MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”
DEPARTMENT OF BIOMEDICAL ENGINEERING

Danilova V. A., Shlykov V. V.

TELEMEDICINE AND COMPUTER NETWORKS: LABORATORY WORKSHOP IN CISCO PACKET TRACER

Workshop on discipline for students of specialties 163 "Biomedical Engineering"

Kyiv
Igor Sikorsky Kyiv Polytechnic Institute
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

В.А. Данілова , В.В. Шликов

ТЕЛЕМЕДИЦИНА ТА КОМП'ЮТЕРНІ МЕРЕЖІ: ЛАБОРАТОРНИЙ ПРАКТИКУМ У CISCO PACKET TRACER

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за спеціальністю 163 «Біомедична інженерія»

Київ
КПІ ім. Ігоря Сікорського
2021

Рецензент	*Богомолов М.Ф.,* к.т.н., доцент кафедри БМІ КПІ ім. Ігоря Сікорського, *Дубко А.Г.*, к.т.н., доцент, наук. співроб. відд. зварювання та споріднених технологій в медицині та екології Інституту електрозварювання ім.Є.О.Патона
Відповідальний редактор	*Зубчук В.І.*, к.т.н., доц., доцент кафедри біомедичної інженерії КПІ ім. Ігоря Сікорського

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 1 від 16.09.2021 р.)
за поданням Вченої ради факультету біомедичної інженерії
(протокол № 16 від 30.08.2021 р.)

Данілова Валентина Анатоліївна, старший викладач,
Шликов Владислав Валентинович, д-р техн. наук, доц.

ТЕЛЕМЕДИЦИНА ТА КОМП'ЮТЕРНІ МЕРЕЖІ:

ЛАБОРАТОРНИЙ ПРАКТИКУМ У CISCO PACKET TRACER

«Телемедицина та комп'ютерні мережі: Лабораторний практикум у Cisco Packet Tracer»: навч. посіб. для студ. спеціальності 163 - «Біомедична інженерія» / уклад. В.А. Данілова, В.В. Шликов; КПІ ім. Ігоря Сікорського.– Київ: КПІ ім. Ігоря Сікорського», 2021. – 70 с.

Навчальний посібник розроблено для отримання студентами практичних навичок з проектування та налаштування комп’ютерних мереж. Навчальне видання призначене для студентів, які навчаються за спеціальністю 163 – «Біомедична інженерія» факультету біомедичної інженерії КПІ ім. Ігоря Сікорського.

Telemedicine and Computer Networks: Laboratory workshop in Cisco Packet Tracer: workshop on discipline for students of specialties 163 «Biomedical Engineering» / V.A. Danilova, V. V. Shlykov; Igor Sikorsky Kyiv Polytechnic Institute.– Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2021. – 70 p.

Educational and methodical edition

TELEMEDICINE AND COMPUTER NETWORKS: LABORATORY WORKSHOP IN CISCO PACKET TRACER

Workshop on discipline for students of specialties 163 "Biomedical Engineering"

Authors: ***Valentyna Danilova***, Senior Lecturer, Department of Biomedical Engineering,
Vladyslav Shlykov, Doctor of Engineering, Associate Professor.

Editor-in-Chief: *Viktor Zubchuk,* Ph.D., Associate Professor

Reviewers: *M.F.Bogomolov,* Ph.D., Associate Professor,
A.G Dubko, Ph.D., Associate Professor,
Researcher of Department of Welding and Related Technologies in Medicine and Ecology

Edited by the authors

CONTENT

INTRODUCTION

Computer networks appeared relatively recently, in the late 60's of last century. However, they have brought something completely new to the telecommunications world - the inexhaustible reserves of information created by civilization, which are replenished at an increasing rate.

The availability of computer networks in combination with powerful and compact computing and communication tools allows us to take a new step towards the development of mobile computing and communications, "cloud" technologies.

The discipline "Telemedicine and computer networks" is designed to study the basic principles, methods and means of building computer networks, including the structural organization of local and global networks, the architecture of network operating systems and network technologies.

The guidelines include a series of partially interrelated labs, during which students have the opportunity to gain experience with the Cisco Packet Tracer environment.

Before performing laboratory work, students must:

- to get acquainted with methodical instructions;
- to repeat the lecture material related to laboratory work;
- prepare answers to the questions given in the guidelines at the end of each laboratory work.

After completing these tasks, the student must demonstrate to the teacher the work on the computer, draw up a report on the results of this laboratory work, defend it and pass it to the teacher.

LABORATORY WORK №1.

Topic: Cisco Packet Tracer simulation environment

Purpose: Learn about Cisco Packet Tracer for computer network simulation.Learn the interface of the program, its main functionality, gain practical skills in the basic configuration of network devices.

Theoretical information

Today in the IT market there are such well-known networks

simulators like:

• BOSON NET SIM;

• CISCO Router eSim;

• Cisco Packet Tracer;

• Network Emulator;

• Dynamips;

• Cisco 7200 Simulator.

Of these, the most common in terms of use for training are Boson NetSim, Cisco Packet Tracer and Network Emulator. We will focus on the Cisco Packet Tracer.

This software product was developed by Cisco and is recommended for use in the study of telecommunications networks and network equipment. Packet Tracer is flexible software that is a tool for modeling and visualizing the operation of IP networks. It is designed to teach network technologies and to assess students' knowledge.

Packet Tracer has the following features:

• modeling of logical topology: workspace for

• to create networks of any size;

• real-time simulation;

• simulation mode;

• modeling of physical topology: interaction with physical devices, using such concepts as city, house, etc .;

• GUI, necessary for a quality understanding of network organization, the principles of devices;

• multilingual support: the ability to translate this software product into almost any language;

• images of network equipment with the ability to add or remove various components;

• The presence of the Activity Wizard allows you to create network templates and use them later.

With this software product, you can build and configure networks and troubleshoot them. This simulator allows you to design your own networks, creating and sending various data packets, save and comment on your work.

Once the network is designed, you can proceed to configure the selected devices using terminal access or the command line. To build a network model, Packet Tracer allows you to model the main types of network equipment: computers, servers, Ethernet switches, routers, etc. A variety of network configurations can be created by "dragging" active network elements from the network component panel to the workspace and connecting them with cables and communication channels.

Each unit of equipment must be configured accordingly to power the network. The hardware is configured using a graphical interface (the interface window appears when you left-click on the hardware icon image). For Cisco routers and Catalyst switches, only the master settings can be set using the graphical interface. The main amount of router configuration is provided by the Command Line Interface (CLI).

The CLI interface reproduced by Packet Tracer corresponds exactly to the interface of real Cisco Systems equipment.

After starting the Packet Tracer program, the main program window opens (Fig. 1.1).

The main program window contains 6 main menus, 4 of which are used most often.

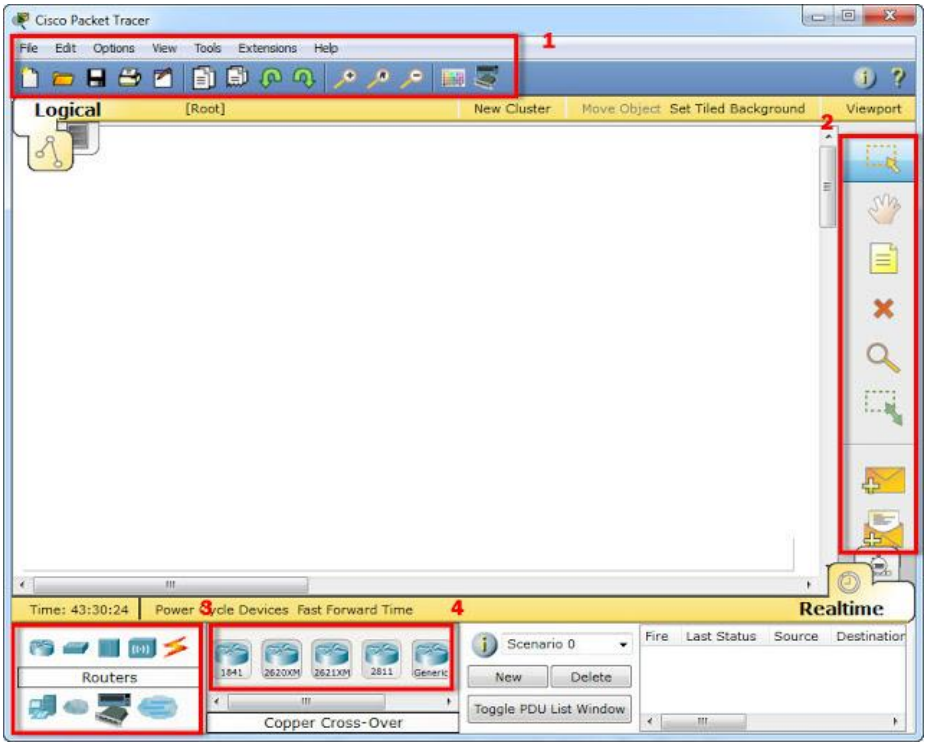

Fig. 1.1 - Cisco Packet Tracer interface

The main menu of the program (1) contains:

• File - contains operations of opening / saving documents;

• Corrections - standard operations "copy / cut, cancel / repeat";

• Settings;

• View - the scale of the workspace and toolbar;

• Tools - color palette and customization of end devices;

• Expansion - project wizard;

• Help;

The right graphical menu (2) contains fairly recognizable tool icons for working with the project and project objects. Each of the tools located in this menu is activated by clicking the mouse on the corresponding icon, and, for faster access, you can use the keyboard.The first menu tool (top to bottom) Select (shortcut - [Esc]).

Fig. 1.2 - Select menu tool

As with most other programs, it is used to select one or more objects. Usually for further moving, copying or deleting.

The next tool in this graphical menu, Move Layout ([M]), is used to scroll through large projects.

Fig. 1.3 - Move Layout menu tool

Although the main program window used to build a project has scroll bars, having an additional tool with a similar function, which is activated with a single keystroke, can be very convenient when working with large topologies.

The Place Note tool ([N]) adds a signature to any part of the project. It is convenient to use for comments or to place the basic information of the script directly in the project for further work.

Fig. 1.4 - Place Note menu tool

The Delete ([Del]) tool deletes an object or group of objects.

Fig. 1.5 - Delete menu tool

The Inspect tool ([I]), looking like a magnifying glass, is not used to enlarge project objects.

Fig. 1.6 - Delete menu tool

This tool allows, depending on the type of device, to view the contents of the ARP table, routing table, NAT table, etc.

Located at the bottom of this menu, the tools Add Simple PDU ([P]) and Add Complex PDU ([C]) are designed to emulate sending with subsequent tracking of any data packet within the project.

Fig. 1.7 - Add Simple PDU and Add Complex PDU menu tool

The two graphical menus (3 and 4) located in the left corner of the program are the most used.

Menu 3 allows you to select the type of device, and menu 4 directly the device itself. The most used are:

Routers - allows you to add Cisco routers to the project. Cisco 1841, Cisco 2820 XM, Cisco 2821 XM, Cisco 2811 are available in Cisco Packet Tracer 5.3.3.

The router is used to find the optimal route for data transmission based on special routing algorithms, such as selecting a route (path) with the least number of transit nodes. OSI models work at the network level.

Fig. 1.8 – Router

Switches - used to add switches. The following Cisco Catalyst WS-C2950-24, Cisco Catalyst WS-C2950T-24, Cisco Catalyst WS-C2960-24TT models are available.

Switches are devices that operate at the channel level of the OSI model and are designed to combine multiple nodes within one or more network segments. The switch transmits packets on the basis of an internal table - the switching table, so the traffic goes only to the MAC address to which it is assigned, and not repeated on all ports (as on the hub).

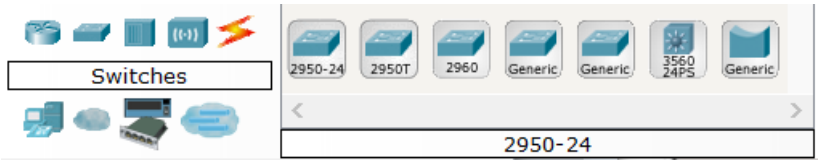

Fig. 1.9 - Switch

The hub repeats the packet received on one port on all other ports.

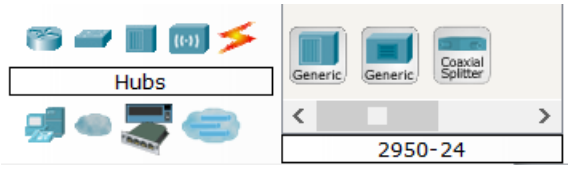

Fig. 1.10 - Concentrator

Wireless Wi-Fi technologies and networks based on them. Includes access points.

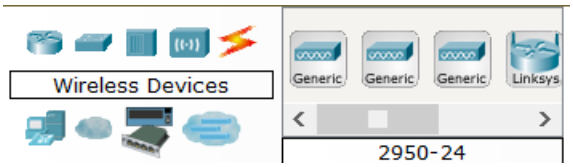

Рис. 1.11 — Точки доступу

Connections - select the connection type for project topology objects.

With the help of these components, connections are created into a single circuit. Packet Tracer supports a wide range of network connections. Each cable type can only be connected to certain types of interfaces.

Fig. 1.12 - Communication lines

Connection - different types of connections between devices:

1. Auto - automatically determines the type of connection (automatically determines the best way to connect devices).

2. Console - connection using a console cable (COM port on a PC and Console input on Cisco devices). The console connection can be made between the PC and the routers or switches. Some requirements must be met for a console session to work with a PC: the connection speed on both sides must be the same, there must be 7 bits of data (or 8 bits) for both parties, the parity control must be the same, there must be 1 or 2 steppe bits (but they don't have to be the same), and the data flow can be anything for both parties.

3. Copper Straight-Through - connection with a cable type twisted pair straight. This type of cable is a standard Ethernet transmission medium for connecting devices that operate at different levels of OSI. It must be connected to the following types of ports: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) and copper 1000 Mbps (Gigabit Ethernet).

4. Copper Cross-Over - the connection with a cable type twisted pair cross. This type of cable is an Ethernet transmission medium for connecting devices that operate at the same OSI levels. It can be connected to the following types of ports: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) and copper 1000 Mbps (Gigabit Ethernet).

5. Fiber - connection using a fiber-optic communication line (FOC). An optical medium is used to connect between optical ports (100 Mbps or 1000 Mbps).

6. Phone - connection via a telephone line. A telephone line connection can only be made between devices that have modem ports. The standard view of a modem connection is an end device (such as a PC) that is dialed into the network cloud.

7. Coaxial - connection with a coaxial cable. A coaxial medium is used to connect between coaxial ports, such as a cable modem connected to the Packet Tracer cloud.

8. Serial DCE and Serial DTE - serial communication channels. Serial ports are often used for WAN connections. To set up such connections, you must set up synchronization on the DCE side. DTE synchronization is optional. The DCE side can be identified by a small "clock" icon next to the port. When you select the Serial DCE connection type, the first device to which the connection is applied becomes a DCE device, and the second automatically becomes a DTE party. The reverse arrangement of the sides is also possible if the Serial DTE connection type is selected.

End devices - selection of end devices. Personal computers, laptops, IP phones and servers.

Fig. 1.13 - Terminal devices

The network is created by selecting the required active network components in the component panel and placing them on the workspace, as well as connecting the components with cables. Cables are also taken from the component panel.

To select a component, you must: a) click on it with the left mouse button in the components panel, b) click on the workspace, to the desired location of the component.

To connect the cable you need to: a) click on the image of the cable, b) click on the image of the component to which you want to connect the cable - an image of free interfaces of the component will appear, c) click on the image of the connected interface, d) similarly connect the second the end of the cable to the required interface of the second component.

In the workspace, network components can move freely and can be deleted.

Laboratory task

Make a network with a topology from fig. 1.14, configure computer 0 and computer 1, check that the settings are correct.

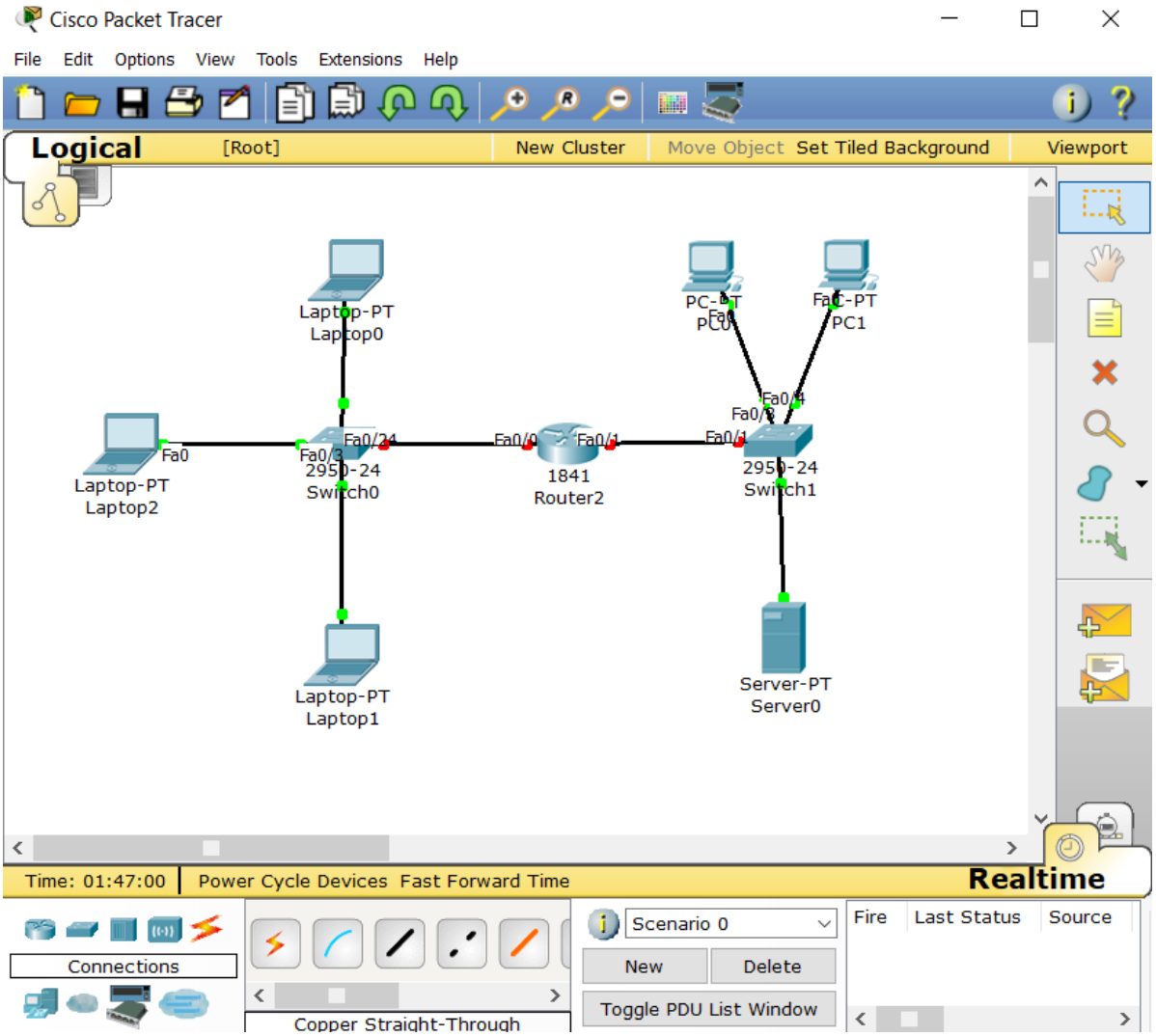

Fig. 1.14 - Network topology

Progress:

1. Add a router to the project.

In order to add a router to the network project, you need to left-click on this type of equipment, also select the model and add to the project by clicking on the work field of the program. The whole process of adding a new unit is done in three clicks.

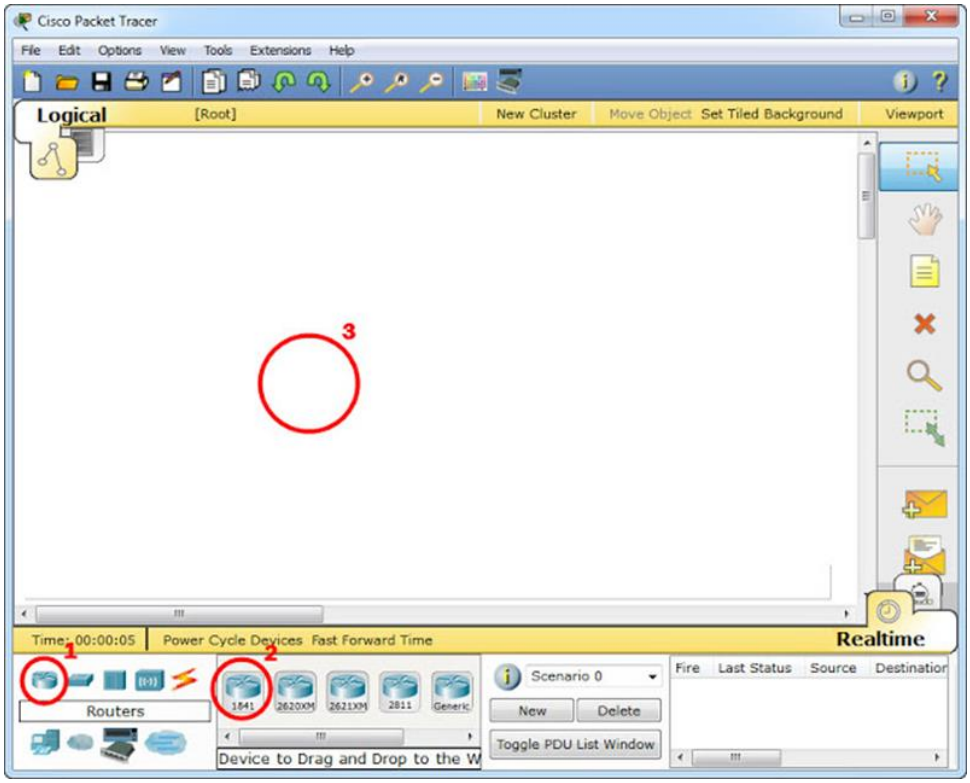

Fig. 1.15 - Adding a router

2. Adding a switch to the project.

Adding a switch to a project is almost identical to adding a router. Differences in the initial stage when selecting the panel and in the window of the parameters of the added device.

3. Adding end devices: computers, laptops, server.

Network endpoints, such as servers, workstations, and laptops, are added to the topology identically to other project devices.

4. Connect devices.

After all the necessary devices for the selected scenario of laboratory work are added to the project, it is necessary to connect all units of equipment among themselves according to the scenario. To do this, use the Connections menu.

The choice of cable depends on the equipment to be connected and the connection technology. In this particular case, it will be Copper Straight-Through. Each time you connect the equipment, you will be offered a choice of interface, if any are available and do not participate in another connection.

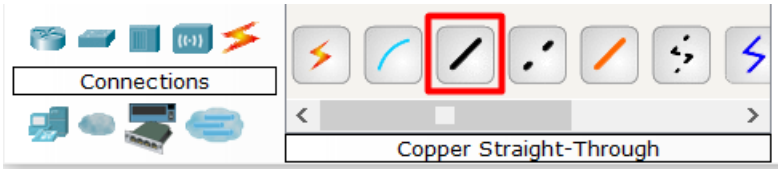

Fig. 1.16 - Select connection type

5. Set up computers.

Now you need to configure the static IP address of the computer, for this click on the first double click and go to the Desktop menu and select IP Configuration.

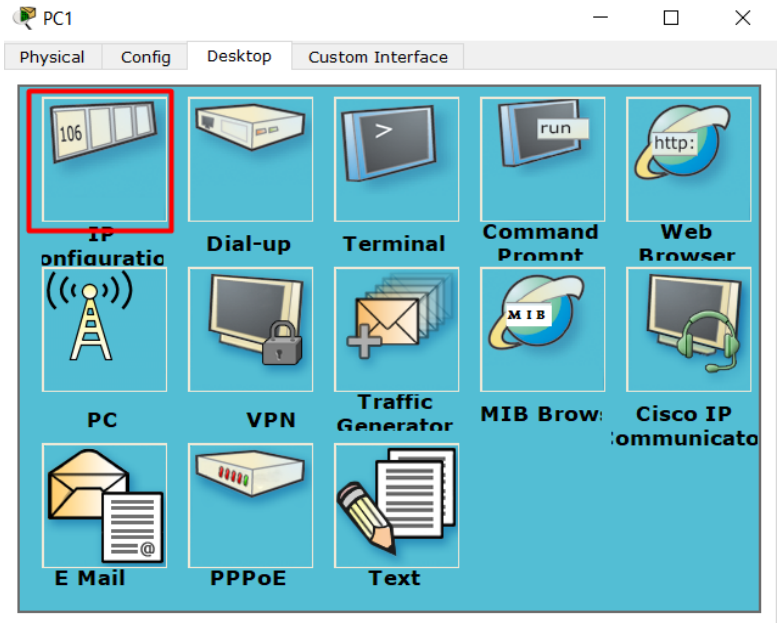

Fig.. 1.17 — IP Configuration

Now you need to specify the IP address and mask under the network. For computer 1: 192.168.1.2 and mask 255.255.255.0.

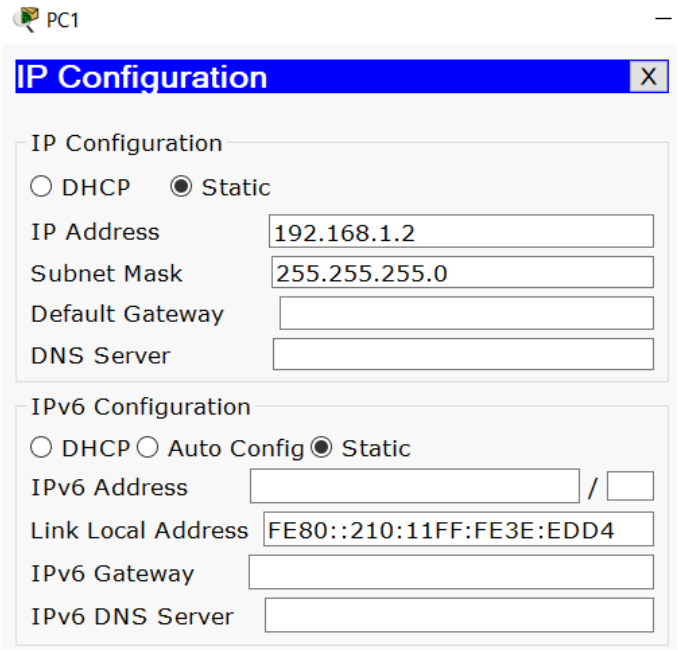

Fig. 1.18 - PC1 settings

For computer 0: 192.168.1.1 and mask 255.255.255.0.

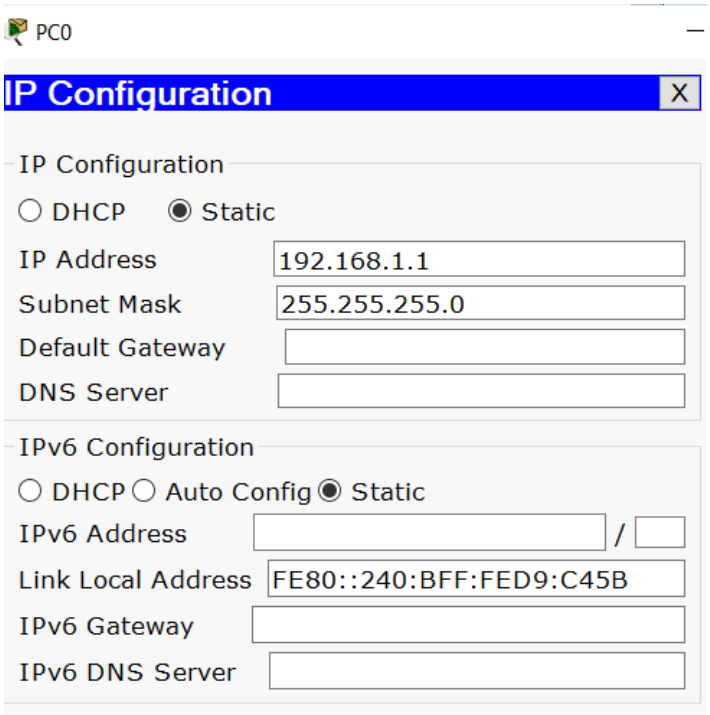

Fig. 1.19 — Налаштування PC0

To check if there is a connection between the two computers, select Command Prompt on one of the computers.

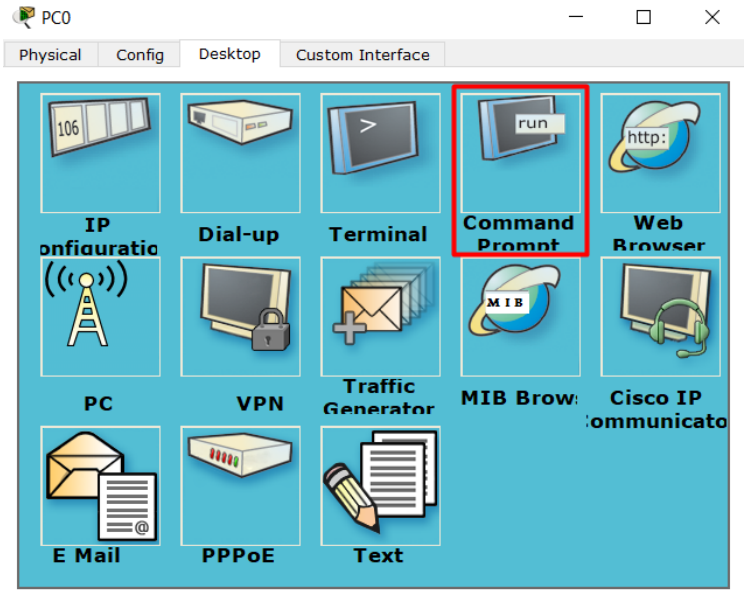

Fig. 1.20 —PC0: Command Prompt

And enter the command Ping the IP address of another computer.

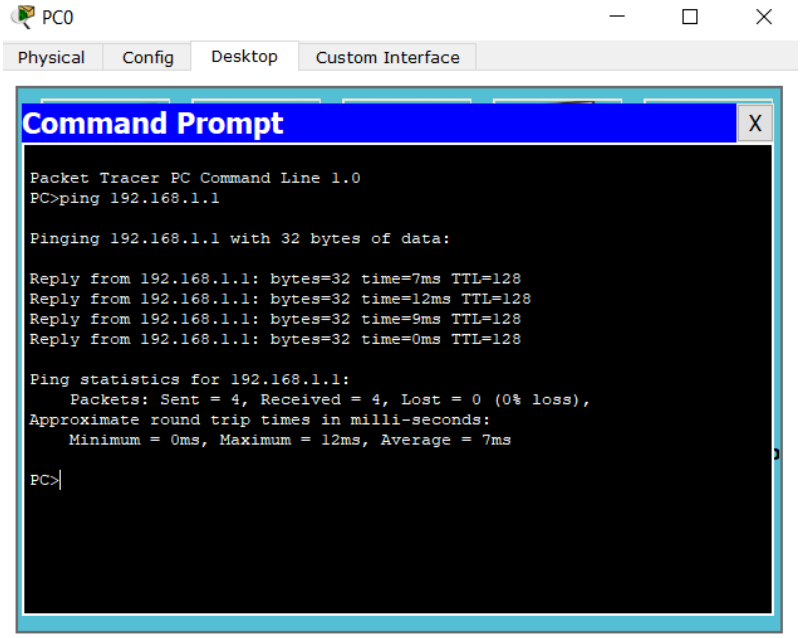

Fig. 1.21 —PC0: Command Prompt

We receive a message that 4 packets have been sent, 4 received and the transmission time.

Control questions

1. What is the purpose of Cisco Packet Tracer?
2. What network simulators do you know?
3. What types of network connections do you know in Packet Tracer?
4. What is the purpose of the ip config utility?
5. What is the purpose of the ping utility?
6. Which cable should be used when connecting two PCs together?
7. At what level of the OSI model does the switch work?

LABORATORY WORK №2.

Topic: Static routing

Purpose: to get acquainted with the main features of the Cisco Packet Tracer environment; acquire skills to configure packet routing using static routes.

Theoretical information

Routing - the process of determining the route of information between networks. The router makes a decision based on the IP address of the packet recipient. In order to forward the packet, all devices on the path use the recipient's IP address. To make the right decision, the router must know the directions and routes to remote networks.

When using static routing, routes are set manually by the administrator.

Because static routes are configured manually, any changes in the network topology require administrator involvement to add and remove static routes according to the changes. On large networks, maintaining manual routing tables can be time consuming for the administrator. In small networks it is easier to do. Static routing does not have the scalability that dynamic routing has due to additional administrator configuration and intervention requirements. But even in large networks, static routes are often configured for special purposes in combination with dynamic routing protocols, because static routing is more stable and requires a minimum of router hardware resources to service the table.

Static routing has the following **features:**

1. Provides routing support for small networks that are not expected to expand significantly;
2. Provides routing for the final (dead-end) network;
3. Specifies a single default route to any network, unless the network contains a more specific path.

Advantages of static routing:

1. Minimal CPU usage;
2. Easier for the administrator to understand;
3. Easier to configure in small networks;
4. Predictability at any time.

Disadvantages of static routing:

1. Configuration and maintenance takes a long time;
2. Errors are possible during configuration (especially in large networks); administrator intervention is required to support the replacement of route information;
3. With the growth of the network scales poorly; requires proper knowledge of the entire network for proper execution.

Example of static routing settings

In fig. 2.1 shows a topology with three subnets. To configure static routing in this case, follow these steps:

1. Configure the IP address, subnet mask, gateway IP address and DNS server IP address on each end device (computers, laptops, servers);
2. Configure similarly to the end devices each of the router interfaces;
3. Configure static routes for each of the subnets on the router.

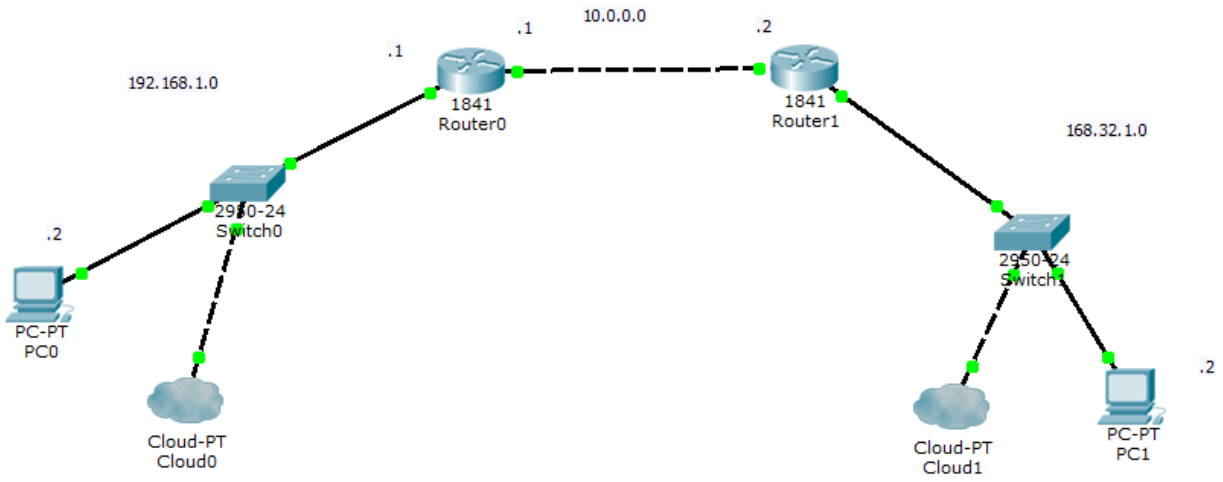

Fig. 2.1 - Topology with three subnets

Consider the example of setting up the end device on the example of a computer PC0 (Fig. 2.2).

In fig. 1.2 shows the Desktop tab of the PC0 setup menu. To set the necessary settings for it, you need to go to the IP Configuration menu. In this case, a window will open, shown in Fig. 2.3.

That is, for each of the devices you need to set settings similar to those shown in Fig. 2.3.

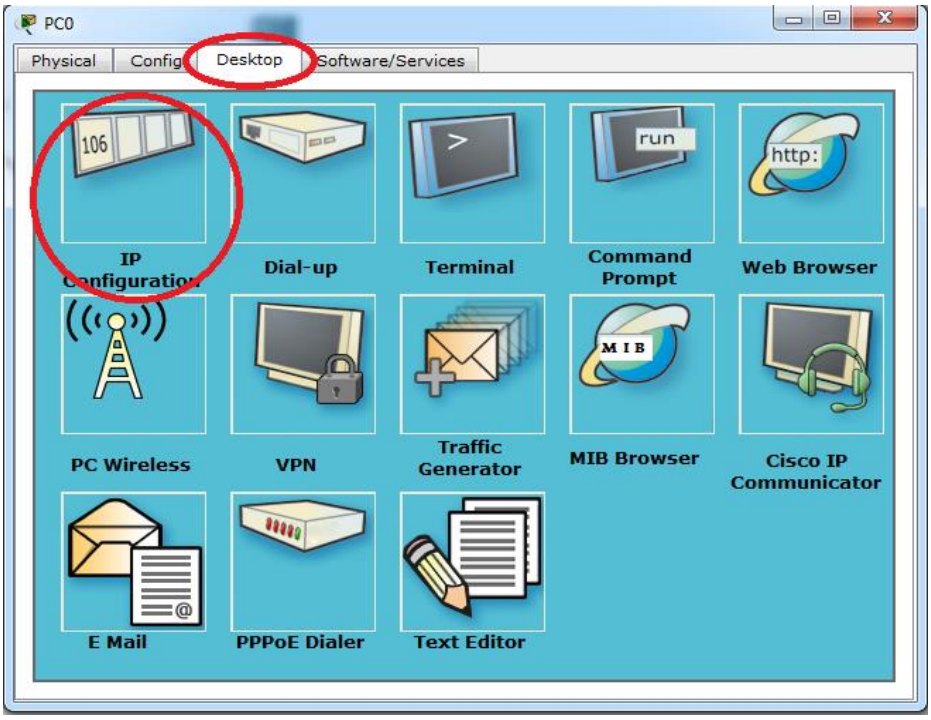

Fig. 2.2 - Location of the computer settings menu

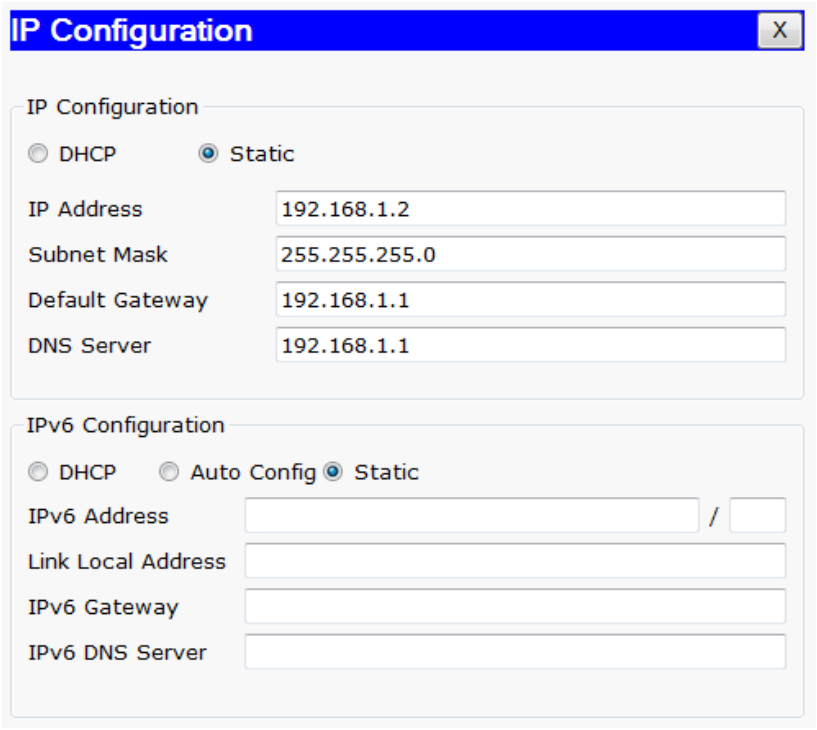

Fig. 2.3 - PC0 computer settings

The router is configured as follows:

Router>enable

Router#conf igure terminal

Router(config)#interface fa0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#int fa0/1

Router(config-if)#no shutdown

Router(config-if)#ip address 10.0.0.1 255.255.255.252

Router(config-if)#exit

Router(config)#ip route 168.32.1.0 255.255.255.0 10.0.0.2

Consider the commands that were used to configure the router:

- *enable* – used to access the router configuration mode, enter the administration mode
- *configure terminal* – transition to router configuration mode;
- *interface fa0/0* – transition to the configuration mode of the fa0 / 0 interface;
- *no shutdown* – turn on the interface (supply power to it);
- *ip address < IP address>< subnet mask >* – set the router interface IP address and subnet mask;
- *exit* – go back one level of configuration;
- *ip route < The IP address of the network you want to access > < the network mask you want to access > < IP address of the router interface, through which access to the desired network is obtained >* - command to configure a static route.

Router1 is configured similarly.

Laboratory task

The computer network has the structure shown in Fig. 2.4:

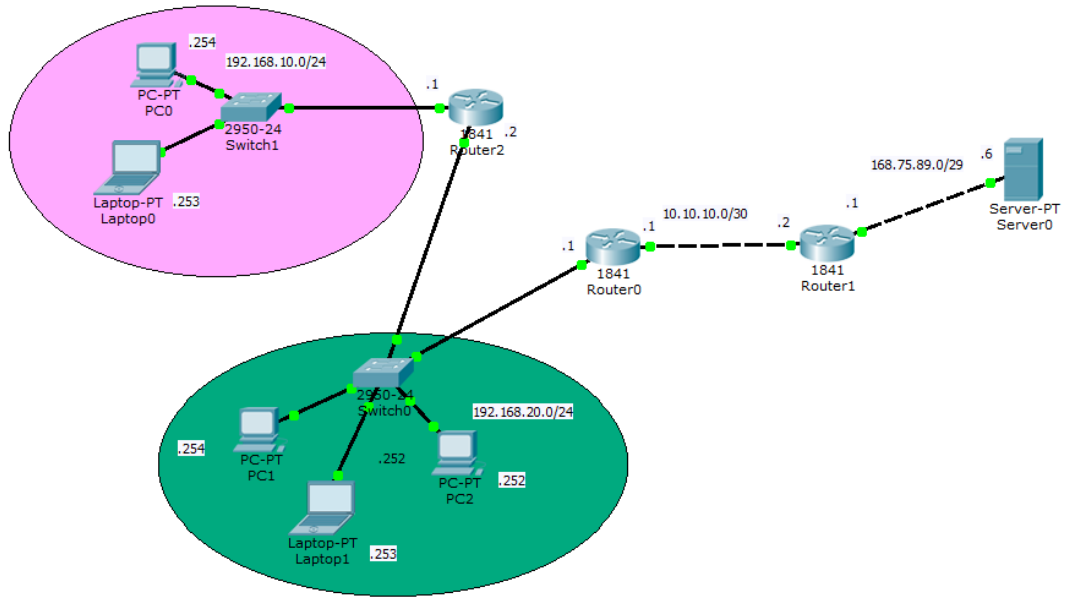

Fig. 2.4 - Topology of the task for laboratory work №1

There are four networks: 192.168.10.0/24, 192.168.20.0/24, 10.10.10.0/30 and 168.75.89.0/29. To ensure communication between networks, you need to configure static routes on each of the routers that are not directly connected to the networks. You must configure static routing between all networks.

Progress:

1. For each of the end devices (laptops, computers, and servers), you must set the IP address for that device, the subnet mask, the gateway IP address, and the DNS server IP address. The required IP addresses are listed next to each of the devices.

2. For all routers in the topology it is necessary to set IP addresses and subnet masks for each of the interfaces.

3. Configure static routes on each of the routers that are not directly connected to the networks. To lay static routes, you must use the following command:

ip route [IP address of the network to which we route] [subnet mask] [IP address of the interface through which we access]

4. Check the operation of routing by sending packets.

Control questions:

1. What is routing?
2. Define the concept of static routing.
3. Specify the features of static routing.
4. Give the advantages of static routing.
5. What are the disadvantages of static routing?
6. Specify the algorithm for setting up static routing in the network.
7. What commands are needed to configure static routing?
8. Name the purpose of the IP address and subnet mask.

LABORATORY WORK №3

Topic: DHCP protocol

Purpose: to get acquainted with the DHCP protocol, to acquire practical skills in setting up DHCP servers.

Theoretical information

Dynamic Host Configuration Protocol (DHCP) is an application-level protocol that allows computers to automatically obtain the IP address and other parameters required to operate on a TCP / IP network. This protocol works on the "client-server" model, ie a special DHCP server responds to client requests. The role of such a server can be a server (any computer with configured appropriate software) and a router (router, router). The range of addresses distributed by the DHCP server is usually specified by the network administrator. This range is called the pool (pool) of DHCP addresses. DHCP is used in most large TCP / IP networks. In addition to the IP address, DHCP can also inform the client of additional parameters required for normal network operation. These parameters are called DHCP options, of which the most commonly used are: default gateway IP address, DNS server address, DNS server domain.

There are the following **types of distribution of IP addresses** by DHCP:

1. Manual allocation - the network administrator manually determines the IP address for each MAC address;

2. Automatic distribution - the client is given any available IP address for permanent use;

3. Dynamic distribution - similarly to the previous case, the client is given any free IP address, but not for permanent use, but for a certain period, after which the IP address is again considered free.

It is clear that the latter type of distribution is the most flexible and requires a minimum of attention from the network administrator. That is why it is the most common.

Also, it should be noted that in the case of dynamic distribution, if the end device has received an IP address and is actively using it, then at the end of its "lease" it will be extended. However, if the computer stops sending packets marked with this address (it is turned off or disconnected from the network), then after running into possession of the IP address, it will return to the pool of available addresses, and can be provided to another device.

The DHCP protocol is a client-server, ie the DHCP client and the DHCP server take part in its work. Data transfer is based on the UDP protocol. The server receives requests on port 67, and clients receive messages on port 68.

To perform its functions, DHCP uses **the following message**s:

1. Find DHCP (DHCPDISCOVER) - broadcast request (own IP address = 0.0.0.0, destination IP address = 255.255.255.255), a client to search for an available DHCP server;

2. DHCP offer (DHCPOFFER) - after the server receives the request, it sends a packet with the proposed configuration;

3. DHCP Request (DHCPREQUEST) - by selecting one of the configurations that was offered by DHCP servers, the client sends a request to the server, which contains the address selected by the client;

4. DHCP Confirmation (DHCPACK) - the server confirms the client's request, after which the client can configure its interface according to the selected configurations.

Also, DHCP has several **other messages** for rejection, cancellation, release from the proposed configuration and a request for additional parameters:

1. DHCP failure (DHCPDECLINE) - if while holding a packet of the DHCPPACK type, the client finds a device with a similar address in the network, it sends a message of this type, after which the address request procedure is repeated.

2. Cancel DHCP (DHCPNACK) - the server cannot provide the client with the IP address that he requested in the request.

3. DHCP release (DHCPRELEASE) - the client terminates the lease of the IP address.

4. DHCP information (DHCPINFORM) - a type of message designed to hold additional network parameters, DNS server address, default gateway, etc.

DHCP is widely used in modern computer networks due to its advantages, but there are some disadvantages.

The advantages of using the DHCP protocol are:

1. Reliability of adjustment - as a rule, automatic adjustment is more reliable as there is no human factor;

2. Reduced time to configure the network.

Disadvantages of DHCP:

1. Low level of security, which is due to the use of UDP and IP protocols;

2. Networks are not protected from the appearance of unauthorized DHCP servers on the network;

3. Relatively frequent protocol failures.

Example of DHCP protocol:

The IP addresses that will be distributed by the DHCP server are stored in the DHCP pool. An example of setting up such a pool of addresses is shown in Fig. 3.1. You must specify the Pool Name, Default Gateway, DNS Server IP Address, Pool

Start Address, Subnet Mask, and the maximum number of addresses that can be distributed.

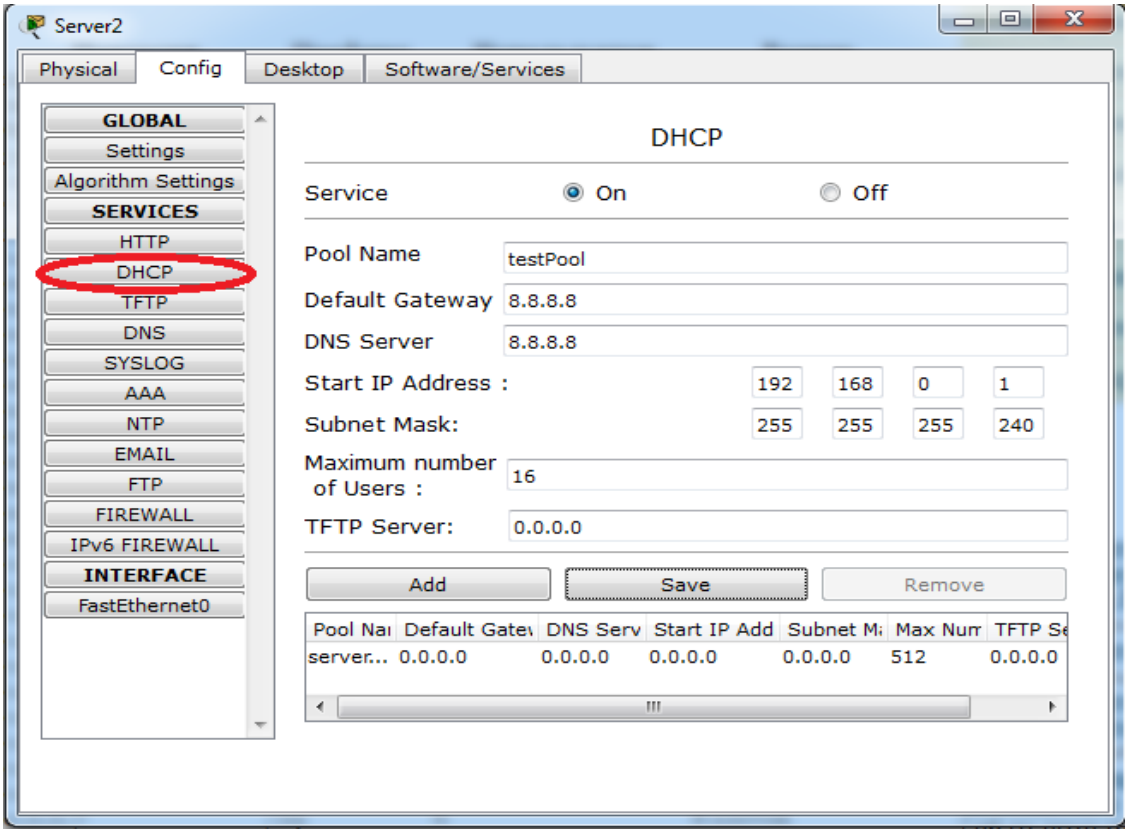

Fig. 3.1 - Example of setting up a DHCP pool

The router can also act as a DHCP server. Configuring the DHCP protocol on the router is performed using the following commands:

- int [router interface name] - switch to interface configuration mode;

- ip add dhcp - DHCP interface settings;

- ip dhcp pool [pool name] - create a pool with the specified name;

- network [subnet mask] [subnet IP address] - use the network IP addresses with the specified parameters for distribution;

- default-router [IP address of the router interface in the subnet] - set the default port for this pool;

- dns-server [DNS server IP address] - set the DNS server address for this pool.

Example:

Router (config) #ip dhcp pool routerPool

Router (dhcp-config) #network 192.168.0.0 255.255.255.240

Router (dhcp-config) # default-router 8.8.8.8

Router (dhcp-config) # dns-server 8.8.8.8

It is often necessary to remove from the pool addresses that are already assigned to the interfaces of the router or end device. The following command is used for this:

- ip dhcp excluded-address [IP address to be excluded from the pool] - exclusion of the IP address from the pool.

Example:

Router (config) #ip dhcp excluded-address 8.8.8.1

Laboratory task

The computer network has the structure shown in Figure 3.2.

There are two networks: 192.168.10.0/24 and 192.168.15.0/24. The task of the laboratory work is that the end devices in the network 192.168.10.0 must be configured using the DHCP protocol, which is configured and activated on Server0. Computers on the 192.168.15.0 network receive settings from Roter0.

Note that the router interface on the 192.168.10.0 network also receives configuration from the server using DHCP.

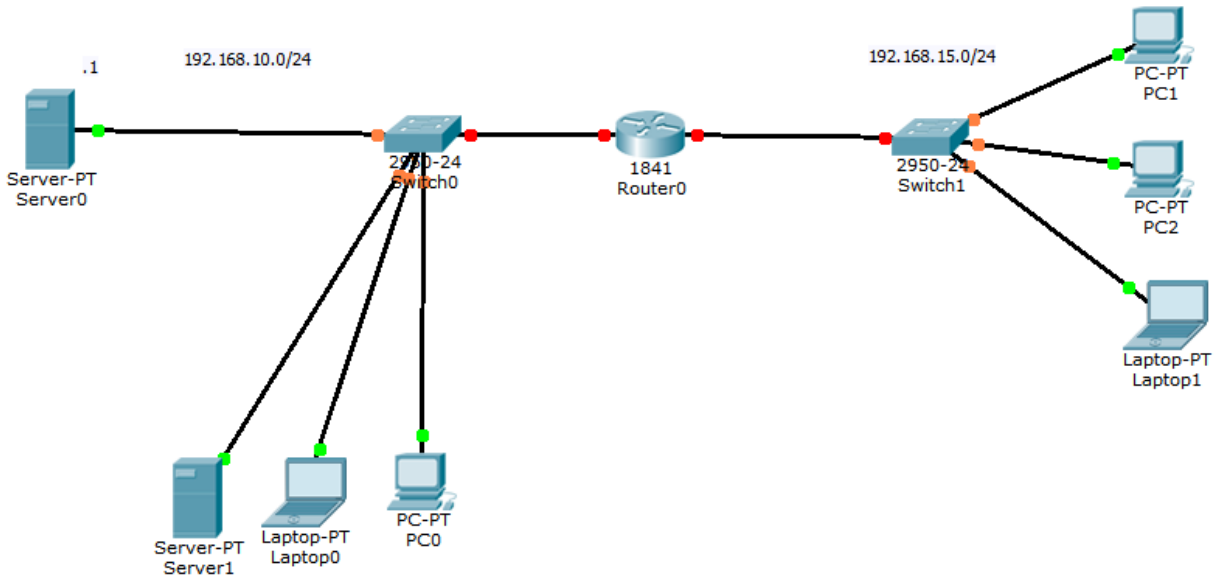

Fig. 3.2 - The structure of the computer network

Progress:

1. Activate the DHCP protocol on the server and configure the pool as specified in the task.

2. Configure the router.

3. The interface of the router, which is connected to the subnet with a DHCP server, must obtain an IP address via DHCP.

4. For another interface, manually configure the IP address as specified in the task.

5. Create a DHCP pool on the router (the required parameters are specified in the task).

6. Exclude from the pool the address occupied by the router interface.

7. All end stations must receive settings via DHCP.

Control questions

1. Why is the DHCP protocol intended?
2. Specify the features of the DHCP protocol.
3. What is a DHCP pool?
4. What parameters are specified when setting up the DHCP protocol?
5. What commands are used to configure DHCP on the router?
6. What command is used to exclude an IP address from a DHCP pool?
7. Specify the benefits of using DHCP.
8. List the disadvantages of using the DHCP protocol.
9. Is DHCP used in modern computer networks?

LABORATORY WORK №4

Topic: Configuring NAT technology

Purpose: to get acquainted with the technology of translation of NAT network addresses and gain practical skills in its configuration using the Cisco Packet Tracer software environment.

Theoretical information

NAT (Network Address Translation) is a mechanism used in TCP / IP networks to convert the IP addresses of packets passing through a given network.

There are **three modes** of NAT technology:

1. Static NAT - one IP address is replaced by another IP address (to each other);

2. Dynamic NAT - replacement of an unregistered address with one of the addresses of the reserved group (many to many);

3. Overloaded NAT - a type of dynamic NAT, when several unregistered addresses use the same IP address, using different ports (many to one).

NAT is designed to perform **the following functions:**

1. Saving IP addresses - addresses within the network can be replaced by one external public address;

2. Restriction of packets within the network;

3. Filtering of source packets;

4. Providing the ability to restrict access to certain servers within the network.

But this technology also has **certain drawbacks**, such as problems with user identification and incompatibility with older protocols.

NAT technology settings

The following commands are used to configure NAT on the router:

- ip nat inside source static [IP address of the interface through which we access] [IP addresses in the network to which network addresses are broadcast] - activation of NAT in static mode;

- ip nat inside source list [list number] [list IP addresses] overload - activation of NAT in overload mode;

- ip nat inside - specify the interface directed "in the middle" of the network whose IP addresses need to be changed (used in the interface configuration mode);

- ip nat outside - specify the interface that is directed "outwards" (used in the interface configuration mode).

Laboratory task

There are two networks: internal 192.168.10.0/24 and external 192.168.20.0/24. Routing between networks is provided by Cisco 1841 routers, which form a subnet 87.14.58.0/30. To ensure access of clients from the internal network to the resources of the external network on routers, you need to configure the translation of network addresses using NAT technology. The structure of the computer network is shown in Fig. 4.1.

As a result, the packets after passing the router must change the destination IP address to the corresponding address of the router interface. The response packet must also change the destination IP address after passing the router.

Progress:

1. For each of the end devices (laptops, computers, and servers), you need to set the IP address of this device on the network, the network mask, the IP address of the

gateway, and the IP address of the DNS server. The required IP addresses are listed next to each of the devices.

2. Configure router interfaces (enable them and assign IP addresses and masks for networks).

3. Configure NAT in static mode on the Nat-Static router.

4. Configure NAT in overload mode on the Nat-Overload router.

5. Ensure that IP addresses are replaced on both subnets.

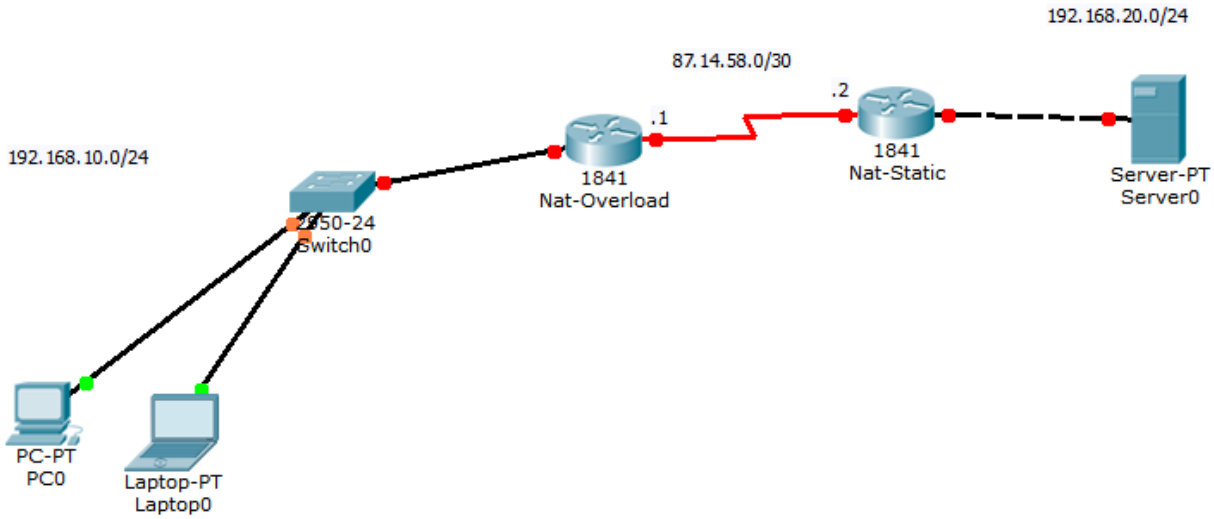

Fig. 4.1 - The structure of the computer network

Control questions

1. Specify the purpose of NAT technology.
2. What NAT modes exist?
3. List the commands you want to use when setting up NAT in static mode.
4. Specify the commands to use when configuring NAT in overload mode.
5. List the advantages of NAT technology.
6. Is NAT technology used in modern computer networks?

LABORATORY WORK № 5

Topic: Dynamic routing. RIP dynamic routing protocol

Purpose: to get acquainted with the basic concepts of dynamic routing; gain the skills to configure dynamic routing using the RIP protocol.

Theoretical information

Dynamic routing is a type of routing in which routes are calculated automatically using dynamic routing protocols or routing daemons. A dynamic routing daemon is a special program for calculating routes, usually it can use several different routing protocols. Such demons as Quagga, GNU Zebra, XORP, Bird are widespread. Common dynamic routing protocols are RIP, OSPF, EIGRP, IS-IS, BGP, HSRP and others. These protocols receive information about the topology and status of communication channels from other routers in the network.

Dynamic routing protocols are divided into two major groups:

1. Remote-vector protocols for dynamic routing (Disance-vector Routing Protocols);

2. Link-sate Routing Protocols.

The main difference between these protocols is that remote-vector protocols build a complete graph of a computer network in memory, while the protocols of the state of communication channels determine and use only the best routes.

Routing Information Protocol (RIP) is one of the routing protocols in small computer networks, which allows routers to dynamically update route information (direction and range in hops, hop), receiving it from neighboring routers.

A hop is a process of transmitting a packet between network nodes, on each hop the parameter of the TTL packet is reduced by one. The more hops - the longer and more difficult the route.

In this protocol, all networks have numbers (the method of number formation depends on the network layer protocol used in the network), and all routers have identifiers. The RIP protocol makes extensive use of the term "distance vector". The distance vector is a set of pairs of numbers that are network numbers and distances to them in hops.

Distance vectors are iteratively propagated by routers over the network, and after a few steps, each router has data about the networks available to it and the distances to them. If the connection to any network is lost, the router notes this fact by assigning the element of the vector corresponding to the distance to this network, the maximum possible value, which has a special meaning - "no connection". This value in the RIP protocol is the metric number 16. The maximum number of hops allowed by RIP is 15 (metric 16 means "infinitely large metric", ie unreachable network segment). By default, each RIP router notifies the network of its complete routing table every 30 seconds, generating quite a bit of traffic on low-speed lines.

The format of the RIP packet includes entries with routing information: command - command that determines the destination (1 - Request; 2 - Response), version - protocol version number (depending on the version, the packet format is determined), must be zero - the value must be zero, RIP Entry (RTE) - record RIP route information. The RIP protocol operates at the application layer of the TCP / IP stack using the UDP protocol and port 520.

Also, the RIP protocol has an authentication option. If it is enabled, only those packets that contain the correct authentication code are processed. This code is encrypted using the MD5 algorithm.

When using the RIP protocol, the Bellman-Ford algorithm (Bellman – Ford algorithm) works, and the solution found with its help is not optimal, but close to optimal. The advantage of the RIP protocol is its computational simplicity, and the

disadvantages are the increase in traffic when periodically sending broadcast packets and the suboptimal nature of the found route.

RIP routing protocol settings

The following commands are used to configure RIP remote vector routing:

- router rip - go to the configuration mode of the RIP protocol;

- network [IP address of the external network] - add a network that is not directly connected to the router for processing by RIP.

Consider the configuration of the dynamic routing protocol RIP in a simple topology, as shown in Fig. 5.1.

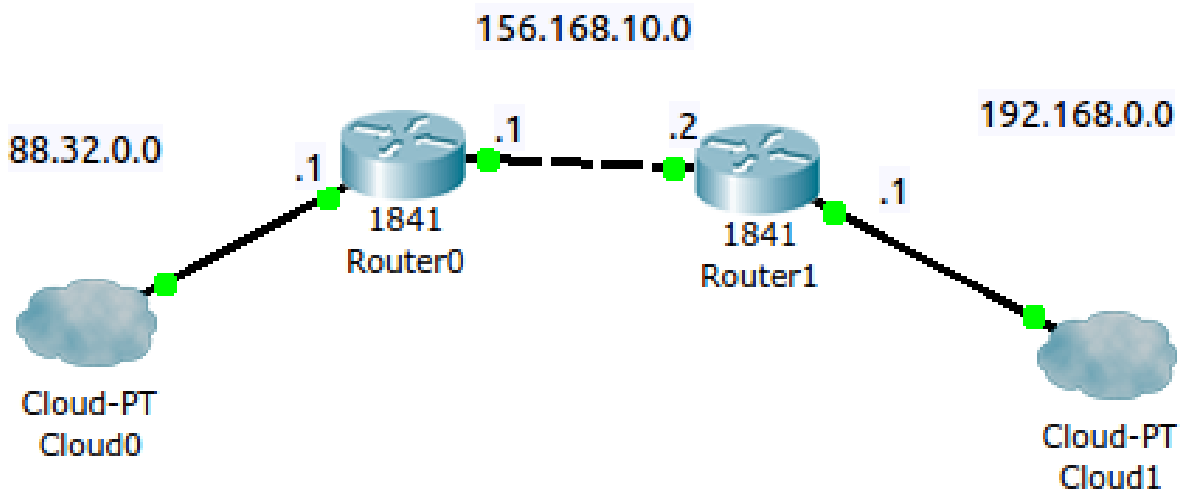

Fig. 5.1 - Simple topology for setting up dynamic routing

Router0:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 88.32.0.1 255.255.255.0

Router (config) #interface fastEthernet 0/1

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.1 255.255.255.0

Router (config-if) #exit

Router (config) #router rip

Router (config-router) #network 88.32.0.0

Router (config-router) #network 156.168.10.0

Router1:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.2 255.255.255.0

Router (config-if) #exit

Router (config) #interface fastEthernet 0/1

Router (config-if) #ip address 192.168.0.1 255.255.255.0

Router (config-if) #no shutdown

Router (config-if) #exit

Router (config) #router rip

Router (config-router) #network 192.168.0.0

Router (config-router) #network 156.168.10.0

Router (config-router) #exit

Laboratory task

There are three networks: 192.168.10.0/24, 192.168.20.0/24, 8.8.8.0/30. To ensure communication between networks, you need to configure routes on each of the

routers using the remote-vector RIP routing protocol. The structure of the network is shown in Fig. 5.2.

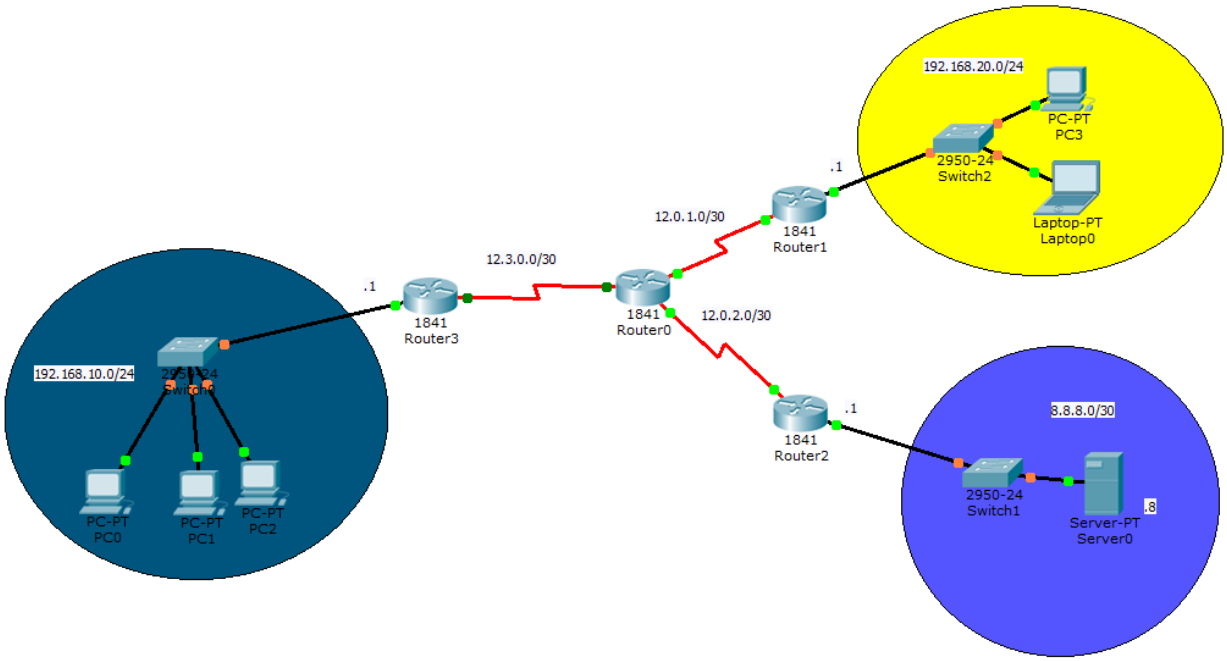

Fig. 5.2 - The structure of the laboratory work network

Progress:

1. For each of the end devices (laptops, computers, and servers), you need to set the IP address for that device, the network mask, the gateway IP address, and the DNS server IP address. The required IP addresses are listed next to each of the devices.

2. For all routers in the topology, you need to set the IP addresses and masks on the RIP domain for each of the interfaces.

3. Configure routing between all subnets using the RIP dynamic routing protocol.

Control questions

1. What is dynamic routing?
2. How is dynamic routing different from static routing?
3. What are the advantages of dynamic routing over static?
4. Does dynamic routing have disadvantages compared to static routing?
5. How do remote-vector protocols differ from state protocols?
6. Name the features of the RIP protocol.
7. Name the disadvantages and advantages of RIP.
8. Name the commands used when configuring the RIP protocol.

LABORATORY WORK № 6

Topic: Dynamic routing. OSPF dynamic routing protocol

Purpose: to get acquainted with the features of the OSPF protocol, to gain skills in setting up dynamic routing using the OSPF protocol.

Theoretical information

The Open Shortest Path First (OSPF) protocol is based on link-state technology, which uses Dijkstra's algorithm to find the shortest path.

Protocol operation algorithm:

1. Routers exchange hello packets through all interfaces on which OSPF is activated; if routers have a common channel, they become neighbors;

2. Routers that have become neighbors exchange routing tables;

3. Routers constantly report to neighboring routers the status of their channels;

4. Each router sends the received data on a condition of channels of other routers to the neighbors;

5. At the end of such packet exchange, all network routers have the same network channel state database;

6. Using the Dijkstra algorithm, each router, using the channel state database, calculates a graph that will describe the shortest path to each network node with it as the root;

7. On the basis of the found graph the router routing table is constructed.

The OSPF dynamic routing protocol uses the following **packet types:**

1. hello-package - designed to establish and maintain contact with neighbors;

2. Database Description - contains the contents of the database state of the router channel;

3. Link State Request - used to query part of the database of a neighboring router;

4. Link State Update - designed to notify other routers about the change in channel status;

5. Link State Acknowledgment - designed to confirm receipt of the Link State Update package.

The OSPF protocol calculates routes in IP networks, while maintaining other protocols for exchanging route information. Each router stores information about the state it thinks its neighbor is in. The router relies on neighboring routers and transmits data packets to them only if it is sure that they are fully operational. In addition to information about neighbors, the router in its ad lists the IP subnets to which it is connected directly. According to Dijkstra's algorithm, the router calculates the path not to a specific network, but to a router connected to this network. Each router has a unique identifier that is passed in the connection status announcement. This approach makes it possible not to spend IP addresses on point-to-point connections between routers to which workstations are not connected.

OSPF routing protocol settings

The following commands are used to configure the OSPF protocol:

- router ospf [process index] - go to the OSPF protocol configuration mode;

- network [external network IP address] [network mask] area [network index] - add a network for OSPF processing.

Consider the settings of the OSPF protocol in the network shown in Fig. 6.1.

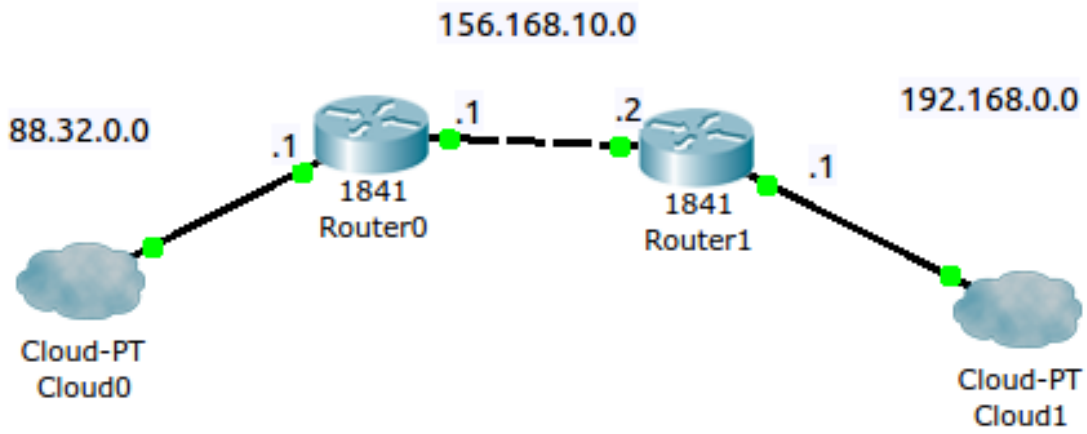

Fig. 6.1 - A simple topology with three subnets

Router0:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 88.32.0.1 255.255.255.0

Router (config) #interface fastEthernet 0/1

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.1 255.255.255.0

Router (config-if) #exit

Router (config) #router ospf 10

Router (config-router) #network 88.32.0.0 0.0.0.255 area 5

Router (config-router) #network 156.168.10.0 0.0.0.255 area 5

Router1:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.2 255.255.255.0

Router (config-if) #exit

Router (config) #interface fastEthernet 0/1

Router (config-if) #ip address 192.168.0.1 255.255.255.0

Router (config-if) #no shutdown

Router (config-if) #exit

Router (config) #router ospf 10

Router (config-router) #network 192.168.0.0 0.0.0.255 area 5

Router (config-router) #network 156.168.10.0 0.0.0.255 area 5

Laboratory task

There are three networks: 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 and a server in the 8.8.8.0/30 network. To ensure communication between networks, you need to configure routes on each of the routers using the OSPF dynamic routing protocol. The structure of the computer network is shown in Fig. 6.2.

Progress:

1. For all routers in the topology, you need to set the IP addresses and masks on the OSPF domain for each of the interfaces.

2. For each of the end devices (laptops, computers, and servers), you need to set the IP address for that device, the network mask, the gateway IP address, and the DNS server IP address. The required IP addresses are listed next to each of the devices.

3. Configure routing between networks using OSPF.

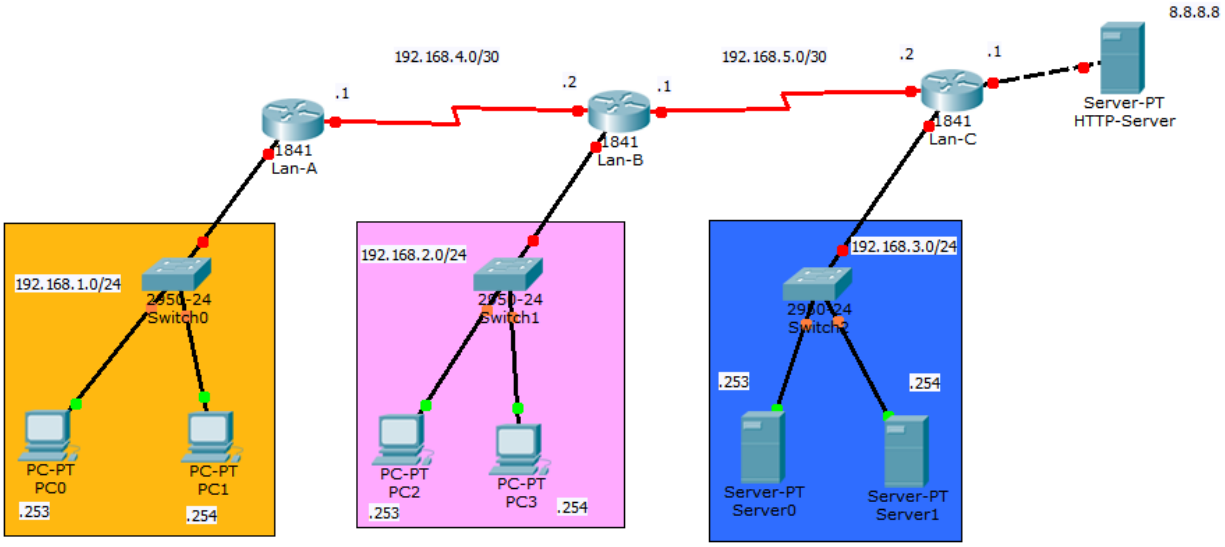

Fig. 5.2 - The structure of the computer network laboratory

Control questions

1. What is dynamic routing?

2. How is dynamic routing different from static routing?

3. How do channel state protocols differ from remote-vector protocols?

4. What are the advantages of dynamic routing over static?

5. Specify the features of the OSPF protocol.

6. Provide the algorithm of the OSPF protocol.

7. What are hello packages? Specify their purpose.

8. Compare the RIP and OSPF protocols, what are the disadvantages and advantages of each of them?

9. Specify the commands used to configure the OSPF dynamic routing protocol.

LABORATORY WORK № 7

Topic: Routing using the EIGRP protocol

Purpose: to get acquainted with the features of the EIGRP protocol, to gain skills in setting up dynamic routing using the EIGRP protocol.

Theoretical information

EIGRP (Enhanced Interior Gateway Routing Protocol) is a remote-vector dynamic routing protocol developed by Cisco. This protocol is sometimes called a hybrid protocol because it has the features of both remote-vector protocols and channel state protocols.

To implement network routing, the EIGRP protocol uses the following types of **messages:**

1. hello - used to find neighbors;

2. udate - contain information about changes in routes, can be sent to a specific router or group of routers;

3. query - request packets used in the case when the router lists the route to a particular network and does not find a backup route to this network;

4. reply - response to the received query package;

5. acknowledgment - acknowledgment package for update, query or reply packages.

For EIGRP, it is important to confirm the delivery of the packet, so the Real-time Transport Protocol (RTP) is used to transmit packets.

The calculation of new routes is performed using the DUAL algorithm (Diffusing Update Algorithm). The main step in this algorithm is to calculate the metrics for each route. Metric is a coefficient that quantitatively characterizes the quality of the route. The following values are used to calculate the **route metric:**

1. bandwidth - data rate along the route (kbit / s);

2. delay - packet delay on all interfaces of routers which it passes;

3. reliability - the worst indicator of reliability on all route which will be defined by means of keep-alive connections is used;

4. loading - the worst rate of link loading all the way, calculated using the packet rate (several packets that pass through the link per second), and bandwidth interface;

5. MTU - the minimum MTU (maximum transmission unit - the maximum size of the useful data block of one packet) of all route is used.

By default, only the first two components are used. The use of other components is not recommended, as this may lead to frequent recalculation of routes.

The route metric is calculated according to the following algorithm:

1. By default, the values of the coefficients: K1 = K3 = 1, K2 = K4 = K5 = 0.

2. Calculate the value of bandwidth:

bandwidth = (10000000 / bandwidth (s)) * 256,

where bandwidth (i) is the lowest bandwidth of all interfaces on the route.

3. Calculate the value of the parameter delay:

delay = delay (s) * 256,

where delay (i) is the sum of all route interface delays in tens of microseconds.

4. When using the value of the parameter K5 = 0 (default value), use the formula (1):

Metric = (K1 * bandwidth) + [(K2 * bandwidth) / (256 - load)] + (K3 * delay) (1)

5. If the values of the coefficients K1, K2, K3 are equal to the default values, then formula (1) is simplified:

Metric = bandwidth + delay.

6. If K5 is not equal to 0, then formula (1) has the form:

Metric = metric * [K5 / (reliability + K4)].

The values of the coefficients K are transmitted by routers in hello packets.

EIGRP routing protocol settings

The following **commands** are used to configure the EIGRP protocol:

- router eigrp [network index] - switch to EIGRP configuration mode;

- network [IP address of the external network] [network mask] - add a network for processing by EIGRP protocol;

- no auto-summary - disable automatic route summarization (used for compatibility with older devices).

Consider the settings of the OSPF protocol in the network shown in Fig. 7.1.

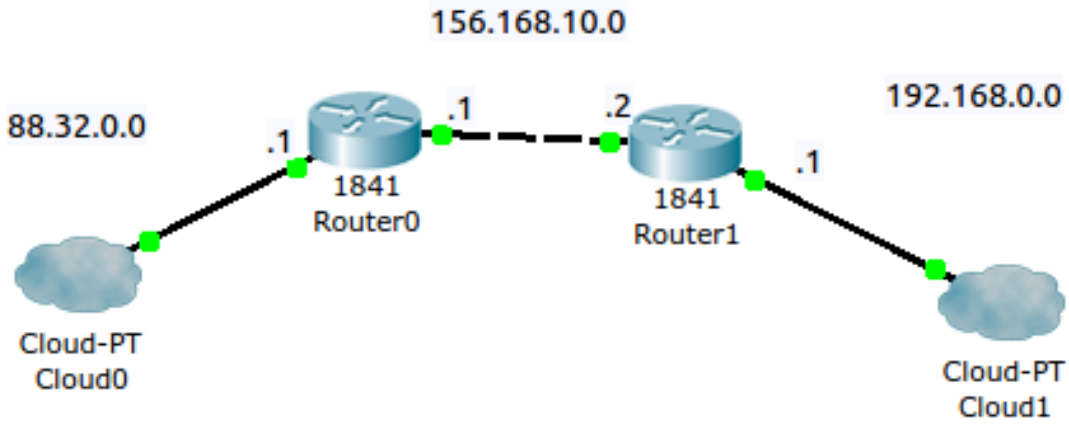

Fig. 7.1 - A simple topology with three subnets

Router0:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 88.32.0.1 255.255.255.0

Router (config) #interface fastEthernet 0/1

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.1 255.255.255.0

Router (config-if) #exit

Router (config) #router eigrp 20

Router (config-router) #network 88.32.0.0 255.255.255.0

Router (config-router) #network 156.168.10.0 255.255.255.0

Router (config-router) #no auto-summary

Router1:

Router> enable

Router # configure terminal

Router (config) #interface fastEthernet 0/0

Router (config-if) #no shutdown

Router (config-if) #ip address 156.168.10.2 255.255.255.0

Router (config-if) #exit

Router (config) #interface fastEthernet 0/1

Router (config-if) #ip address 192.168.0.1 255.255.255.0

Router (config-if) #no shutdown

Router (config-if) #exit

Router (config) #router eigrp 20

Router (config-router) #network 192.168.0.0 255.255.255.0

Router (config-router) #network 156.168.10.0 255.255.255.0

Router (config-router) #no auto-summary

Laboratory task

The network topology is shown in Fig. 7.2.

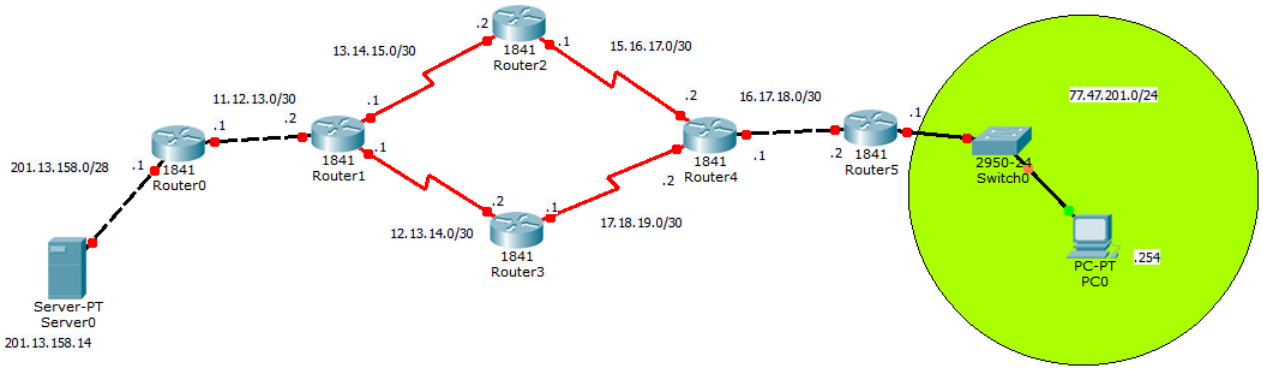

Fig. 7.2 - The structure of the computer network.

You must configure routes on each of the routers in the EIGRP domain for each of the interfaces.

Progress:

1. For each of the end devices (laptops, computers, and servers), you need to set the IP address for that device, the network mask, the gateway IP address, and the DNS server IP address. The required IP addresses are listed next to each of the devices.

2. For all routers in the topology you need to set the IP addresses and masks for each of the interfaces.

3. Configure routing between networks using the EIGRP protocol.

4. Check which of the routers the packets pass through - Router 2 or Router 3.

5. Turn off the router through which the packets pass and verify that the packets are transmitted using another router.

Control questions

1. What is dynamic routing?

2. How is dynamic routing different from static routing?

3. How do channel state protocols differ from remote-vector protocols?

4. What are the advantages of dynamic routing over static?

5. Specify the features of the EIGRP protocol.

6. How is the route metric calculated?

7. Provide the algorithm of the EIGRP protocol.

8. What are hello packages? Specify their purpose.

9. Compare the EIGRP and OSPF protocols, what are the disadvantages and advantages of each of them?

10. Specify the commands used to configure the EIGRP dynamic routing protocol.

LABORATORY WORK № 8

Topic: Virtual local area networks (VLANs)

Purpose: to get acquainted with VLAN technology, to gain skills in setting it up in the Cisco Packet Tracer environment.

Theoretical information

A Virtual Local Area Network (VLAN) is a group of hosts with a common set of requirements that interact as if they were connected to a network domain, regardless of their physical location. A VLAN has the same properties as a physical LAN, but allows endpoints to group together even if they are not on the same physical network. With virtual LANs, you can easily split a network so that network nodes do not use a single DHCP server and receive local addresses, or receive an address from another DHCP server.

Virtual VLANs can be built on switch ports. Port-based VLANs have some limitations. They are very easy to install, but allow you to support only one VLAN for each port. This applies to networks that use hubs or networks with powerful servers that are accessed by many users (the server cannot be included in different VLANs). In addition, making changes to port-based VLANs is difficult because each change requires a physical switching of devices. In the case where several VLANs can correspond to one port of the switch (for example, if the VLAN connection passes through several switches, this port must be a member of the trunk).

Grouping MAC addresses into a virtual network on each switch eliminates the need to connect switches to multiple ports, because in this case the MAC address is included in the virtual network. However, this method requires a large number of manual operations to mark the MAC addresses on each network switch. In the case where virtual VLANs are created based on network addresses, such as an IP address,

the switches must support not only channel layer protocols but also network layer protocols, ie they are combined routers.

Virtual network technology creates a flexible basis for building a large network connected by routers, because switches allow you to create completely isolated segments programmatically without resorting to physical switching. When connecting virtual networks via a router, a separate cable and a separate router port are allocated for each virtual network in this case.

Commands for setting up virtual local area networks

- switchport mode access - set the type of access link (do not transmit information about virtual networks);

- switchport mode trunk - set the link type trunk (transmit information about virtual networks);

- switchport access vlan [virtual network number] - give the virtual network with the specified number access through the interface;

- switchport trunk allowed vlan all - allow packets of all virtual networks to pass through interests;

- encapsulation dot1Q [virtual network number] - pass packets of the virtual network with the specified number through the interface (for the router).

Laboratory task

The task of the laboratory work is to divide the end devices into three virtual subnets using VLAN technology. The router, which also routes packets between all subnets, has to provide settings to end devices. The scheme of a computer network is shown in fig. 8.1.

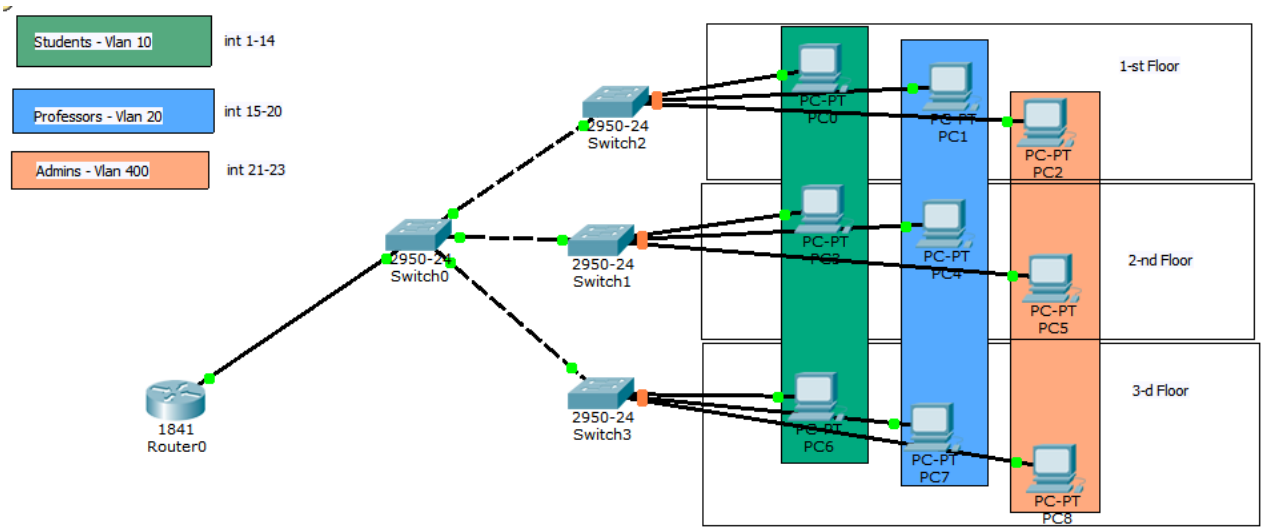

Fig. 8.1 - Scheme of the computer network of the laboratory №7

Progress:

1. Create virtual networks (vlan) with numbers 10, 20 and 400 on each of the switch.

2. For each of the interfaces of the switches set the desired type of data transmission (access or trunk). The names of the vlan and the ports through which they transmit data are indicated on the computer network diagram.

3. Create three sub-interfaces on the router, each must be responsible for its virtual subnet and belong to the corresponding vlan. Set up IP addresses on each of them.

4. Create three address pools. Exclude from the pool the addresses occupied by the sub-interfaces of the router.

Control questions

1. What is a virtual computer network?
2. Indicate the benefits of using local virtual computer networks.
3. What type of devices do most of the work when using VLAN technology?
4. Provide the commands needed to create a virtual computer network.
5. Indicate which parameters can be used to group end devices into logical computer networks?
6. Why are access and trunk links used? What is the difference between them?

LABORATORY WORK № 9

Topic: STP connected tree protocol

Purpose: to get acquainted with the features of connected tree protocols, to gain skills in setting up the STP protocol in the Cisco Packet Tracer environment.

Theoretical information

The main task of connected tree protocols is to prevent the formation of "loops" in networks. Sometimes it happens that the candles are accidentally connected in a ring. This situation is dangerous because some packets, which for some reason could not be routed, are constantly moving in this circle, increasing the load on the network. Packets with Broadcast addresses (those sent by candlelight to all ports) behave similarly. To solve such situations, connected tree protocols are used, which turn off the power on any of the links (link), in order to open the ring.

STP (Spanning Tree Protocol) is not the only protocol that solves this problem. In addition to STP, common connected tree protocols are RSTP (Rapid Spanning Tree Protocol), MSTP (Multiple Spanning Tree Protocol), PVSTP (Per-VLAN Spanning Tree Protocol) and SPB (Shortest Path Bridging).

The operation of the STP protocol is described by the following algorithm:

1. After turning on the candles, each of them considers itself root (so-called root).

2. Each switch has its own identifier (Bridge ID), which is calculated using several parameters (virtual network number, MAC address of the candle, etc.). These identifiers are sent to all ports in hello packets (sent every 2 seconds).

3. If the switch receives a hello packet with an ID less than its own, it stops sending packets with its own ID and forwards the received one.

4. There is only one candle left, which continues to generate and send its own ID - now it becomes a root bridge.

5. For each subnet to which two or more bridges are connected, the designated port is determined - the port through which packets from the root bridge enter this subnet.

6. All ports in the network segment to which two or more bridge ports are connected are blocked, except for the root port and designated port.

Commands for setting up virtual local area networks

- spanning-tree vlan [virtual network number] root primary - make the switch root in the virtual network with the specified number;

- spanning-tree vlan [virtual network number] port-priority [0-240] - set the priority for the switch link in the virtual network with the specified number.

Laboratory task

The scheme of a computer network is shown in fig. 9.1. You need to make sure that each switch is rooted for its virtual network. For switches that are connected by two links, you need to make the inactive link active and vice versa.

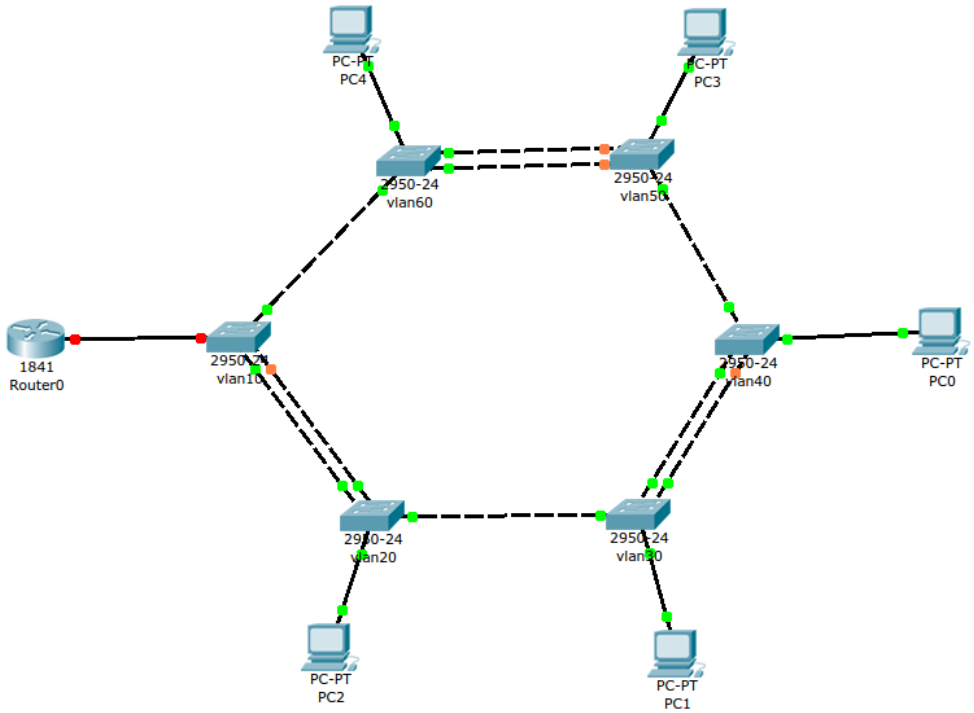

Fig. 9.1 - Scheme of the computer network of the laboratory №9

Progress:

1. Configure virtual networks with the specified numbers.
2. Make each of the switches root in its virtual network.
3. Change link priorities (for switches that are connected by two links)
4. Check the correct operation of the network using the "Simulation" tab.

Control questions

1. What is a virtual computer network?
2. Indicate the benefits of using local virtual computer networks.
3. Why are connected tree protocols used?

4. Give examples of common protocols that work on the algorithm of a connected tree.

5. Describe the algorithm of the STP protocol.

6. Which switch is called the root? What are the features of the root switch?

7. What is the danger of the formation of "loops" in topologies?

8. List the commands used to configure the connected tree protocol.

LIST OF COMMANDS,
WHICH ARE USED IN LABORATORY WORKS

Command	Command assignment
Router>enable	access device configuration
Router#configure terminal	switch to device configuration mode
Router(config)#interface [interface name]	switch to interface configuration mode
Router(config-if)#shutdown	control of voltage supply to the interface (on, off)
Router(config-if)#no [command]	cancel command
Router(config-if)#ip address [IP address] [subnet mask]	set the IP address and subnet mask for the interface
Router(config-if)#exit	go back one configuration level
Router(config-if)#end	go to the initial configuration mode (Router #)
Router(config)#ip route [Network IP address] [Subnet mask] [Interface IP address]	add a static route
Router(config-if)#ip address dhcp	get interface settings using DHCP
Router(config)#ip dhcp pool [name of the pool]	create a DHCP pool of IP addresses
Router(dhcp-config)#network [Network IP address] [subnet mask]	add all network IP addresses to the DHCP pool

Command	Command assignment
Router(dhcp-config)#default-router [IP address]	set the default gateway IP address for DHCP distribution
Router(dhcp-config)#dns-server [IP address]	set the default DNS server IP address for DHCP distribution
Router(config)#ip dhcp excluded-address [IP address]	exclusion of the IP address from the pool
Router(config)#ip nat inside source static [IP address] [IP address]	activation of NAT in static mode (replace one IP address with another)
Router(config-if)#ip nat inside	specify the interface directed "in the middle" of the network whose IP addresses need to be changed
Router(config-if)#ip nat outside	specify the interface that is directed "outwards"
Router(config)#ip nat inside source list [list number] interface [interface name] overload	activation of NAT in overload mode
Router(config-if)#clock rate [size]	setting the data rate of the serial link
Router(config)#router rip	switch to RIP configuration mode
Router(config-router)#network [Network IP address]	add a network that is not directly connected to the router for RIP processing
Router(config)#router ospf [network number]	switch to OSPF configuration mode

Command	Command assignment
Router(config-router)#network [Network IP address] [subnet mask] area [OSPF zone number]	add a network for OSPF processing
Router(config)#router eigrp [network number]	switch to EIGRP configuration mode
Router(config-router)#network [Network IP address] [subnet mask]	add a network for EIGRP processing
Router(config-router)#no auto-summary	Disable automatic route summarization (used for compatibility with older devices)
Switch(config)#vlan [virtual network number]	create a virtual network
Switch(config-vlan)#name [virtual network name]	change the name of the virtual network
Switch(config)#interface range [range of interfaces]	switch to interface range configuration mode
Switch(config-if)#switchport mode access	set link type access
Switch(config-if-range)#switchport access vlan [virtual network number]	give the virtual network with the specified number access through the interface (in access mode)
Switch(config-if-range)#switchport access vlan all	give all virtual networks access through the interface (in access mode)
Switch(config-if)#switchport mode trunk	set link type trunk

Command	Command assignment
Switch(config-if)#switchport trunk allowed vlan [virtual network number]	give the virtual network with the specified number access through the interface (in trunk mode)
Switch(config-if-range)#switchport trunk allowed vlan all	give all virtual networks access through the interface (in trunk mode)
Router(config)#interface [interface name]. [sub-interface number]	create a sub interface
Router(config-subif)#encapsulation dot1Q [virtual network number]	to pass packets of a vital network with the set number through the interface (for a router)
Switch(config-if)#spanning-tree vlan [virtual network number] root primary	make the switch root in the virtual network with the specified number
Switch(config-if)#spanning-tree vlan [virtual network number] port-priority [0-240]	set the priority for the switch link in the virtual network with the specified number

RECOMMENDED LIST

ELECTRONIC SOURCES OF INFORMATION

Address of the source of information	Description of the source of information
http://dflt.ru/articles/networks/tablica-masok-podseti	Table of subnet masks
http://ip-calculator.ru/	IP address calculator
http://xgu.ru/	System Administrator Knowledge Base - Contains a large amount of both theoretical material and practical guides for setting up telecommunications devices
http://www.cisco.com/cisco/web/support/index.html	Official documentation from Cisco

LITERATURE

1. Odom U. Cisco Official CCENT / CCNA Certification Exam Guide ICND1 640-822. ISBN 978-5-8459-1807-9, 978-1-58-720-425-8; 2012
2. Alan Leinwand, Bruce Pinsk. Cisco Router Configuration - Cisco Router Configuration. - 2nd type. - M .: "Williams", 2001. - ISBN 1-57870-241-0.
3. Cisco Systems Cisco Interdomain Multicast Solutions Guide. - M .: «Williams», 2004. - ISBN 5-8459-0605-9.
4. Jakab František, Janitor Jozef, Visual Learning: Case Study of Cisco Networking Academy's PACKET TRACER 5.0 Application, Proc. Of 6th International Conference on Emerging eLearning Technologies and Applications, ICETA 2008, Stara Lesna, 11.-13.10.2008, Kosice, elfa, s.r.o., 2008, ICETA, pp. 407-410, ISBN 978-80-8086-089-9
5. Janitor, J.; Jakab, F.; Kniewald, K., "Visual Learning Tools for Teaching/Learning Computer Networks: Cisco Networking Academy and Packet Tracer," Networking and Services (ICNS), 2010 Sixth International Conference on , vol., no., pp.351,355, 7-13 March 2010
6. Gupta, S. G., Ghonge, M. M., Thakare, P. D., & Jawandhiya, P. M. (2013). Open-source network simulation tools: An overview. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(4), pp-1629.
7. Makasiranondh, W., Maj, S. P., Veal, D., 2010. Pedagogical evaluation of simulation tools usage in network technology education. Engineering and Technology 8, 321-326.
8. Ma, J.,& Nickerson, J. (2006). Hands-on, simulated, and remote laboratories: A comparative literature review. ACM Computing Surveys, 38(3), 7. doi: 10.1145/1132960.1132961

9. Shea,J., Converting SSFNet Simulation Definition to Genesis Format, Computer Science Master's Project, Rensselaer Polytechnic Institute Troy, NY 12180.
10. Hao, J., Wu, J., & Guo, C. (2011, May). Modeling and simulation of CAN network based on OPNET. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (pp. 577-581). IEEE.
11. https://www.cisco.com/c/tr_tr/training-events/networking-academy.html