);
- **Attribute of size** – sets the font size of text regarding to the main text, ex. size = «1» (range is from «-2» to «+4»);
- **Attribute face** – gives a certain type of font, for example face = «Arial».

Tag **<body> </ body>** also has a number of attributes: Attribute text sets the color of the text of the document, such as <body text= «# CC0000»>;

Attribute bgcolor sets the background color of the document, such as <body bgcolor = «# 000000»>.

Tag **
** performs forced the setting up of the text to another line, and the tag has no mandatory closing tag. Tag **<p> </ p>** – paragraph, with the help of the tag aligning of texts and objects in the document are performed.

This tag has only one attribute align, which can take four values:

align = «center» – center alignment of the document;

align = «right» – right-alignment of the document;

align = «left» – aligned on the left of the document;

align = «justify» – alignment on both sides of the document.

Tag **<center> </ center>** – the alignment of text in the center, it has no attributes.

Tag **<Hx>** – headlines, there are six levels of headlines H1, H2, H3, H4,H5, H6, among them **<H1> </ H1>** are the largest and **<H6> </ H6>** are smallest.

Tag ** </ b>** – highlight text in bold.

Tag **<i> </ i>** – highlight text in italics.

Tag **<u> </ u>** – underlined text.

7.2.6.3 Examples of creating HTML documents

HTML documents are created in any text editors (such as Notepad) or in specialized programs (such as – «HTML Edit»). To create an HTML document you need to open a text editor, then type there the source code and save the created file with the **.html** extension. Examples of creating HTML documents are shown bellow.

Example 2. Simple HTML Document

```
<html>
<head>
<title> Checking the HTML</title>
</head>
<body bgcolor="#0033FF">
<center>
<h1>
<Font color="#FFFFFF">
Now you may see: Server Apache works in HTML.
<br> Hosting: localhost.
</font>
```

```
</h1>
</center>
</body>
</html>
```

Having opened this HTML document through a browser you will see the following web-page (see Fig. 7.2.9).



**Now you may see: Server Apache works in HTML.
Hosting: localhost.**

Figure 7.2.9 – Simple web-page

Example 3. A more complex web-page

```
<html>
<head>
<title>A more complex HTML document</title>
</head>
<body text="#FF0000» bgcolor="#000000» >
<center>
<h1>
<font color="#FFFFFF»>
Now you may see: Server Apache works in HTML.
<br> Hosting: localhost.
</font>
</h1>
</center>
<p align="justify»>
```

This page contains a more complex * <i> HTML code </i> *, than a page created in * <u> example 1 </u>, * but it is not the most difficult pages that you can create.

```
</body>
</html>
```

If you open this HTML document through a browser you will see the following web-page (Fig. 7.2.10).



**Now you may see: Server Apache works in HTML.
Hosting: localhost.
Вы видите: сервер Апачи работает в HTML!**

Данный страница содержит более сложный HTML код, чем страница созданная в примере 1, но это и не самая сложная страница которую можно создать.

Figure 7.2.10 – A more complex web-page

7.3 CHECK-UP QUESTIONS

- 7.3.1 Specify the destination and the main advantages of Apache.
- 7.3.2 What port and transport protocol are used for Apache?
- 7.3.3 What hosts are called virtual, and what they are for?
- 7.3.4 How a virtual host can be created?
- 7.3.5 How to allow the access to the virtual host only for some users, and ban for all the rest?
- 7.3.6 Give the definition of HTML.
- 7.3.7 What parts does an html-document consist of?
- 7.3.8 Explain the purpose of attributes.
- 7.3.9 How can be the general background of HTML-document set?
- 7.3.10 What tags are obligatory for any HTML-document?

7.4 HOME ASSIGNMENTS

- 7.4.1 Learn the key principles.
- 7.4.2 Prepare answers to check-up questions.
- 7.4.3 Draw the structure of HTML-document.

7.5 LABORATORY ASSIGNMENTS

- 7.5.1 Install web-server Apache on PC.
- 7.5.2 Correct a file of server configuration file httpd.conf.
- 7.5.3 Create an html-document named as index.html. Customize the color of document with Appendix B.
- 7.5.4 Using the generated html-document, test the basic Host (localhost) of Apache server.
- 7.5.5 Set up two virtual hosts.
- 7.5.6 Set up for one of the virtual hosts, authentication, and log on passwords.
- 7.5.7. Create two html-document named as index.html and again index.html (do not use the documents listed in the examples).
- 7.5.8. Test the virtual hosts of Apache using the generated html-document.

7.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

- 7.6.1 The name of laboratory work.
- 7.6.2 Purpose of the work.
- 7.6.3 Results of home assignments.
- 7.6.4 Short description of the work done.
- 7.6.5 Conclusions about the work done.
- 7.6.6 Date, the signature of a student, the remark of a teacher.

LABORATORY WORK № 8

THEME: CONFIGURE PROXY SERVER

8.1 PURPOSE OF THE WORK

Research the general principles of the Network Service Proxy server and get practical skills of configuring this service.

8.2 KEY PRINCIPLES

According to the dictionary, proxy – it's someone (or something), who is authorized to act on behalf of his client and «delivering» specific items to the customer.

Proxy server («representative or authorized») – a service for computer networks, allowing to clients to indirect requests to other network services. At first, the client connects to a proxy server and requests a resource (for example e-mail), located on another server. Then the proxy server either connects to the specified server and gets the resources from it. In some cases, a client request or server response can be changed by proxy server for certain purposes. Also, a proxy server allows you to protect the client computer from some network attacks.

8.2.1 The process of network mediation and the appointment of a proxy server

As a rule, the proxy server is the base server process. This server process is a listener, that listens to a particular port, waiting for requests for a particular protocol. When a connection is established with the client and received a valid request, it «repeats» the request to another server on behalf of the client, as defined in its rules for this type of query. When the server responds, the proxy sends the response back to the user or client process that had previously carried out an inquiry by applying all the necessary conversions.

Most often the proxy server is used for the following purposes:

- Providing of the access from the computer network to the Internet.
- Data caching: if there are frequent appeals to the same external resources, we can keep their copy on the proxy server and generate on demand, thereby reducing the load on the channel to the external network and speeding up receiving of the requested information by the client.
- Data compression: the proxy server downloads information from the Internet and transmits the information to the end user in a compressed form. Such proxy servers are used mainly in order to save external traffic.
- Protecting the local network from the external access: for example, you can configure the proxy server so that the local computer will look to external resources only through it, and the external computers can not access to local ones at all (they «see» only the proxy server).
- Restricting access from the LAN to the outside: for example the access, can be restricted to certain websites, the use of the Internet is restricted for some local users, set quotas on traffic or bandwidth, filter ads and viruses.

- Anonymization of the access to various resources. The proxy server can conceal information about the source of the request about user. In this case, the destination server sees only the information about the proxy server, for example, IP-address, but is unable to determine the true source of the request. There are the also distorting proxy servers that send to your target server false information about the true user.

8.2.2 Types of proxy servers

Often the proxy server performs several functions simultaneously, for example, proxy server can provide opportunities for caching, and authentication in addition to the basic function of providing a network-house applications. However, it is more correctly to interpret the different ways a proxy server as separate types of proxy servers.

Today proxy servers can be classified as the following types:

- forward proxies;
- transparent proxies;
- caching proxies;
- security proxies;
- reverse proxies.

The forwarding proxy. The forwarding proxy server is a server that helps users in one security zone to query the content of the «next» zone, following the direction, which is usually outgoing (this means that the client is within a closed network, while a server is somewhere on the internet).

From a security standpoint a simple proxy server hides the workstation or process requested resource. It can be also used to hide some of the other attributes of the user's session. A typical example of this type is the corporate proxy, which serves the internal users by allowing them access to outside sites, or any other form of interaction with the Internet.

In terms of topology (as in a general sense, and respected to the bandwidth) sending proxy always has a greater constraint in network speed in relation to its users, due to the fact that the speed of the external channel is always less than the speed of the corporate network.

Transparent proxy server. Transparent proxy server – it is a proxy server, which is present in the network and performs its functions, but users are not explicitly aware of the presence of a proxy server on the network. Transparent proxy server – this is a forwarding proxy with additional modules (blocks) that listen to all traffic to specific protocols for a certain segment of the network and intercept it. In this case, the user creates the illusion of direct communication with external resources (for example with the site), although, in reality, the queries that generate a user process are intercepted by proxy server, processed it and only then transferred to an external resource.

Consequently, we can say that the proxy server is an opaque, (announced), when users are aware of its presence in the network and browser settings need to specify its parameters.

Strictly speaking, a transparent proxy server can not be attributed to a particular type of proxy servers. More correct is the following statement – any proxy server can be configured to work as transparently and in the declared (non-transparent) mode.

Caching proxy. Caching proxy, as indicated in their titles, are proxy servers that are configured to reuse the cached content of images (copies) when it is available and possible. The most important aspect for caching proxy is a need to ensure that the server cache only what you need. For example, a dynamic, regularly changing content makes no sense to cache, since it has constantly changing content. In the case of HTTP-content, HTTP headers show the ability to cache content by means of special signs «cache». In most cases forwarding proxy server is configured also to act as a caching proxy. Fig. 8.2.1 shows a portion of the network with the proxy server acting as a forwarding and caching traffic.

Proxy Server Security. In some cases, proxy servers can be configured so that they could act as a filter network traffic, that is to carry out certain rules of security policy. This type of server can provide the treatment (or act as intermediaries in the process) requests authentication and authorization. In these cases, the client authentication and client authentication for the access to the certain content is controlled by the proxy server. Further, the security certificate is sent from the proxy server to the server resource with the query and the destination server must be configured to provide confidence for proxy certificate which is provided.

In most cases, features of security can be added to the Standard Proxy Server as a plug-in plug-in. There are also separate products, such as IBM Tivoli Access Manager for e-Business, which serve only as a proxy security.

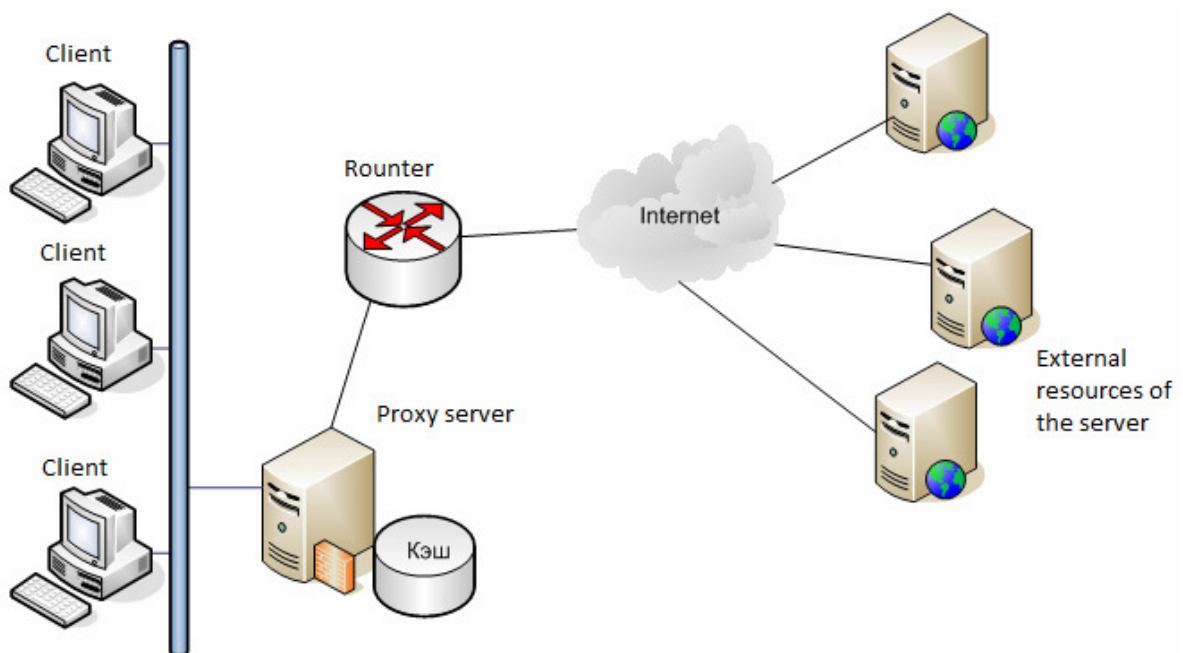


Figure 8.2.1 – Proxy server caching, and traffic forwarding

Reverse proxy. Reverse proxy is a proxy server, which is in contrast to direct one, relays client requests from the external network to one or more servers that are

logically located on the internal network. It is often used for network to load balancing across multiple Web servers and improve their security, while performing the role of a firewall at the application level.

Reverse proxy servers have a lot to do with the forwarding proxy servers – virtually the same products can be configured to work as a regular Proxy Server, as well as a reverse proxy server.

Reverse proxy server is transparent by definition. For the reverse proxy server, the user does not know about his communication with a proxy server. The user believes that communicates with a real resource – a server that hosts the content. Reverse proxy servers are usually implemented in order to provide insulation and content areas. However, if necessary, you can also add a reverse proxy server functionality for caching traffic for better performance with the simultaneous benefits of security. Fig. 8.2.2 shows a fragment of a network with a reverse proxy server.

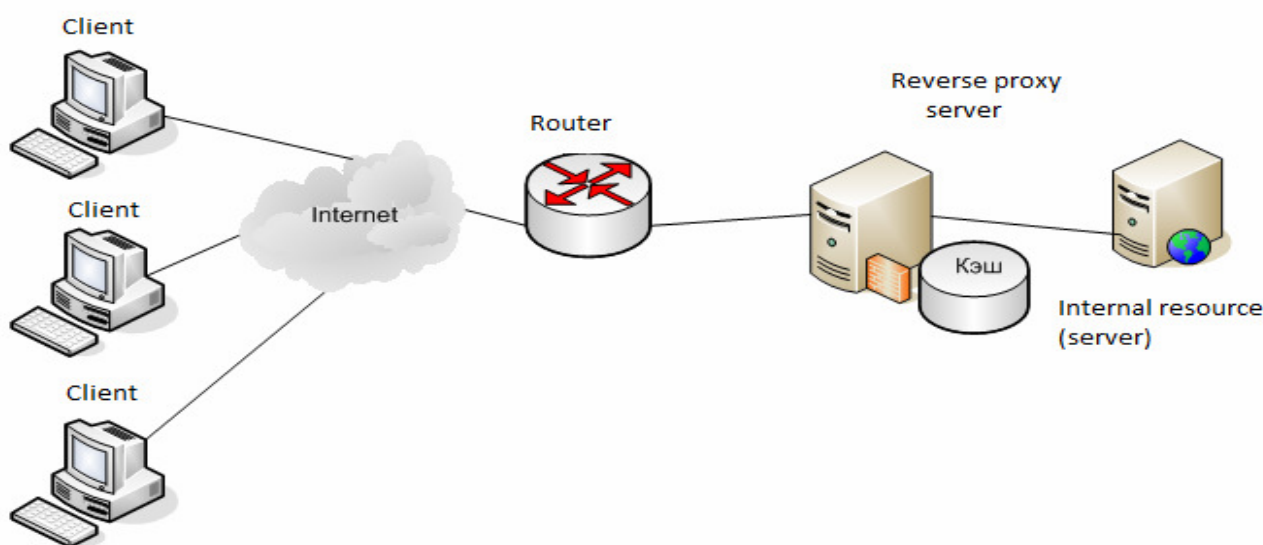


Figure 8.2.2 – Fragment of a network with the reverse proxy server

There are also reverse proxy servers with additional security, known as Reverse Proxies Secure Servers (RPSS) servers, which combine the functions of «pure» reverse proxy and security features content. Such products have RPSS embedded component (which handles requests for access and authorization) is combined with a central control system access and security companies, which actually checks the user or customer to access and authorization. This embedded component is sometimes called the blade (blade).

8.2.3 The most common proxy servers

Today, there are quite a number of proxy servers, which are designed by different manufacturers and are designed to run on different operating systems. Below are the most popular ones:

- Squid;
- Microsoft ISA Server;
- 3proxy;
- Traffic Inspector;

- UserGate;
- Kerio winroute firewall;
- HandyCache;
- CoolProxy;
- WinGate;
- WinProxy.

8.2.4 Proxy server UserGate

Proxy – Server User Gate is a full-featured solution that allows the administrator to organize the users on the LAN to the Internet, as well as centrally managed Internet connectivity through a flexible system of rules. It allows for caching of network resources, has built-in billing system, and system statistics. With a flexible system of rules of the network, an administrator can block users from accessing certain resources, regulates the speed of the connection, sets the timetable for the various users. The program provides detailed monitoring of active Internet – user sessions in real time - IP address, a user name, the exact number of incoming and outgoing traffic as well as visited URL.

The composition of User Gate includes statistics module that allows to compose the various statistical reports. Among other features of the program – the various methods of user authentication, filters URL, allowing prohibit access to undesirable; port assignment to divert traffic from one port to another, and publication resources (access to internal network resources from the Internet); integrated firewall, caching of HTTP resources ; redial your ISP, the ability to remotely administer.

The program supports all the protocols of the stack IP/TCP – HTTP, FTP, POP3, SMTP, IMAP4, Telnet, IRC, NNTP, ICQ and others.

User Gate consists of several modules:

- User Gate Server – it is the server itself. It is installed on your computer directly connected to the Internet. The server implements the user’s access to the Internet, performs traffic counts, keeps statistics works, carries out anti-virus scanning, etc.
- User Gate Administrator – This module is designed for system administration. With it you can customize your function proxy – server. This module does not necessarily have to reside on the server, you can remotely control User Gate;
- User Gate Statistics – is used to view statistics regarding to usage of the Internet and create reports based on it;
- UGClient – designed to enable the user’s authentication through Active Directory.

Fig. 8.2.3 shows an example of a network with a proxy server, UserGate.

8.2.5 System requirements

UserGate proxy server is focused on work that is running Windows, namely Windows 2000/XP/2003/2008. A computer with UserGate has the direct access to the

Internet. The remaining users' computers must have a connection to the server UserGate (be in the same address space). Hardware requirements are given in Table 8.2.1

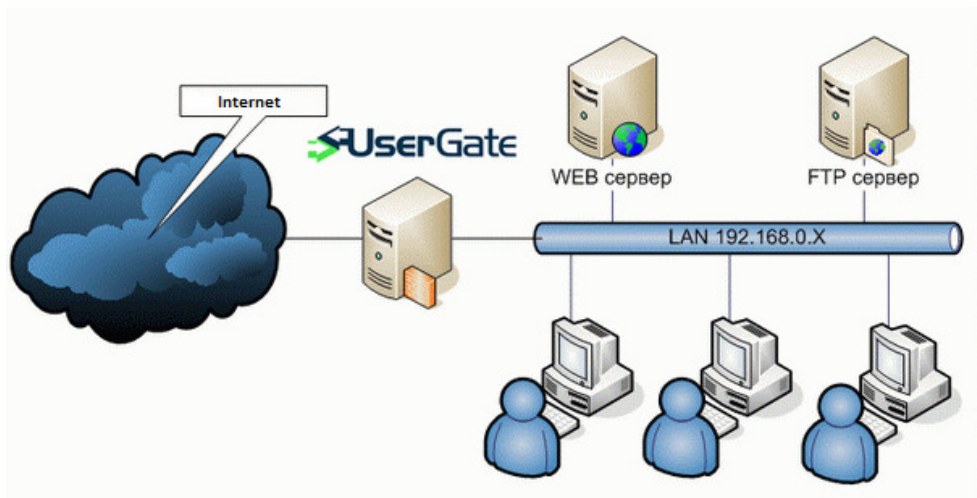


Figure 8.2.3 – Example network with a proxy server UserGate

Table 8.2.1 – Hardware Requirements

Network Configuration	Minimal Requirements	Recommended Requirements
Small LAN: 2-5 users	Pentium 300 with 128 MB RAM Windows 2000 256 Kbit/s installed TCP/IP and (Router и Remote Access Service, only for NT)	Pentium 1000 with 256 MB RAM Windows 2000 512 Kbit/s installed TCP/IP and (Router и Remote Access Service, only for NT)
Average LAN: 5-20 users	Pentium 1000 with 256 MB RAM Windows XP 512 Kbit/s installed TCP/IP and (Router и Remote Access Service, only for NT)	Pentium 1400 with 512 MB RAM Windows XP 1 Mbit/s installed TCP/IP and (Router and Remote Access Service, only for NT)
Big LAN: 20 users	Pentium 2000 with 1 MB RAM Windows 2003/2008 E1 and more installed TCP/IP and (Router and Remote Access Service, only for NT)	Pentium 2000 with 2 MB RAM Windows 2003/2008 E1 and more installed TCP/IP and (Router and Remote Access Service, only for NT)

8.2.6 Example of setting the proxy server UserGate

To configure the proxy server must run the component UserGate Server and UserGate Administrator. Running these components may be implemented by the system tray icon, if UserGate is installed as a service, or via the Start menu - UserGate 4 - UserGate Server (Start - UserGate 4 - UserGate Administrator).

Administrator module is designed to set up and subsequent management of proxy servers. Fig. 8.2.4 shows the module the Administrator.

To configure the proxy server it is needed to connect to the detected network connections. For this, in the main window Administrator one must go to the Connection tab to select from a list of your connection and press the Connect button (see Fig. 8.2.5)

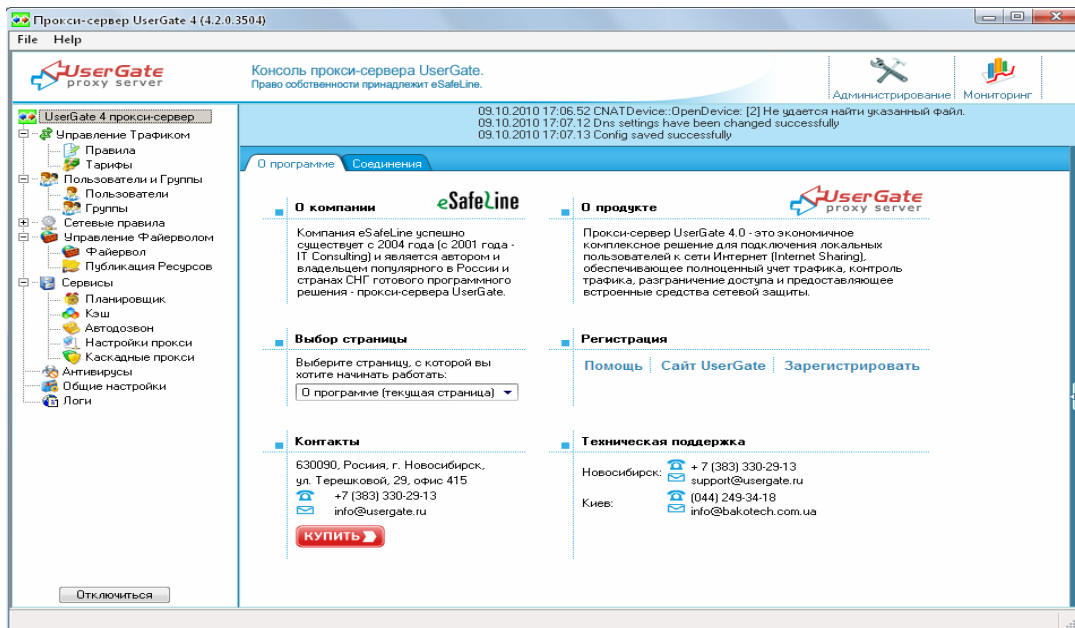


Figure 8.2.4 – Window Module Administrator

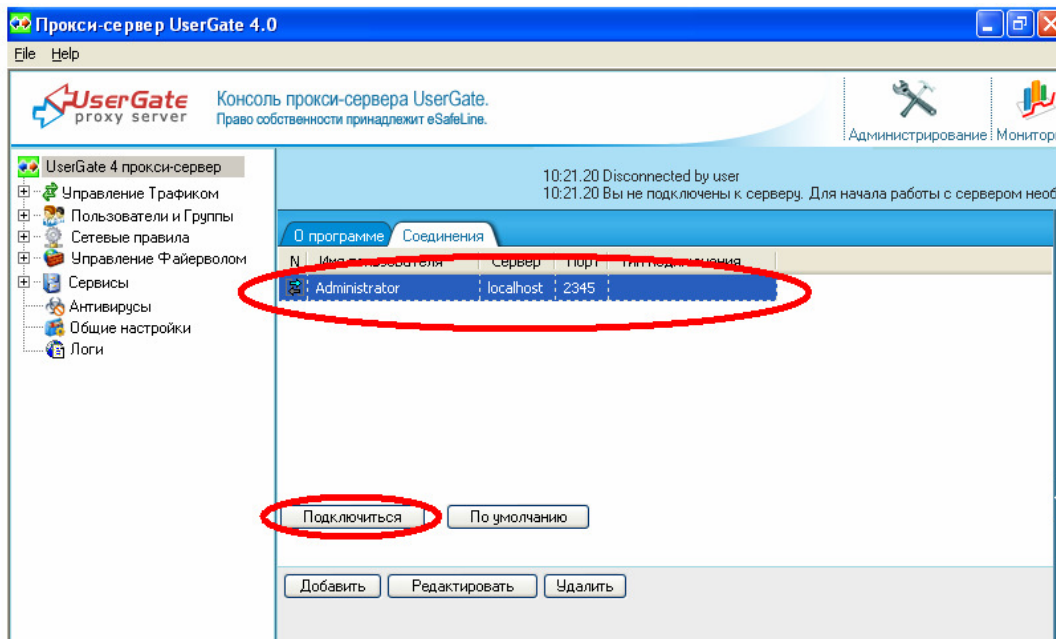


Figure 8.2.5 – Connecting a network connection

After connecting to the network connection one should go to the Users and Groups and create a new local user to specify all the necessary settings - user name, the type of authentication required to connect the rules for handling traffic (see Fig. 8.2.6).

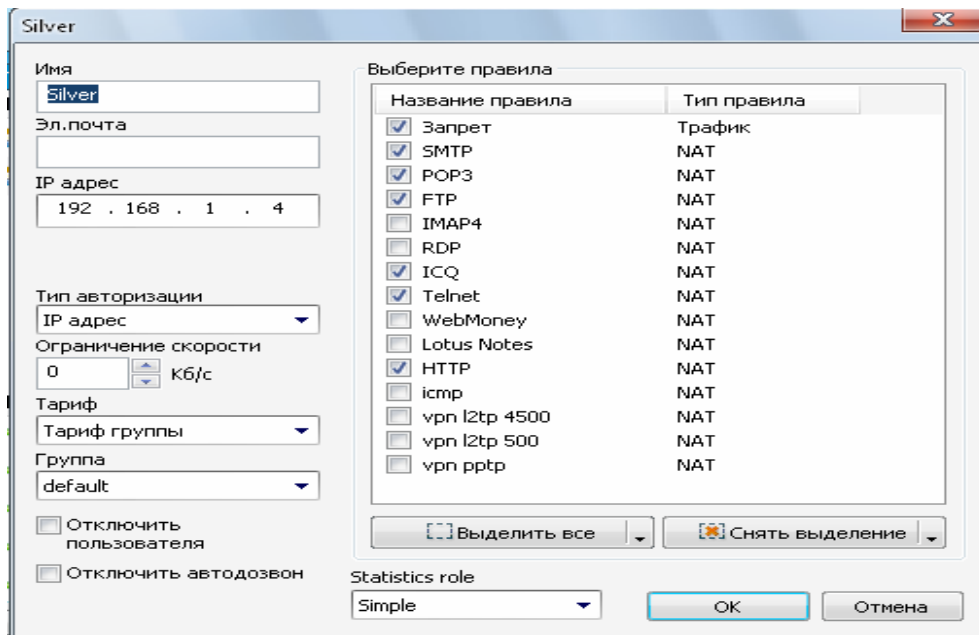
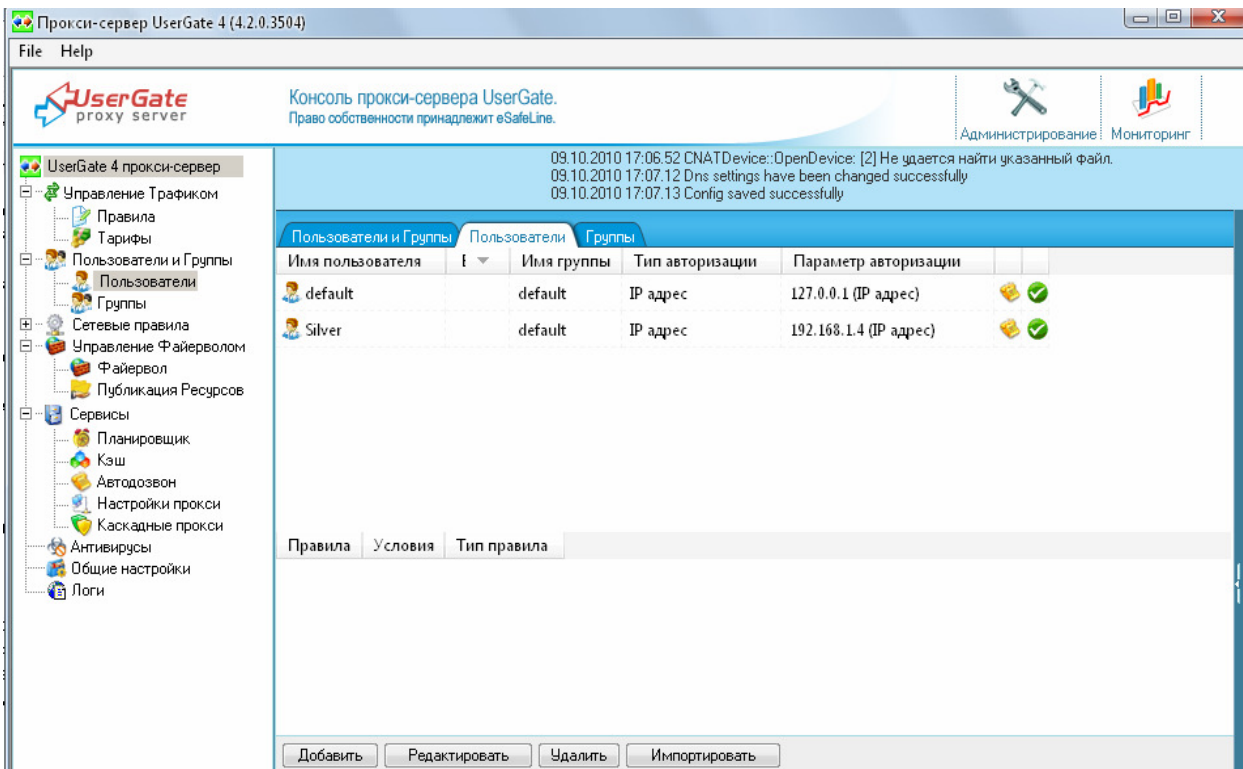


Figure 8.2.6 – Creating a user

As the simplest type of authentication is better to use the IP address, that is, authentication is carried out on the network address of the computer. After this it is necessary to include itself Proxy server, it is necessary to go to Tools -> Configure Proxy, then turn on HTTP Proxy, click the left mouse button twice in the dialog box, choose the intranet - the interfaces on which the Proxy will listen for requests (see Fig. 8.2.7).

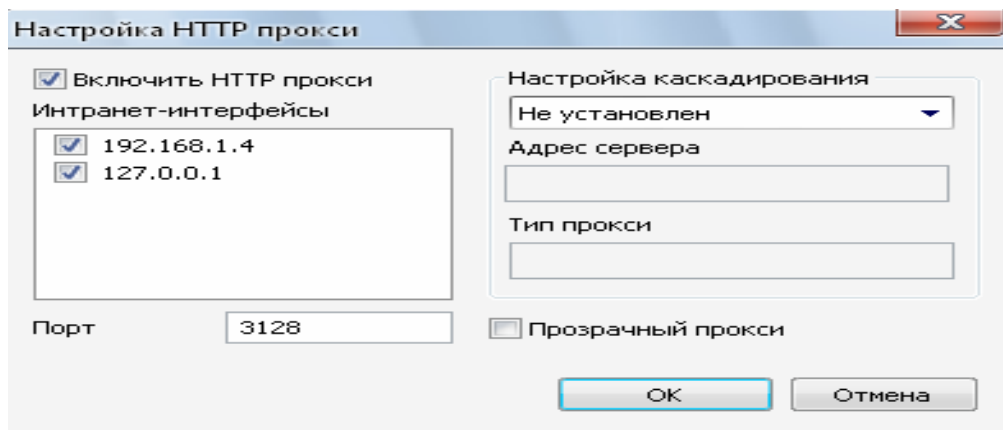
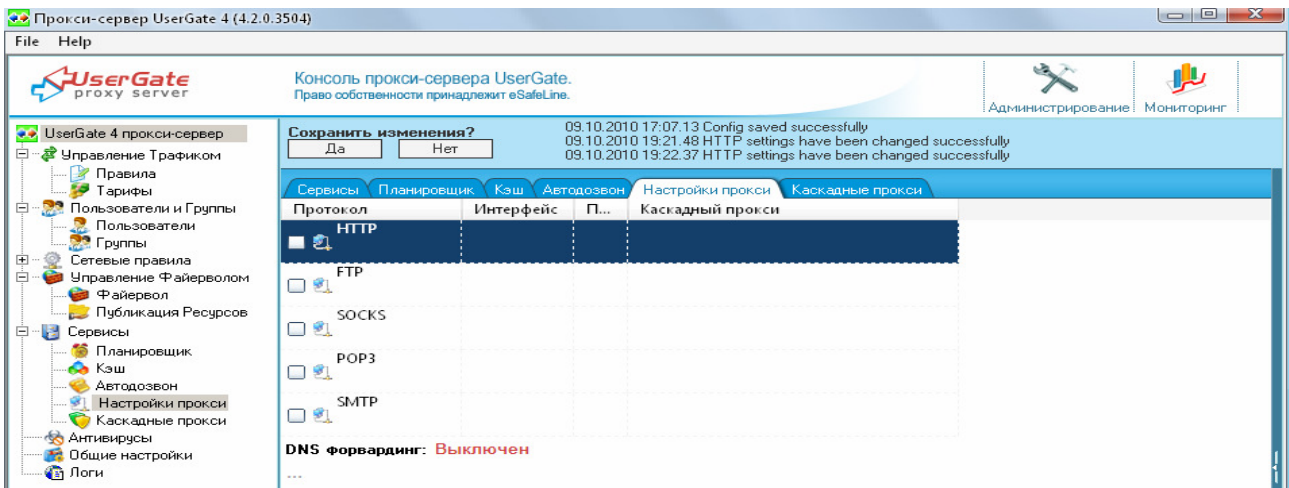


Figure 8.2.7 – Setting up a proxy server

These settings are enough to ensure the work of a proxy server. To verify that the server you should in your browser settings, specify the proxy server (the address and port used) and open the site. If the Web page opens, it means that the server is configured and working properly.

8.2.7 Configuring additional features of a proxy server

First of all as additional settings it is needed to configure the rules restricting access for users to specific resources, as well as limiting the amount of traffic generated by users. This function is realized through the traffic control menu (see Fig. 8.2.8).

To create a rule, you must run the wizard in Figure 8.2.9 shows an example of a rule forbidding access to the server mail.ru. Rule Wizard includes 5 steps, in this case we need to use 1, 2 and 5 steps, which we give the name of the rule, actions of the rule for which protocol this rule applies, and what resources it prohibits. Steps 3 and 4 are used for limiting the amount of traffic and specifying the duration of the rule. After creating the rule it must be applied to specific users or user groups.

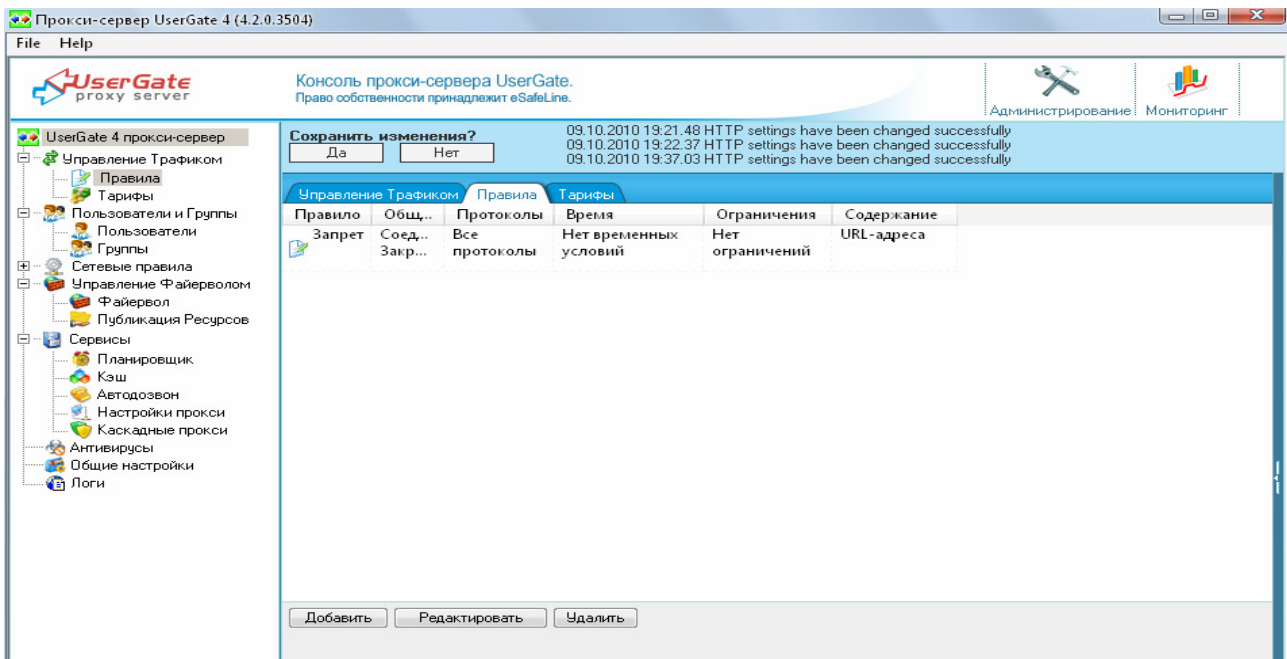


Figure 8.2.8 – Module of Traffic management

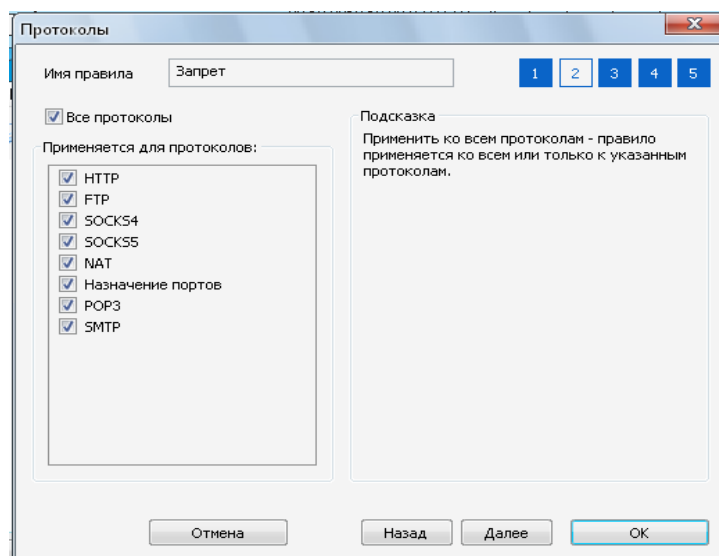
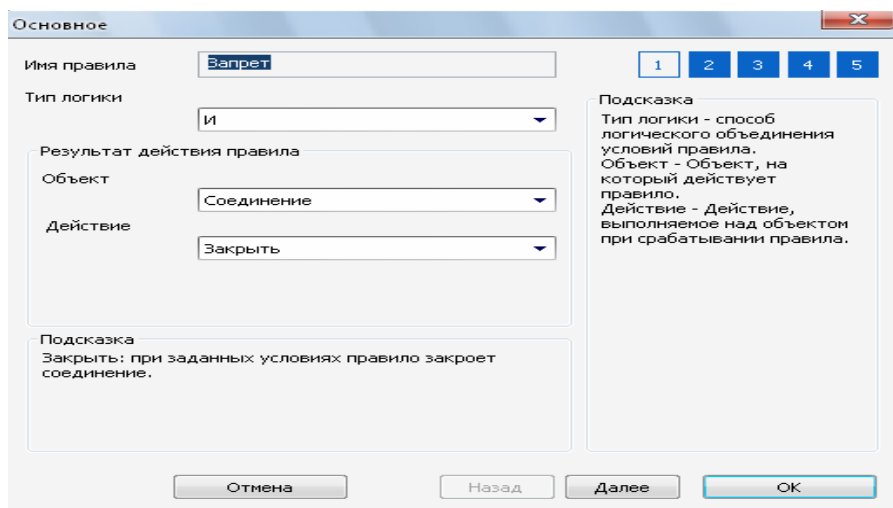


Figure 8.2.9 – Example of creating a rule

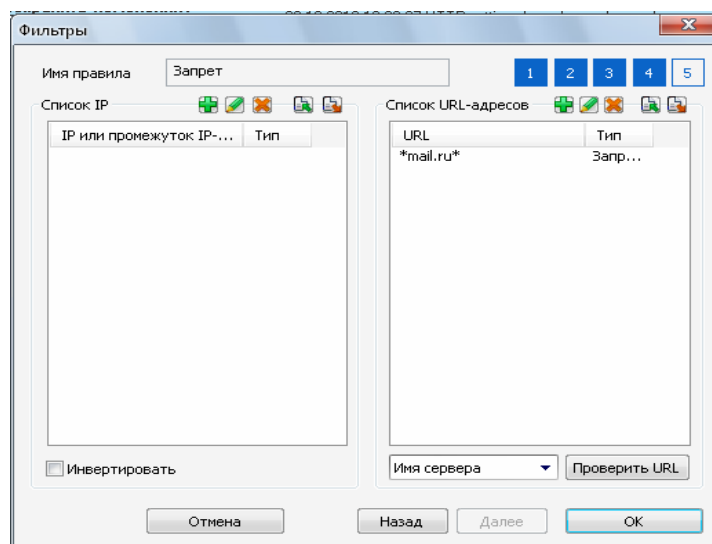


Figure 8.2.9 – Example of creating a rule (continuation of figure 8.2.9)

If the rule is created correctly, the result of its application in the browser will show a message (Fig. 8.2.10).

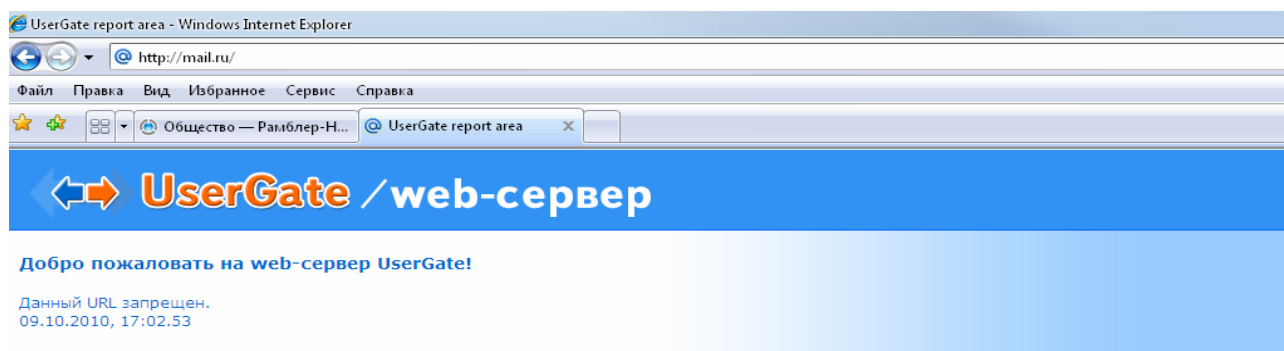


Figure 8.2.10 – Post from a proxy server about the lock a resource.

In addition, the user can view their statistic for this in the address bar of your browser to dial `http:// [server address]: [port http] or http://usergate` (Fig. 8.2.11)

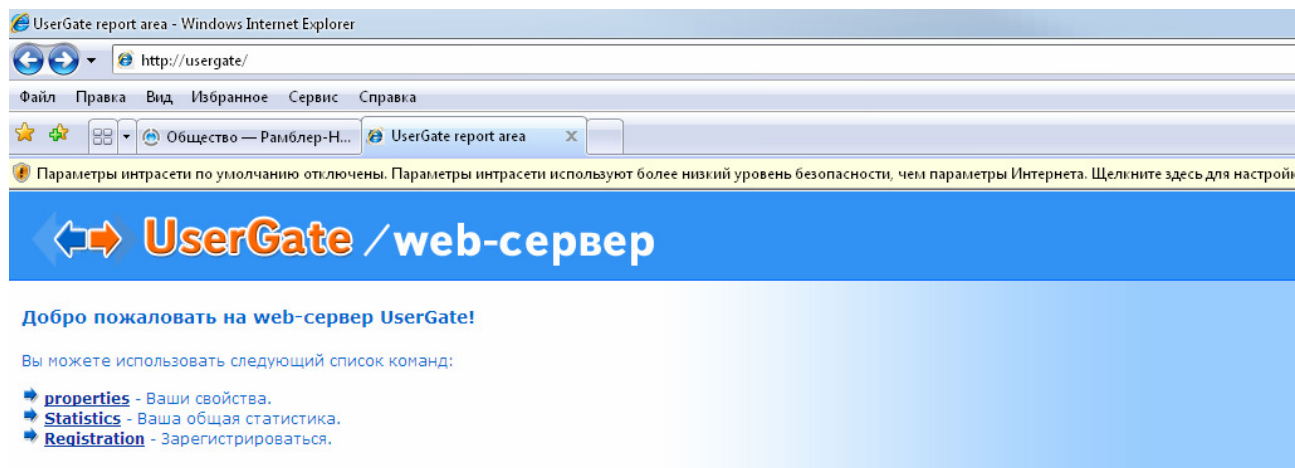


Figure 8.2.11 – To view user statistics

In addition, the administrator can view statistics for all users by using the statistics module, which runs through the Start menu-UserGate-Statistics (see Fig. 8.2.12).

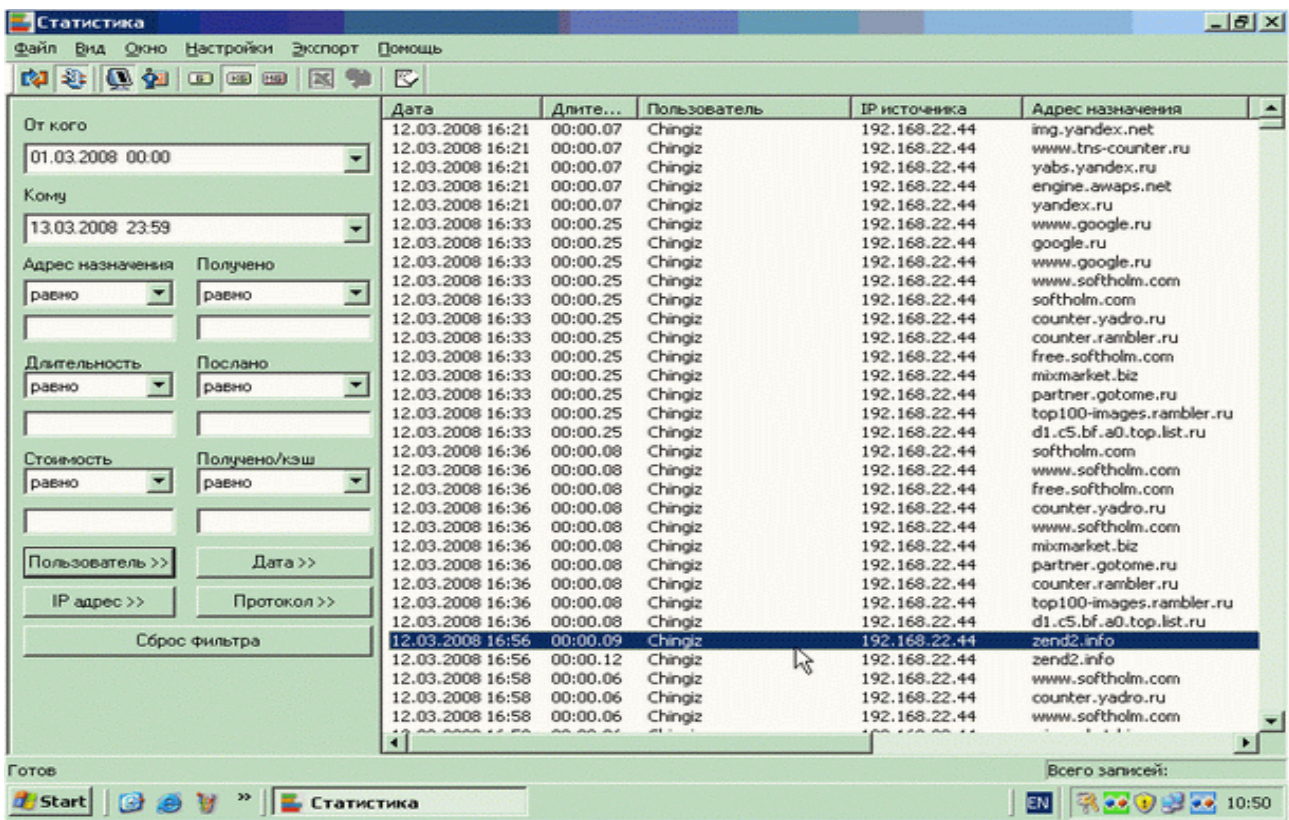


Figure 8.2.12 – Module General statistics

Besides the above discussed possibilities, UserGate proxy server provides the ability to cache traffic. In addition, this server has a built-in firewall and network address translation module that allows the flexibility to configure different security policies for different users, user groups and resources. Also in this server is implemented ability to check external traffic for viruses.

8.3 CHECK-UP QUESTIONS

- 8.3.1 Definition of the proxy server.
- 8.3.2 For what purpose a proxy server is used?
- 8.3.3 Types of proxy servers.
- 8.3.4 What is caching proxy server?
- 8.3.5 Which proxy server is transparent?
- 8.3.6 What is a Reverse proxy server?
- 8.3.7 What type of proxy servers does Usergate belong to?
- 8.3.8 Which modules of UserGate do you know?
- 8.3.9 List the apparatuses requirements for server UserGate.

8.4 HOME ASSIGNMENTS

8.4.1 Learn the key principles.

8.4.2 Prepare answers to check-up questions.

8.4.3 Draw the structure of the network with a proxy server.

8.5 LABORATORY ASSIGNMENTS

8.5.1 Set the proxy server UserGate.

8.5.2 Run-ins and UserGate Server UserGate Administrator

8.5.3 Connect to a network connection.

8.5.4 Create a local user.

8.5.5 Enable and configure the proxy server module

8.5.6 In a browser, configure the Proxy server and test its performance.

8.5.7 Create a rule forbidding access to certain sites (the site is given by the teacher).

8.5.8 To test the established rules.

8.5.9 View statistic of the user experience and general statistics.

8.6 REQUIREMENTS TO CONTENT OF THE PROTOCOL

8.6.1 The name of laboratory work.

8.6.2 Purpose of the work.

8.6.3 Results of home assignments.

8.6.4 Short description of the work done.

8.6.5 Conclusions about the work done.

8.6.6 Date, the signature of a student, the remark of a teacher.

A1. Specifications of software products for video conferencing (Table A1)

Table A1 – Technical characteristics of software products for video conferencing

Characteristic	Business Video Conferencing System 3.0 of Intel company	NetMeeting of Microsoft company	LiveLAN 3.0 of PictureTel company	CU-SeeMe 3.1b of White Pine Software company
CPU or a supported platform	Intel Pentium*	Intel 486/66 or more powerful	Intel Pentium	Intel 486 or more powerful Macintosh
Supported OS	Windows 95, 3.1	Windows 2000, NT 4.0	Windows 95 with stack compatible with WinSock 1.1	Windows 95, NT 4.0 Mac OS
Standards Supported video conferens connection	H.323, H.320	H.323	H.323, H.320	H.323 (wit usage of a Meeting-Point server)
<i>Standards Supported video codec</i>				
H.263	•	•	•	•
H.261	•	•	•	•
<i>Standards Supported of sound compression</i>				
G.728 LD-CELP	•	○	○	○
G.723 MPC-MLQ	•	•	○	•
G.711 MULAW	•	•	•	○
Duplex sound	•	•	•	•
Echo suppression	•	○	•	•
Types of Videoconferencing	Duplex	Duplex	Duplex	Duplex, multidirectional
Types of communication for users to work together on documents	Duplex, multidirectional	Duplex, multidirectional	Duplex, multidirectional	The same
<i>Supporting users on documents</i>				
Standart	T.120 (NetMeeting)	T.120 (NetMeeting)	T.120 (LiveShare)	T.120
Total virtual classroom board	•	•	•	•
Sharing applications	•	•	•	○
"Conversation» ** / messaging/file transfer	•/○/•	•/○/•	•/•/•	•/○/○
Remote management	○	○	•	○
Collaborating users online	•	•	•	○
Tool management videoconferencing	LANDesk	N/D	LiveManager	MeetingPoint

NOTE: • - is, ○ – no, N/D – no data. * processor with MMX is required . ** exchange by short text messges (Chat).

A2. Standard H.323 multimedia communication

Adoption of the International Union (ITU) standard H.323 has opened doors for a seamless integration of multimedia conferencing with existing packet networks, including local, intranet and Internet. Prior to it is issuing, the companies, which wanted to have a standards-based conferencing, handed using equipment that is compatible with the ITU recommendation H.320. Although this standard has greatly contributed to the spread of teleconferencing, as it provides collaboration products from different manufacturers, it imposes some limitations. Most of H.320-compatible systems work only on the lines of basic access ISDN (BRI), so companies had to complement their existing network infrastructure channel ISDN. ITU Recommendations included in the standard H.323, provides for multimedia conferencing over packet networks, including LAN Ethernet. They define the mode of operation of terminals in networks with shared resources, not guaranteeing the quality of service (QoS). The standard of H.323 protocol is not associated with IP, however, appears to most implementations of H.323 will be based on this protocol, as it is widely used in corporate networks. Many well-known manufacturers, including the Corporation Intel (a family of products, ProShare) and Microsoft (in the product NetMeeting), providing support for H.323

A3. Versions and standards of the family H.32x

A set of recommendations of the ITU H.323 defines the network components, protocols and procedures to organize multimedia communications over packet networks. The latter refers to the network, based on the functioning on the principle of packet switching. Package – a small piece of data that is headed, which contains the address and other business data. Packets from different users are transmitted through a communications channel in a statistical time-sharing mode, which provides a very high utilization bandwidth connection. A classic example of packet networks is IP-based networks (including Internet). H.323-compatible devices can be used for telephony (IP-telephony), audio and video (video telephony), as well as audio, video and data (multimedia conference.) H.323 standard is approved by the 16 th Study Group of ITU. Its first version was adopted in October 1996, identified the requirements for audiovisual systems and LAN equipment.

In connection with the appearance of multiple hardware and software of telephone communications over IP need to make changes in specifications H.323, since these funds were often incompatible with each other. In particular, it was necessary to ensure interaction of telephone devices based on the PC and traditional telephone networks, which operate on the principle of circuit switching. The second version of H.323 that takes into account new requirements, adopted in January 1998.

The next version of the standard is been preparing. It will describe the creation of packet networks, facsimile and organization of communication between H.323 gateways

We are talking about these features, common in modern telephony, as notification of receipt of the second call and help. Some companies are seeking for inclusion in the H.323 support multimedia features based on the protocol proposed by

IETF Session Initiation Protocol. In addition to the «phone» functions, the new version will be complemented by tools that take into account the parameters of sessions for the purposes of billing, as well as support directories – instead of digital IP-addresses can be used names and numbers.

The standard H.323 is a family of recommendations N.32h describing the organization of multimedia communications in networks of various types:

- H.320 – Narrowband digital switched network, including ISDN;
- N.321 – Broadband ISDN and ATM;
- N.322 – packet networks with guaranteed bandwidth;
- N.324 – telephone network (PSTN).

One of the main objectives of developing the H.323 standard – ensuring interoperability with other types of networks, multimedia communications. This task is implemented using gateways, which perform signaling translating and data formats.

A5. Main components H.323

Standard H.323 defines four major components, which together with the network structure can have bilateral (point-to-point) and multilateral (point-to-multipoint), multimedia conference.

H.323 terminal may be a PC or a standalone device that can carry multimedia application. He is obliged to ensure a sound relationship and may additionally support the transmission of video or data. Due to the fact that the main function of H.323 terminal is audio, it plays a key role in providing IP-telephony service.

H.323 terminal must support the protocols N.245, Q.931, RAS, RTP / RTCP and a family of protocols N.450, but also include the audio codec G.711. It is additional components may be other audio codecs and video codecs N.261 and / or H.263. The optional protocol is to support collaborative work on documents T. 120.

Gateway (gateway) is not included in the mandatory components of network H.323. It is necessary only if you want to connect to the terminal of another standard. This link is provided translation protocols installation and disconnect, as well as data transmission formats. Gateways H.323 are widely used in IP-telephony interface IP-based networks, and digital or analog switched telephone networks (ISDN or PSTN).

Gatekeeper (gatekeeper) – an essential component of H.323 network and the central point for all requests within one zone. H.323-zone – a set of terminals, gateways and servers MCU, managed by one controller. In the area there is at least one terminal, and moreover, it can include LAN segments combined routers. Gatekeepers – optional component of H.323 networks, but if it is present in the network, terminals and gateways must use its services. Note that it can be executed as part of a gateway server or MCU

H.323 standard defines the basic (mandatory) and additional functions of the controller area (see table A2). The first group includes address translation, control of establishing connections between terminals and the latter with the gateways and servers, MCU, bandwidth management, etc. The second group includes, in particular, such an important function, as call routing. It allows you to increase network

efficiency, since the controller is able to choose a route based compounds, such as data loading locks its zone. This feature can also serve to divert the call when you are unable to connect to the caller.

Table A2 – Functions of gatekeeper

Function	Description
1	2
<i>Basic</i>	
Translation of Address	Converting internal LAN addresses and phone numbers E. 164 format (used in networks ISDN) in the transport address protocols, IP or IPX
Management of access	Authorization of access to the H.323 network through the exchange of RAS-messaging «Registration request» (ARQ), «satisfaction query» (ACF) and (Rejection of a request «(ARJ). For example, if a network administrator set a limit number of simultaneous connections, then when a ! This threshold zone controller will reject new requests Idostup. The setting of this function can be set "0», which means tolerance of all endpoints in the H.323 network
1	2
Management of Stripe transmission	Used RAS-messages «request bandwidth» (BRQ), «satisfaction query» (BCF) and «rejection of a request» (BRJ). The setting of this function can be set to «O», which means automatic satisfaction of all requests to change the bandwidth
<i>Additional</i>	
Management of Process Establishment compounds	When bilateral conference controller can handle service messages signaling protocol Q.931. Controller may serve as a simple relay of messages from endpoints
Authorization of Connections	In accordance with the specifications Q.931 allowed deviation controller connection requests. Among reasons - Restriction of rights or time of access, as well as other criteria are outside the standard H. 323
Management of Call	Gatekeepers can track the status of all active compounds that can manage calls, ensuring the allocation of necessary bandwidth and load balancing of network resources by diverting calls to other terminals and gateways

Server multilateral conference (MCU) connects three or more H.323 terminals. All terminals participating in the conference establish a connection to the MCU. The server manages the resources of the conference, agrees opportunities

Terminal handling audio and video, identifies audio and video to be sent to many addresses.

A6. Other components and protocols

Videoconferencing of H. 323 standard does not depend on the type of packet switching network and transport protocols used to carry them out. However, the standard defines the components and protocols, without which a multimedia conference with application software and hardware from different vendors becomes impossible (Fig. 2). These mandatory elements are audio and video codecs, protocols, RAS, Q.931, N.245, RTF, RTCP, family advice N.450. Audio Codec is designed to digitize the analog audio signal and the received digital signal compression, as well as a reverse operation. The standard H.323 provides for the possibility of using the

five code – G.711 (3.1-kHz conversion of the analog signal for transmission in digital form at speeds of 48, 56 or 64 kbps), G.722 (7 kHz, 48, 56 or 64 kbps), G.723 (3,1 kHz, 5,3 or 6.3 kbps), G.728 (3,1 kHz, 16 kbps) and G.729 (3,1 kHz, , 8 kbit / s). Each terminal must maintain at least one audio codec. Video codec used to encode / decode the video frames. Although the H.323 standard specifies support for video as an optional service, each video display must include a codec N. 261 It provides the transfer of digital video over a single or multiple channels with a bandwidth of 64 kbps. The feature of this codec is that part of the frame is encoded entirely, and the remaining frames - only to change them. In addition, H.323 permits the use of H.263 codec. It provides better transmission of video, but at lower speeds (codes are transmitted only change of personnel). Interaction between the terminals and H.263 N.261 possible because they both support the format resolution QCIF (176x144 pixels). Protocol signaling RAS (registration, confirmation and status) is used to transmit service messages between terminals and gatekeepers. RAS-messages are used for the registration of terminals, their admission to the communication session, changes in use of bandwidth, information on the status of the session and its termination. In the absence of gatekeepers protocol RAS not involved.

Q.931 signaling protocol used for establishing and breaking connections between the two terminals H.323, as well as between the terminal and the gateway. Service messages of this protocol are transmitted over TCP.

Control Protocol multimedia conferencing N.245 provides:

- To harmonize the components;
- To establish and divide the logical channels;
- Transfer requests for the establishment of priority;
- Flow Control (network bandwidth);
- The transfer of common commands, and indicators.

Messages are transmitted by the protocol N.245 N.245-channel management. It is logical channel «O», which, unlike the channels for the exchange of multimedia streams, permanently open. Mezhterminalny exchange parameters can coordinate modes and formats of information coding that provides the interface terminals from different manufacturers. In the process of messaging on the parameters specified capabilities of terminals to receive and transmit various types of traffic. RTF protocol (RFC 1889) provides in IP-network delivery to the addressee of audio and video streams in real time. According to the H.323 standard, in networks with non-guaranteed bandwidth in order to minimize delays and maximize the available bandwidth for transmission of audio and video streaming, as well as the RAS signaling protocol is used User Datagram Protocol (UDP). This protocol involves the mechanism of multicast (IP Multicast) for non-guaranteed delivery of audio and video certain number of users. On top of IP Multicast works RTP, which creates the necessary conditions for normal playback streams received at the subscriber terminals. RTP identifies the type and number of the package, it sets the label synchronization. Based on this information receiving terminal synchronizes audio, video and data, carries out their consistent and continuous playback. Correct

functioning of RTP possible if the subscriber terminals mechanisms buffering the received information. The transport control protocol real-time RTCP (RFC 1889) controls the implementation of functions RTP. It also monitors the quality of service and to provide relevant information components involved in the conference. Additional services in the networks H.323 defines a family of recommendations N.450. As such N.450.1 describes the signaling protocol between the two components of the network, which provide additional services and N.450.2 – mechanisms of transformation services call (Call Transfer), whereby the connection between terminals A and B is converted into a connection between B and C. Additional Service Call Diversion, which determines the recommendation N.450.3 provides an opportunity to redirect the call when the called subscriber is busy, does not answer or when the first install the appropriate option.

Standard H. 323 also determines the procedure for interaction with the terminals of other standards. Most often this problem arises when you pair telephone networks with packet switching and circuit switching.

Network standard H.323 compatible with other types of N.32h networks. Interworking of different networks determines N.32h recommendation N.246. Telecommunications world in process of convergence networks, telephony and data transmission. Internet-telephony, call centers, Web-based and other applications that tipped a big future, provide voice and video simultaneously with the data and rely on the same standard – H.323. It determines everything – from the procedures of communication to the various services that can provide PCs, servers, gateways and other devices, forming a new infrastructure of the universal connection. If the voice and video signals are combined with the data in one application, then to implement it requires hardware that supports a number of mandatory features. Realizing the need for such support, the International Telecommunication Union (ITU) approved in the 1996/98 years. H.323 standard, which regulates video conferencing in packet-switched networks. ITU H.323 is considered rather as a union of different specifications under one roof, rather than as a baseline standard, so it included (in some cases – in an expanded form) is already known standards. Thus, under the wing of H.323 housed five specifications that define the work of audio codecs, the two standards for video codecs, a standard for multiplexing the data, three standard signaling and protocol version to a real time (Real-Time Transport Protocol, RTF), voice and video-packets

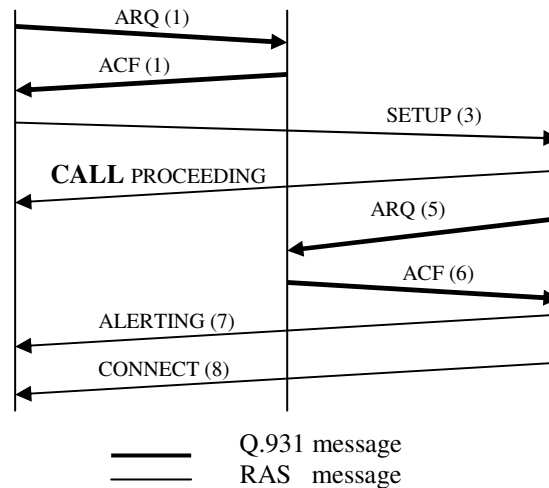
Means of universal communication, the relevant H.323, should not support each of its constituent specification. These products provide only a certain subset of functions, the choice of which depends on the role of a particular device in the H.323 system. Such roles are only four, so all the equipment of the universal network is divided into four types: terminals, gateways, controllers zones and servers multilateral conference. Implementing H.323 profitable corporate users, because it allows you to combine different network infrastructures. Companies will have an

integrated network for voice and data, which is much easier to work and exploitation of which would cost them much cheaper. The standard H.323 will benefit and the end user, as will serve as a catalyst for the emergence of various applications using the versatile capabilities of communications networks . This, for example, applications for joint work or universal messaging system in which one and the same mailbox can be used to obtain both the electronic and voice mail. In a business environment is increasingly gaining popularity based on standard H.323 «free» long distance and international telephone communications, as well as LAN telephony. In the first case, a gateway that meets the recommendations H.323, takes calls from the phone company's network converts voice signals into data packets and sends them on the global IP-connection to the destination .There, in turn, H.323 gateway performs the inverse transformation package to analog signals that are received in the telephone network to another organization, then - to subscribers. LAN telephony develops these capabilities: like PBXs, local area network provides voice, which are activated telephony servers, embedded institutional PBX or implemented on the basis of Windows NT. In order to transfer calls within the LAN, telephone server creates a connection between the user's PC and IP-phones, manages and terminates them within a packet network. Connections to users located outside the local network, implemented by H.323 gateway. Both methods can reduce the cost of telephone calls In addition, they provide the basis for an easy transition to support video conferencing. And it is - just the beginning. Many observers and analysts believe the most important component of H.323, enabling the convergence of networks. Organizations that deal with standards falling in H.323, seek to accelerate the process of final approval, so that users are able to as quickly as possible to use these specifications in real projects. By the experts from 3Com and the next stage of development of IP-telephony to the specifications of H.323, the relevant lower levels EMVOS, will be added. They will record the possibility of the classes (class-of-service, CoS) and quality of service (quality-of-service, QoS), ie, services related, respectively, to the second (channel) and third (network) levels. The development of specifications for CoS / QoS deals with a number of organizations, including working groups IEEE 802.1r and IETF Diff-Serv, and also the European Institute of Standardization in the field of telecommunications (ETSI), which included food H.323 in its draft Telecommunications and Internet Protocol Harmonization Over Networks.

A7. Connect terminals P.323

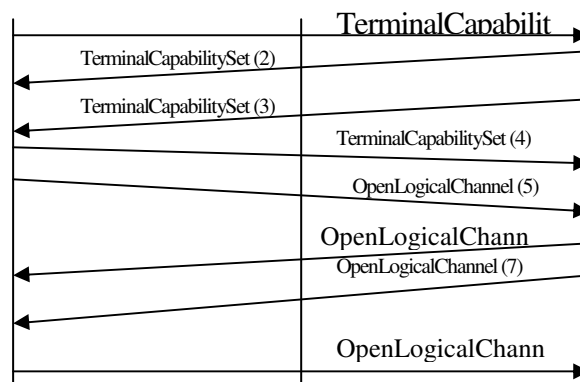
Let's consider the sequence of steps to establish communication between two H.323 multimedia terminals (T1 and T2), connected to the controller area. The last condition does not preclude direct calls.

Passage of connection requests



- 1 T1 sends the gatekeeper a message for the ARQ RAS-channel and asks for permission to use the direct channel signaling with T2.
2. The controller satisfies the request zone T1 message ACF.
3. T1 sends the terminal T2 (3.931-message «setup».
4. T2 responds Q.931-with the message «call proceeding».
5. T2 is recorded in the zone controller by sending him a message on the RAS-ARQ channel.
6. Gatekeeper confirms the registration of RAS-message ACF.
7. T2 T1 notifies its registration (and hence on the resolution to establish a connection) Q.931-message «alerting».
8. After the connection T1 T2 informs the completion of the procedure Q.931-sooobscheniem «connect»

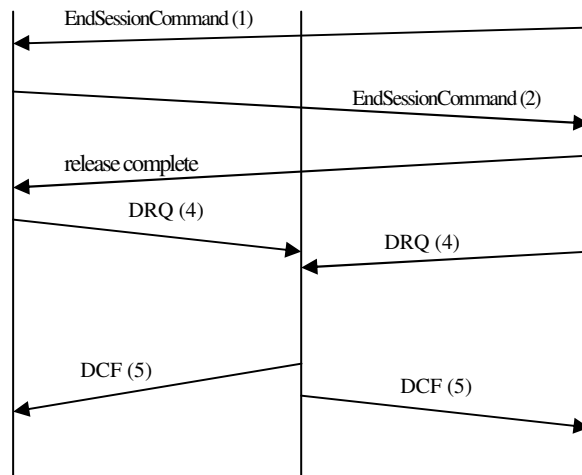
A8. Connect protocol H.245



1. T1 sends a message «Terminal Capability Set» Terminal T2.
2. T2 confirms the beginning of the session to harmonize the message «Terminal Capability Set Ack».
3. T2 informs the terminal T1 of its parameters, the message «TerminalCapabilitySet».
4. T1 completes the process to harmonize the message «Terminal Capability Set Ack».

5. T1 opens the channel of multimedia information in the direction of T2 message «openLogicalChannel» (it includes the transport address of the RTCP-channel).
6. T2 confirms discovery of a unidirectional logical channel from the T1 message «open Logical Channel Ack» (it also includes the RTP-mail terminal T2 and RTCP-address obtained from the T1).
7. T2 opens a media channel in the direction of T1, informing the message «open Logical Channel» (in its composition - RTCP-address).
8. T1 confirms the establishment of a unidirectional logical channel from the T2 message «open Logical Channel Ack» (it includes the RTP-mail terminal T1 and RTCP-address obtained from T2). In this process of establishing a bidirectional connection is completed

A9. Disconnection



1. T2 initiates the separation, sending N.245-message «End Session Command».
2. T1 completes the exchange of data and confirms the separation of presentation «EndSessionCommand».
3. T2 closes the connection after sending Q931-message «release complete».
4. T1 and T2 initialize its disconnection from the zone controller RAS-message DRQ.
5. The controller disables the zone T1 and T2, after notifying them of this message DCF.

Table of base colors

255.255.204 FFFFCC	255.255.153 FFFF99	255.255.102 FFFF66	255.255.51 FFFF33	255.255.0 FFFF00	204.204.0 CCCC00
255.204.102 FFCC66	255.204.0 FFCC00	255.204.51 FFCC33	204.153.0 CC9900	204.153.51 CC9933	153.102.0 996600
255.153.0 FF9900	255.153.51 FF9933	204.153.102 CC9966	204.102.0 CC6600	153.102.51 996633	102.51.0 663300
255.204.153 FFCC99	255.153.102 FF9966	255.102.0 FF6600	204.102.51 CC6633	153.51.0 993300	102.0.0 660000
255.102.51 FF6633	204.51.0 CC3300	255.51.0 FF3300	255.0.0 FF0000	204.0.0 CC0000	153.0.0 990000
255.204.204 FFCCCC	255.153.153 FF9999	255.102.102 FF6666	255.51.51 FF3333	255.0.51 FF0033	204.0.51 CC0033
204.153.153 CC9999	204.102.102 CC6666	204.51.51 CC3333	153.51.51 993333	153.0.51 990033	51.0.0 330000
255.102.153 FF6699	255.51.102 FF3366	255.0.102 FF0066	204.51.102 CC3366	153.102.102 996666	102.51.51 663333
255.153.204 FF99CC	255.51.153 FF3399	255.0.153 FF0099	204.0.102 CC0066	153.51.102 993366	102.0.51 660033
255.102.204 FF66CC	255.0.204 FF00CC	255.51.204 FF33CC	204.102.153 CC6699	204.0.153 CC0099	153.0.102 990066
255.204.255 FFCCFF	255.153.255 FF99FF	255.102.255 FF66FF	255.51.255 FF33FF	255.0.255 FF00FF	204.51.153 CC3399
204.153.204 CC99CC	204.102.204 CC66CC	204.0.204 CC00CC	204.51.204 CC33CC	153.0.153 990099	153.51.153 993399
204.102.255 CC66FF	204.51.255 CC33FF	204.0.255 CC00FF	153.0.204 9900CC	153.102.153 996699	102.0.102 660066
204.153.255 CC99FF	153.51.204 9933CC	153.51.255 9933FF	153.0.255 9900FF	102.0.153 660099	102.51.102 663366

153.102.204 9966CC	153.102.255 9966FF	102.0.204 6600CC	102.51.204 6633CC	102.51.153 663399	51.0.51 330033
204.204.255 CCCCFF	153.153.255 9999FF	102.51.255 6633FF	102.0.255 6600FF	51.0.153 330099	51.0.102 330066
153.153.204 9999CC	102.102.255 6666FF	102.102.204 6666CC	102.102.153 666699	51.51.153 333399	51.51.102 333366
51.51.255 3333FF	51.0.255 3300FF	51.0.204 3300CC	51.51.204 3333CC	0.0.153 000099	0.0.102 000066
102.153.255 6699FF	51.102.255 3366FF	0.0.255 0000FF	0.0.204 0000CC	0.51.204 0033CC	0.0.51 000033
0.102.255 0066FF	0.102.204 0066CC	51.102.204 3366CC	0.51.255 0033FF	0.51.153 003399	0.51.102 003366
153.204.255 99CCFF	51.153.255 3399FF	0.153.255 0099FF	102.153.204 6699CC	51.102.153 336699	0.102.153 006699
102.204.255 66CCFF	51.204.255 33CCFF	0.204.255 00CCFF	51.153.204 3399CC	0.153.204 0099CC	0.51.51 003333
153.204.204 99CCCC	102.204.204 66CCCC	51.153.153 339999	102.153.153 669999	0.102.102 006666	51.102.102 336666
204.255.255 CCFFFF	153.255.255 99FFFF	102.255.255 66FFFF	51.255.255 33FFFF	0.255.255 00FFFF	0.204.204 00CCCC
153.255.204 99FFCC	102.255.204 66FFCC	51.255.204 33FFCC	0.255.204 00FFCC	51.204.204 33CCCC	0.153.153 009999
102.204.153 66CC99	51.204.153 33CC99	0.204.153 00CC99	51.153.102 339966	0.153.102 009966	0.102.51 006633
102.255.153 66FF99	51.255.153 33FF99	0.255.153 00FF99	51.204.102 33CC66	0.204.102 00CC66	0.153.51 009933
153.255.153 99FF99	102.255.102 66FF66	51.255.102 33FF66	0.255.102 00FF66	51.153.51 339933	0.102.0 006600
204.255.204 CCFFCC	153.204.153 99CC99	102.204.102 66CC66	102.153.102 669966	51.102.51 336633	0.51.0 003300
51.255.51 33FF33	0.255.51 00FF33	0.255.0 00FF00	0.204.0 00CC00	51.204.51 33CC33	0.204.51 00CC33

102.255.0 66FF00	102.255.51 66FF33	51.255.0 33FF00	51.204.0 33CC00	51.153.0 339900	0.153.0 009900
204.255.153 CCFF99	153.255.102 99FF66	102.204.0 66CC00	102.204.51 66CC33	102.153.51 669933	51.102.0 336600
153.255.0 99FF00	153.255.51 99FF33	153.204.102 99CC66	153.204.0 99CC00	153.204.51 99CC33	102.153.0 669900
204.255.102 CCFF66	204.255.0 CCFF00	204.255.51 CCFF33	204.204.153 CCCC99	102.102.51 666633	51.51.0 333300
204.204.102 CCCC66	204.204.51 CCCC33	153.153.51 999966	153.153.102 999933	153.153.0 999900	102.102.0 666600
255.255.255 FFFFFF	204.204.204 CCCCCC	153.153.153 999999	102.102.102 666666	51.51.51 333333	0.0.0 000000

Literature

1. Гольдштейн Б. С. IP Телефония /Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. М.: Радио и связь, 2001. – 336 с.: ил. ISBN 5-256-01585-0
2. Мак-Квери. Передача голосовых данных по сетям Cisco Frame Relay, ATM и IP /Мак-Квери. М.: Вильямс, 2002.
3. Гольдштейн Б.С. IP-телефония /Гольдштейн Б.С. С-Пб.: Питер, 2001.
4. Ньюмен Д. Системы видеоконференцсвязи стандарта H.323. /Ньюмен Д., Браун Д. Сети и Системы связи – 1998, №2(24), С. 56 – 65.
5. Scott Hawkins Administration Web-server Apache.
6. WWW.CITFORUM.RU
7. WWW.RUMBLER.RU

Educational publication

Tikhonov Victor Ivanovich
Shulakova Ekaterina Sergyvna
Borzdych Tatiana Olegovna

Studying course

TELECOMMUNICATION AND INFORMATION NETWORKS

Part III

**THE NETWORK SERVICES.
THE NETWORK APPLICATIONS**
(Studying module 4.1)

*Methodical instructions for performance
to the cycle of laboratory works
for training bachelors in Telecommunication*

Редактор

Чеплюк Н. І.

Комп'ютерне верстання
та макетування

Корнійчук Є. С.

Здано в набір 11.02.2013 Підписано до друку 25.03.2013
Формат 60/88/16 Зам. № 5087
Тираж 50 прим. Обсяг: 7,5 ум. друк. арк.
Віддруковано на видавничому устаткуванні фірми RISO
у друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
ОНАЗ, 2013