MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION
FEDERAL STATE AUTONOMOUS EDUCATIONAL
INSTITUTION OF HIGHER EDUCATION
NORTH CAUCASIAN FEDERAL UNIVERSITY

GUIDELINES

for the completion of practical work
By discipline "Principles of Communications / Принципы коммуникации"
for students in the field of study
02.04.01 Mathematics and Computer Science

Stavropol, 2026

Introduction

1. The purpose and objectives of mastering the discipline (module)

The purpose of studying the discipline " Principles of Communications / Принципы коммуникации " program develops a set of general cultural and professional competencies for future bachelor's students in the 02.04.01 "Mathematics and Computer Science" program. The competencies developed within this program facilitate the in-depth preparation of bachelor's students for solving professional problems using computer technology and computer systems . as well as the acquisition of a set of general cultural and general professional competencies of the future bachelor's degree in the field of study 02.04.01 "Mathematics and Computer Science".

The objectives of the discipline are:

- study the fundamentals of processing and transmitting information through various channels. Develop knowledge, skills, and abilities in the field of computer architecture and the construction of computer systems;

- improving the skills and abilities of working with a personal computer as a means of information management for solving problems of educational and professional activities.

2. A list of planned learning outcomes for the discipline (module), correlated with the planned learning outcomes for the educational program

Code, formulation of competence	Code, indicator formulation	Planned learning outcomes for the discipline (module), characterizing the stages of formation of competencies, indicators
UK-5 Able to analyze and take into account cultural diversity in the process of intercultural interaction.	ID-1 $_{UK-5}$ A analyzes and draws conclusions on social, ethical, scientific and technical issues arising in professional activities. ID-2 $_{UK-5}$ Objectively evaluates the diversity of cultures and identifies their individual characteristics	Applies, analyzes and draws conclusions on social, ethical, scientific and technical issues arising in professional activities
PC-8. Capable of participating in the management of projects for the creation of information systems and software systems at various stages of the life cycle	ID-1 $_{PC-8}$ Manages the development, development and maintenance of information systems and software systems ID-2 $_{PC-8}$ Knows and applies software development trends in his/her professional activities	applies information and communication technologies to solve problems of professional activity

Practical class No. 1.

General information about network technologies.

Educational questions:

1. Creation And testing direct connecting cable Ethernet.
2. Creation And testing crossed cable Ethernet.
3. Testing And definition character malfunctions cables

Ethernet.

Goals

Create and test straight and crossed unshieldedcable "unshielded twisted pair" For networks Ethernet.

General provisions

In this lab you will be required to make straight connectors .straight cables and crossover cables for Ethernet. In a straight-through cable, the color of thethe water of contact 1 on one end matches the color of the wire of contact 1 on friend at the end cable. For the rest seven contacts situation similar.

The cable will be based on the TIA/EIA T568A or T568B standard. for Ethernet, which specifies the colors of the wires for each pin .we connecting cables usually are used For direct connectionsnode to a hub or computer, or to a wall mount in office.

In a crossover cable, the second and third pairs on the RJ-45 connector at one end of the cable are crossed relative to the other end. Conclusions This cable complies with the T568A standard on one end and the T568A standard on the other. T568B on the other. Crossed cables are commonly used for connection To concentrators And switches or direct connections two nodesFor creation simple networks.

Will be required next resources: two piece cable length 0.6 - 0.9 m(2 – 3 feet) Category 5 or 5e; at least four RJ-45 connectors (may bemore may be required if the wires are connected incorrectly); crimping pliers RJ-45; tester cables Ethernet; nippers.

Table 1. Standard T568A

Стандарт T568A			
№ контакта	**№ пары**	**Цвет провода**	**Функция**
1	2	Белый/зеленый	Передача
2	2	Зеленый	Передача
3	3	Белый/оранжевый	Прием
4	1	Синий	Не используется
5	1	Белый/синий	Не используется
6	3	Оранжевый	Прием
7	4	Белый/коричневый	Не используется
8	4	Коричневый	Не используется

Table 2. Standard T568V

Стандарт T568B			
№ контакта	**№ пары**	**Цвет провода**	**Функция**
1	2	Белый/оранжевый	Передача
2	2	Оранжевый	Передача
3	3	Белый/зеленый	Прием
4	1	Синий	Не используется
5	1	Белый/синий	Не используется
6	3	Зеленый	Прием
7	4	Белый/коричневый	Не используется
8	4	Коричневый	Не используется

1. Creation And testing direct connecting cableEthernet

Step 1: receiving And Preparation cable

a. Determine the required cable length. This may be the distance from a device, such as a computer, to the device it connects to (such as a hub or switch), or between a device and a plug- with an RJ-45 connector. Add to this distance at least 30.48 cm (1 foot). According to standard TIA/EIA maximum length cable equal 5 m (16.4 feet). Standard lengths cables Ethernet: 6 m (20 feet), 1.83 m (6 feet)

or 3.05 m (10 feet).

b. Cut a piece of cable to the required length. For connecting cables ley (cables between end network devices such as PCs and (with an RJ-45 connector) a twisted "unshielded" cable is usually used. twisted pair", since such cables last longer even after repeated bending.baths. They are called twisted because each of the wires in the cable made from several strands of pure copper rather than one single strandwater. Single-core wire is used for cable routes between the connectorRJ-45 And assembly block.

V. WITH help tool For removals isolation clean from shellsboth end cable on 5.08 cm.

Step 2: Preparation And insert wires

A. Determine, Which standard will be used.[T568A |

[T568B]

b. Determine the correct table based on the standard used .darth connections wires.

V. Expand couples cables And put it in order their approximately V requiredin order on basis selected standard.

G. Unbraid short plot steam And put it in order their V in order, exactlycorresponding standard.

It is very important to unravel as small a section as possible. Twisting a-nie Very important, So How it provides suppression interference.

d. Straighten and smooth the wires between your thumb and pointer .bodily with fingers.

e. Make sure, What order wires cable All more corresponds hundred n-dartu.

f. Cut off direct plot cable on distance of 1.25 - 1.9 cm (1/2 - 3/4") from the edge of the cable sheath. If you leave a longer section, to a- the cable will be susceptible to crosstalk (interference created bygray wires).

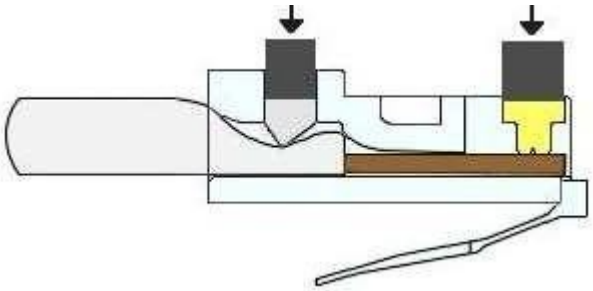
z. When inserting wires, the protrusion (the pin sticking out of the RJ-45 connector) must be With reverse sides And be directed down. Insertwires into the RJ-45 connector until they stop, all wires should fit into the connector maximum length.

Step 3: inspection, bending And repeated cable inspection

a. Inspect the cable and check that the color code is correct when connecting .turning on wires to the correct ones numbers contacts.

b. Inspect the end of the connector. The eight wires should be tightly compressed on at the end connector RJ-45. Some Part shells cable should z a-go into the connector. This weakens the cable tension. If the sheath goes intoconnector not enough deep, That in the end in the end This Maybe bring To By-damage to the cable.

c. If everything is properly aligned and inserted, insert the RJ-45 connector andcable into the crimping pliers. The crimping pliers will crimp the RJ-45 connector with two pistons.



Drawing 1. RJ-45 connector And cable V crimping ticks

d. Re-inspect the connector. If it is not installed correctly ,cut end and repeat process.

Step 4: processing another end cable

a. Follow the steps described earlier to install the RJ-45 connector.45 on friend at the end cable.

b. Re-inspect the connector. If it is not installed correctly ,cut end and repeat process.

Step 5: testing cable

a. Use a cable tester to check the functionality of the direct- my cable. If the cable fails the test, repeat this lab .hard work.

2. Creation And testing crossed cable Ethernet

Step 1: receiving And Preparation cable

a. Determine the required cable length. This may be a distance between hubs, from hub to switch, between switchestors, from a computer to a router or between computers. D o- add to this distance Not less 30.48 cm (1 foot).

b. Cut off piece cable required lengths And With help toolFor removals isolation clean from shells both ends cable on 5.08 cm.

Step 2: Preparation And insert reasons V in accordance with standardT568A

A. Please contact us To table T568A.

b. Expand couples cables And put it in order their approximately V requiredin order on basis standard T568A.

c. Unbraid a short section of pairs and arrange them in order, exactly corresponding to the standard. It is very important to unravel as little as possible. section. Twisting is very important because it provides suppression of thefur.

g. Straighten and smooth the wires between your thumb and pointer .bodily with fingers.

d. Make sure, What order wires cable corresponds standard.

e. Cut the straight section of cable at a distance of 1.25 - 1.9 cm from the edge cable shells. If leave more long plot, cable will in s-receptive To cross interference (interference, created neighboring conduct-ladies).

f. When inserting wires, the protrusion (the pin sticking out of the RJ-45 connector) must be With reverse sides And be directed down. Insertwires into the RJ-45 connector until they stop, all wires should fit into the connector maximum length.

Step 3: inspection, bending And repeated cable inspection

a. Inspect the cable and check that the color code is correct when connecting .turning on wires to the correct ones numbers contacts.

b. Inspect the end of the connector. The eight wires should be tightly compressed at the end of the RJ-45 connector. Some of the cable sheath should bego into the connector. This relieves the tension in the cable, which ultimately in the end may lead to damage cable.

c. If everything is properly aligned and inserted, insert the RJ-45 connector andcable into the crimping pliers. The crimping pliers will crimp the RJ-45 connector with two pistons.

Step 4: processing another end cable V in accordance with standard r-volume T568B

a. Follow the steps described earlier (but using the table and st-dart T568B), to install connector RJ-45 on the other end of the cable.

b. Re-inspect the connector. If it is not installed correctly ,cut end and repeat process.

Step 5: testing cable

a. Use a cable tester to check the functionality of the trans-crossed cable. If the cable fails the test, repeat this procedure.laboratory work.

3. Testing And definition character malfunctions cable e-lei Ethernet.

Determine the nature of the malfunction proposed for investigation cables. Describe the character malfunctions.

Questions:

1. Which standard [T568A | [T568B] better use Houses, If There is home net or required her create?

2. Which Part process creation such cables turned out to be most difficult? Compare your opinion With opinion fellow students.

3. Which length cable chosen And Why?

4. All whether four couples cables twisted the same? Discuss at-ranks in each case.

5. Many technicians include a crossed cable V mine tools. How You do you think, When follows use cross-cable and in what situations such a cable is used by network tech- nickname?

Practical class No. 2

Physical layer of the OSI model (Part 1).

Educational questions:

1. Studying opportunities Packet Tracer.
2. Job With files V simulator.

Theoretical Part

Packet Tracer software products enable you to create e- network topologies from a wide range of routers and switches Cisco, workstations and network connections such as Ethernet, Seri-al, ISDN, Frame Relay. This function can be performed both for training and both for work and for example, to set up the network at another stage. planning or to create a copy of the production network in order to eliminate nia malfunctions.

For launch Cisco Packet Tracer necessary call performing file, PacketTracer5.exe. General view programs presented on rice. 1.1.

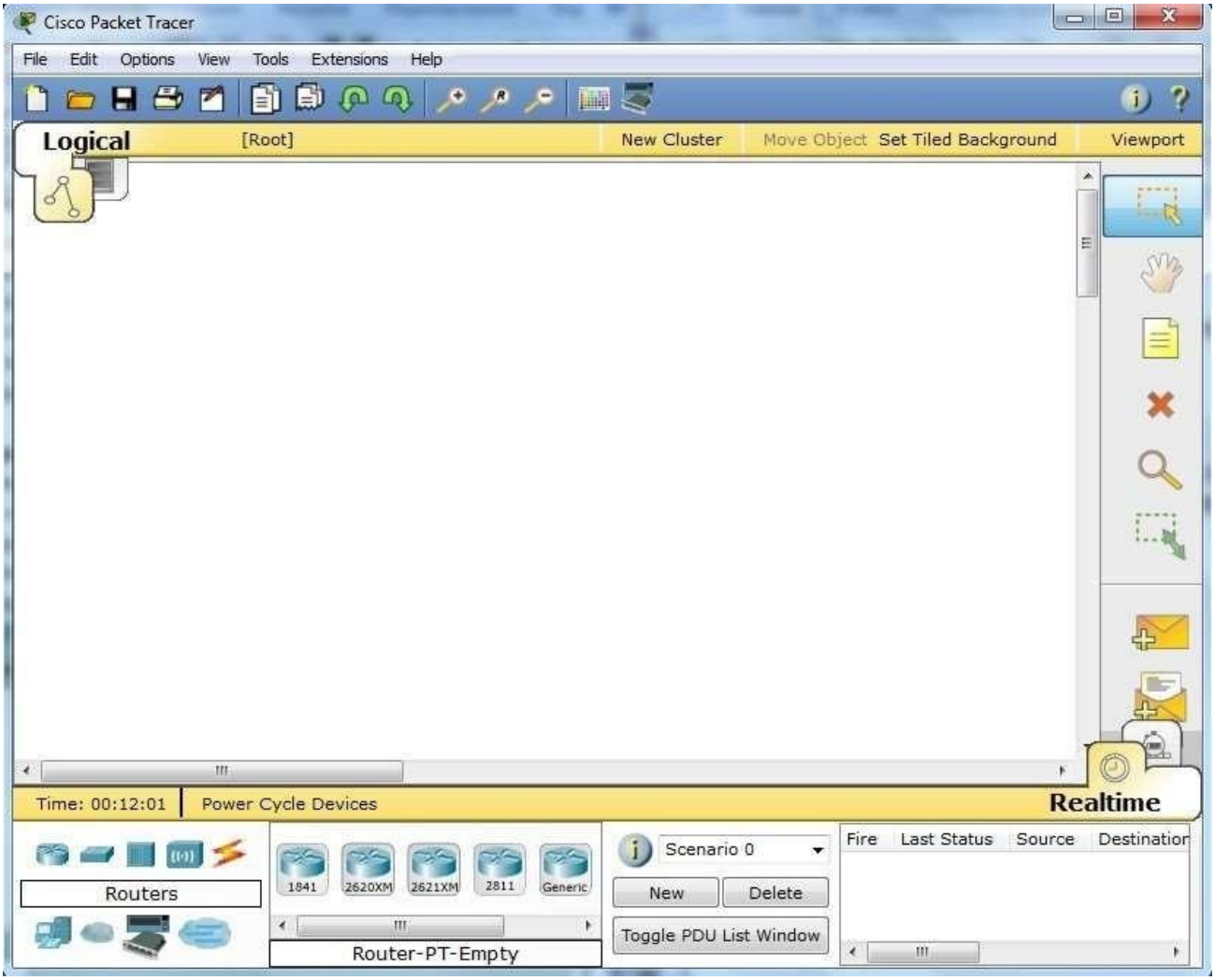


Figure 1.1. General view of the Packet Tracer program Working region windows programs consists of from following elements:

1 **Menu Bar** - panel, which contains menu File, Edit, Options, View, Tools, Extensions, Help.

2 **Main Tool Bar** - contains graphic images labels For to- step to the File, Edit, View, and Tools menu commands, and Also Network Infor- button mation.

3 **Common Tools Bar** – a panel that provides access To most used tools programs : Select, Move Layout, Place Note, De- summer, Inspect, Add Simple PDU and Add Complex PDU.

4 **Logical/Physical Workspace and Navigation Bar** - panel, which allows you to switch the work area: physical or logical- I will, A Also allows move between levels cluster.

5 **Workspace** is the area in which the network is created and conducted . observations of the simulation are made and various information is viewed and tistics.

6 **Realtime/Simulation Bar** – using the tabs on this bar you can switch between Real-time mode and Simulation mode. It also contains buttons related to Power Cycle Devices, Play Control buttons and switch Event List in mode Simulation.

7 **Network Component Box** - This region, V which are selected devices and communications for placing them in the workspace. She contains areas Device Type Selection And Device-Specific Selection.

8 **Device Type Selection Box** - region contains accessible types devices and links in Packet Tracer. The Device-Specific Selection area changes xia V dependencies from selected devices.

9 **Device-Specific Selection Box** - region is used For choice specific devices and connections required for construction in working order space networks.

10 **User Created Packet Window** – This window manages the packets that which were created V networks in time simulations scenario.

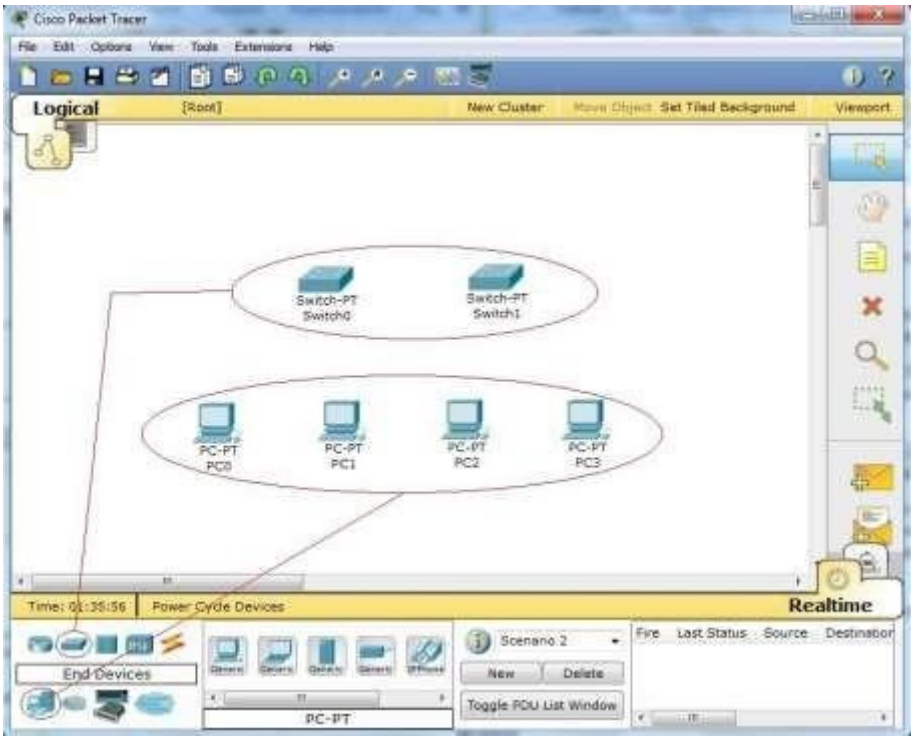
To create a topology, you need to select a device from the Net- panel. work Component, and then from the Device-Type Selection panel, select the device type- After this, you need to left-click in the work area field programs (Workspace). You can also move the device directly from the cloud . Device-Type Selection, but the device model will be selected by default.

For fast creation several copies one And Togo same devices, you need to hold down the Ctrl key and click on the device in the area Device-Specific Selection And let go button Ctrl. After this need to Not- How many once click mouse V working areas For additions copies devices.

IN Packet Tracer presented next types devices:

- routers;
- switches (V volume number and bridges);
- hubs And repeaters;
- final devices - PC, servers, printers, IP phones;
- wireless devices: points access And wireless route from a-torus;
- devices - cloud, DSL modem And cable modem.

Let's add necessary elements V working region programs So, Howshown on Fig.1.2.



Drawing 1.2. Addition elements networks

At addition each element user has opportunity Give it a name and set the necessary parameters. To do this, you need to Click on the desired element with the left mouse button (LMB) and in the dialog box devices go to to the tab **Config** .

Dialogue window properties each element has two tabs:

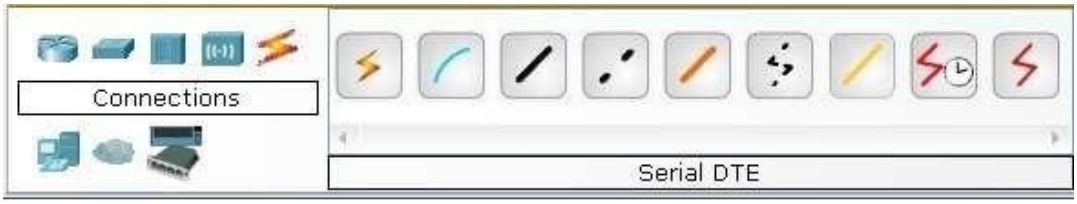
- Physical – contains the graphical interface of the device and allows you toto simulate work With him on physical level.
- Config - contains All necessary parameters For settings device-

state And has comfortable For this interface.

Also, depending on the device, the properties may have additional tab to control the operation of the selected element: Desktop (if you- brano finite device) or CLI (If router selected) And etc.

To remove unnecessary devices from the program workspace and uses button Delete (Del).

We will connect the added elements using connecting links. For To do this, you need to select the **Connections tab** from the Network Component panel. Box. We will see all possible types of connections between devices. Select Check the appropriate cable type. The mouse pointer will change to a "connection" cursor. (looks like a connector). Click on the first device and select the connection vetting interface, To to whom need to execute compound, then click the mouse on the second one device by performing the same operation. You can You can also connect network elements using **Automatically Choose Connection. Type** (automatically connects elements in the network). Select and click on each a house of devices that need to be connected. A network will appear between the devices. cable connection, and the indicators at each end will show the status of the connection . nenia (For interfaces, which have indicator).



Drawing 1.3. Supported V Packet Tracer types cables

Packet Tracer supports a wide range of network connections (see Table 1). Each type of cable can only be connected to certain types of pami interfaces.

Table 1. Types connections V Packet Tracer

Type cable	Descriptio n
Console 	Console compound Maybe be completed between PC And routers or switches. Must be performed There are some requirements for running a console session with a PC: speed connections from both there should be parties the same, there must be 7 data bits (or 8 bits) for both sides, con- The parity check must be the same, it must be 1 or 2 stop bat For both sides.
Copper Straight- through 	This type of cable is the standard Ethernet transmission medium. For connections devices, which is functioning on different OSI levels. It must be connected to the following types ports: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) And copper 1000 Mbps (Gigabit Ethernet).
Copper Cross- over 	This type of cable is the Ethernet transmission medium for connecting devices that operate at the same levels OSI. 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).
Fiber 	Fiber optic medium is used for connection between opti-Czech ports (100 Mbps or 1000 Mbit/s).
Phone 	Connection via telephone line can be madeonly between devices that have modem ports . dart performance modem connections - This ko- a remote device (such as a PC) that dials V network cloud.
Coaxial 	Coaxial medium is used for connection between coax and- ports, such as a cable modem connected to cloud Packet Tracer.
Serial DCE and DTE  	Connections via serial ports are often used for WAN connections. To set up such connections, you need establish synchronization on the DCE device side. Synchro- DTE configuration is optional. The DCE side can be determined divide by the small “clock” icon next to the port. When selecting Serial DCE connection type, the first device to which the connection changes, becoming a DCE device, and the second one - will automatically become the DTE party. The opposite is also possible . position parties, If chosen type connections Serial DTE.

After creating the network, you need to save it by selecting the menu item File -> Save or icon Save on panels **Main Tool Bar** . File saved topologyhas extension *.pkt.

Packet Tracer allows you to simulate the work with the interface to mand line (ICS) operating system iOS, installed on all switches and routers companies Cisco.

Once connected to the device, we can work with it as usual . salt of a real device. The simulator provides support for virtually everyone teams, available on real devices.

Connection to switches or routers can be done by clicking on the required device and going to the tab in the properties window CLI.

For simulations work command lines on terminal device (on a computer) necessary V properties choose tab Desktop, A then press on label Command Prompt.

Job With files V simulator

Packet Tracer gives opportunity to the user keep configurationsome devices, such How routers or switches, V text files. For this necessary go to To properties necessary devices AndIn the Config tab, click the “Export…” button to export the configuration. Startup Config or Running Config. This will bring up a dialog box. to save the required configuration to a file that will have a dis- extension *.txt. Text of the file with the device configuration running-config.txt (nameby default) appears to be similar to the text of the information received to him at use teams show running-config V iOS devices.

It should be noted that the configuration of each device is savedin a separate text file. The user also has the option of change the configuration in the saved file manually using arbitrary leg text editor. For provision device saved or

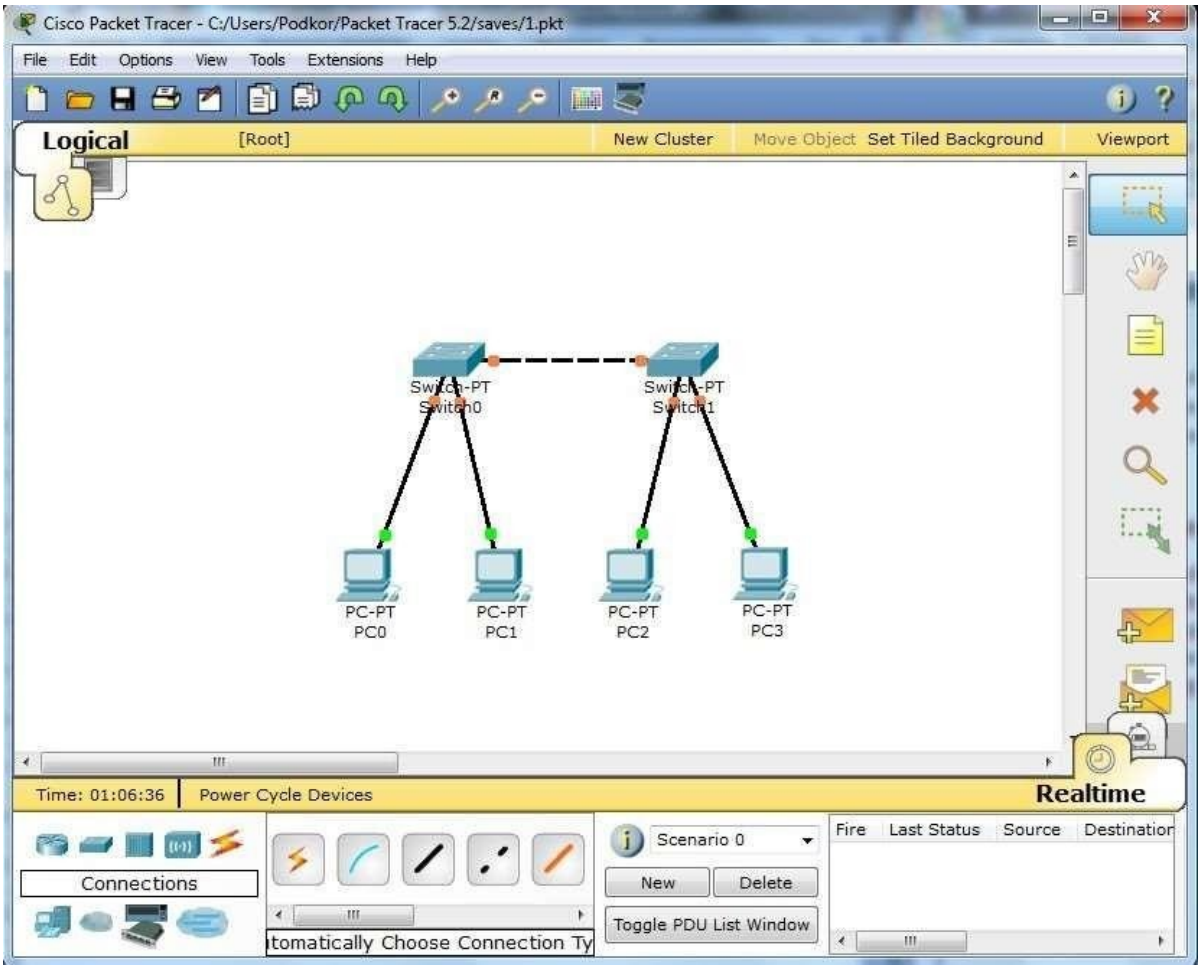
edited settings, need to in tab Config press button “Load...” to load the required Startup Config configuration or the button “Merge…” For downloads configurations Running Config.

Practical Part

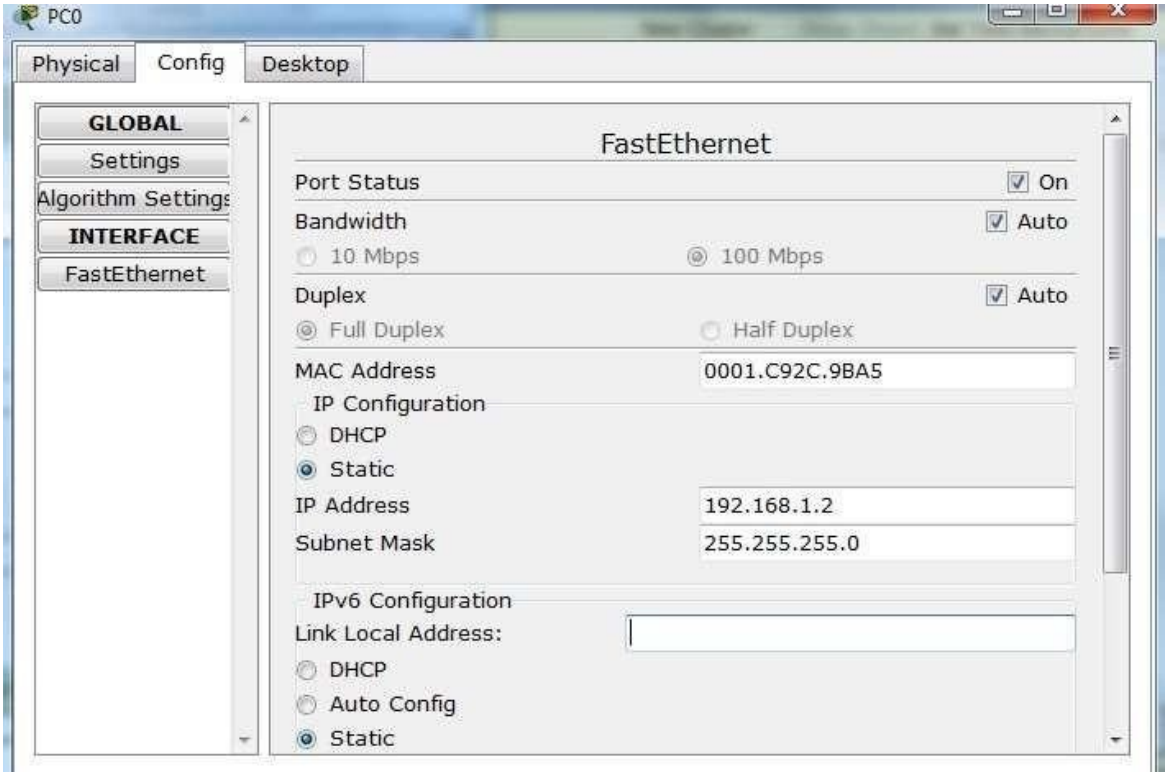
1. Let's add 2 Switch-PT switches to the program's workspace.default They have names - Switch0 And Switch1.
2. Let's add V working field four computer With names By defaultPC0, PC1, PC2, PC3.
3. Let's connect devices V net Ethernet, How shown on Fig.1.4.
4. Let's save it created topology, by clicking button Save (V menu File -> Save).
5. Let's open it properties devices PC0 by clicking mouse By his image- Let's go to the Desktop tab and simulate the work of run by pressing Command Prompt.
6. We will get a list of commands if we enter the command **?** and press Enter. For To configure the computer, we will use the ipconfig command from the command line.lines, For example, For computer PC0:

ipconfig 192.168.1.2 255.255.255.0

The IP address and network mask can also be entered in a convenient graphical and n- device interface (see Fig. 1.4 and Fig. 1.5). In the DEFAULT GATEWAY field the gateway address is entered, in this case this information is not important, since with o- rented out net Not requires routing.



Drawing 1.4. Created fragment networks



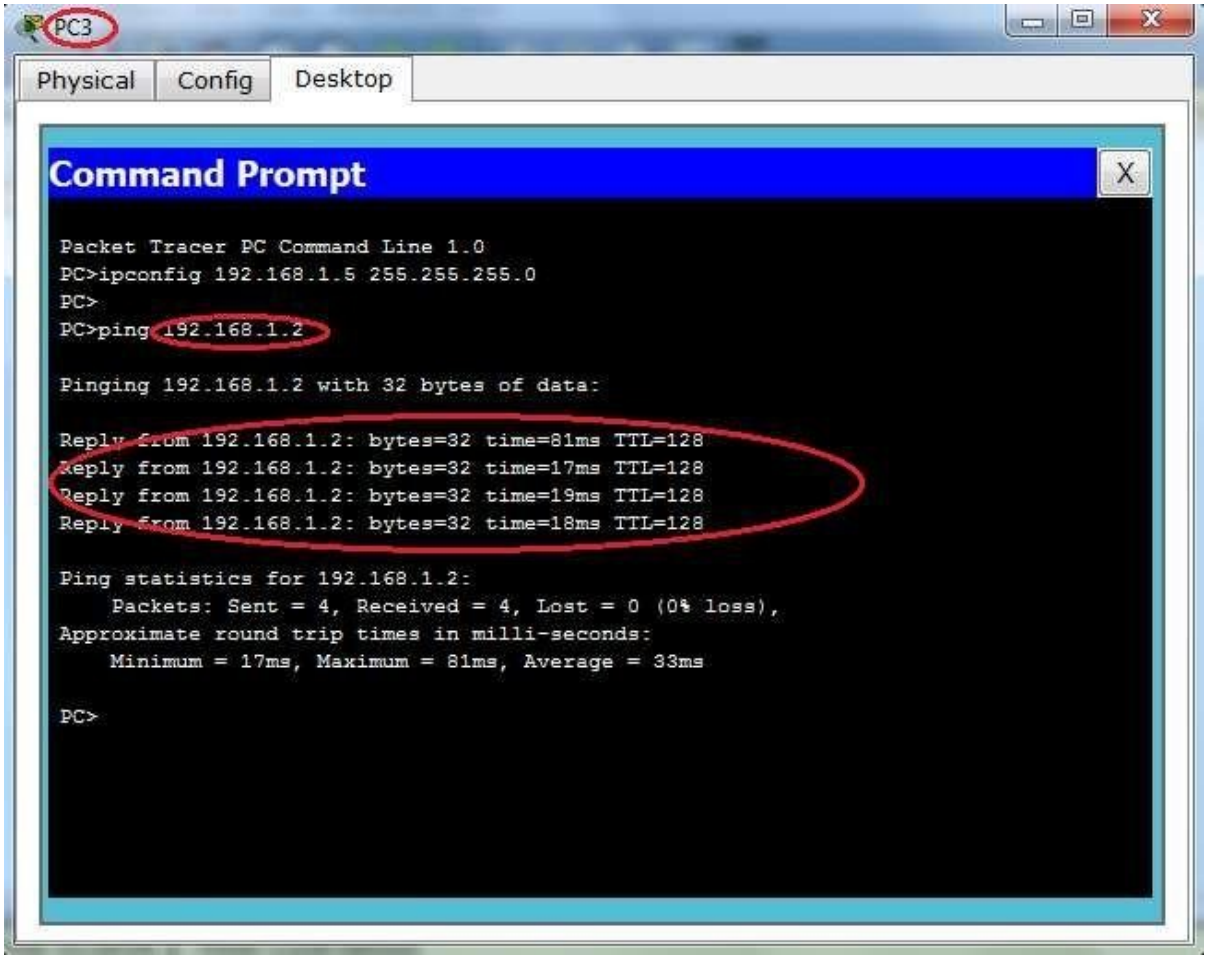
Drawing 1.5. Setting up RS0

Like this same by way let's set it up every computer rice. 1.4.

Table 2. IP addresses And masks computers

Device	IP ADRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

7. On each computer, we will look at the assigned addresses of the com-Run ipconfig without parameters. If everything is done correctly, we will be able to verify the connection of computers using the ping command. For example,Let's go to PC3 and ping it with PC0. We should we see report on ping, like rice. 1.6.



Drawing 1.6. Report O ping RS3

Exercise For independent work

1. Создайте топологию

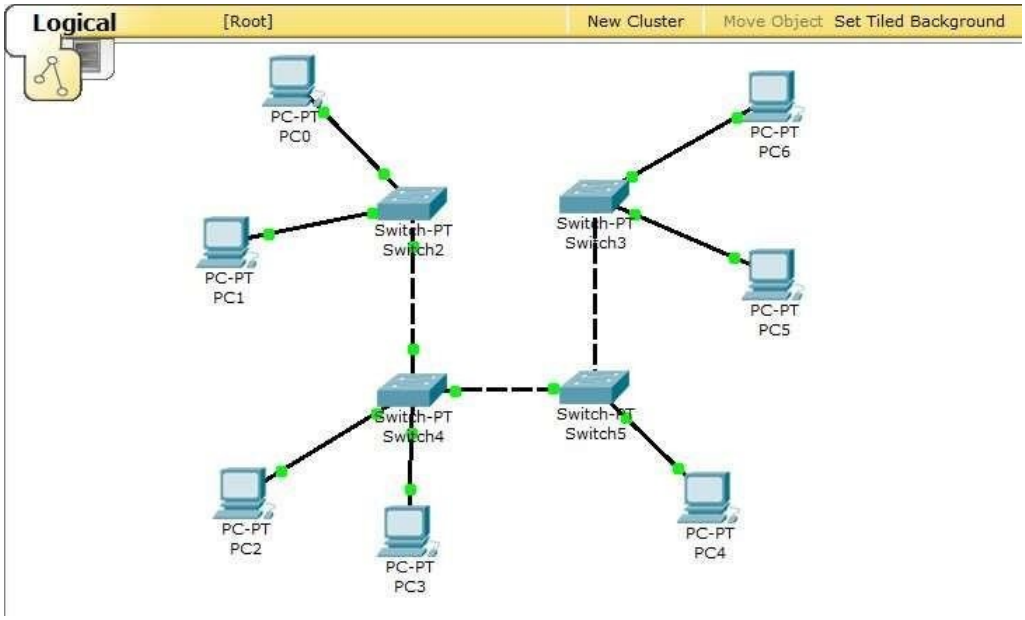


Fig. 1.7.

2. Assign computers addresses, according to to his own option

Table 3. IP addresses And masks computers

Device	IP ADDRESS	SUBNET MASK
PC1	192.168.1.1	255.255.255.0
PC2	192.168.1.2	255.255.255.0
PC3	192.168.1.3	255.255.255.0
PC4	192.168.1.4	255.255.255.0
PC5	192.168.1.5	255.255.255.0
PC6	192.168.1.6	255.255.255.0
PC0	192.168.1.7	255.255.255.0

3. Assign computers different names V command line.
4. If made All Right, You you can ping anycomputer from any another computer.

Table 4. Options tasks

Option No.	Ping from	Ping in	Option No.	Ping from	Ping in
1	PC1	PC6	7	PC0	PC5
2	PC2	PC0	8	PC1	PC6
3	PC3	PC1	9	PC2	PC7
4	PC4	PC2	10	PC3	PC1
5	PC5	PC3	11	PC4	PC2
6	PC6	PC4	12	PC5	PC3

It is assumed that the creation real fragment networks rice. 1.7 And demonstration-

ция команды пинг преподавателю согласно своему варианту.

Order execution And surrender laboratory work

1. To study theoretical And practical Part laboratory work.
2. Submit the theory of work to the teacher by answering the tests in o-requests.
3. Complete the practical part of the lab in Packet Tracer according to your option.
4. Show me to the teacher result execution tasks with o- according to his version. Demonstrate that any computer pings from any computer.
5. Make out And protect report.
6. Report must contain screenshots created topology, A Also execution teams ping, according to to your option.

Control questions:

1. Which maximum quantity devices V networks supports PacketTracer?
2. Which types network devices And connections Can use VPacket Tracer?
3. What way Can go to To interface command linesdevices.
4. How configure devices from another computer?
5. How add V topology And tune new device?
6. How save configuration devices V .txt file?

Practical Lesson 3. Physical layer of the OSI model (Part 2).

Target works: Receipt skills V setting network connections in MS Windows XP AndV work With console.

Exercise

1. Determine parameters network adapter PC
2. Define settings protocol IP his own PC.
3. Definition extended properties network connections his own PC And others PCsubnets.

Brief theoretical intelligence

IP address (abbreviation for Internet Protocol Address) is unique network address of a node in a computer network built using the IP protocol. When communicating via net Internet required global uniqueness addresses, V case work V local networksThe uniqueness of the address within the network is required. It is 4 bytes long. Usually the first and The second byte defines the network address, the third byte defines the subnet address, and the fourthaddress computer V subnets

IP address consists of from two parts: numbers networks And numbers node. In case isolatednetwork, its address can be selected by the administrator from those specially reserved for such networks of address blocks (192.168.0.0/16, 172.16.0.0/12 or 10.0.0.0/8). If the network should work How composite Part Internet, That address networks issued provider.

Number node in protocol IP is appointed regardless of local addresses node. A router, by definition, is part of several networks at once. Therefore, each port router has own IP address. Finite knot Also Maybe enter V some IP networks. IN this case computer must have some IP addresses, By numbernetwork connections.

Like this in this way, IP address characterizes Not separate computer or router, A one network compound.

IP address they call static (constant, unchangeable), If He is registered V settings devices user, or If is appointed automatically at connection devices To networks, But is used V flow unlimited interval time And Not Maybe be assigned to another device.

IP address they call dynamic (inconstant, changeable), If He assigned automatically when the device is connected to the network and is used for limited interval time, How rule, to completion session connections.

Dynamic IP addresses are also virtual, virtual service IP addresses are generated using NAT technology: users are given the opportunity unhindered receive information from networks Internet, at this is lost all sorts the possibility of other access to the computer from the network, for example, a computer with such an IP is notMaybe be used as web server.

Non-virtual IPs are called real, direct, external, public orpublic, "whites" all such IP are static.

MAC address (from English Media Access Control - access control to the environment, also Hardware Address) is a unique identifier assigned to each unit. computer network equipment. Most data link layer network protocols use one of three MAC address spaces managed by the IEEE: MAC-48, EUI-48 And EUI-64. Addresses V each from spaces theoretically should be globally unique. Not All protocols use MAC addresses, And Not All protocols, using MAC addresses, need V similar uniqueness these addresses.

IN broadcast networks (such, How networks on basis Ethernet) MAC address allows unique identify every knot networks And deliver data only

to this node. Thus, MAC addresses form the basis of networks at the data link layer, which is used by higher (network) level protocols. For conversion Special protocols are used to convert MAC addresses to network layer addresses and back. (For example, ARP And RARP V networks TCP/IP).

Addresses type MAC-48 most common; They are used V such technologies such as Ethernet, Token ring, FDDI, WiMAX, etc. They consist of 48 bits, so in this way, address space MAC-48 counts 248 (or 281 474 976 710 656)addresses.

ARP (eng. Address Resolution Protocol — protocol definitions addresses) — a low-level protocol used in computer networks, designed to determining the link layer address from a known network layer address. The greatest This protocol gained popularity due to the ubiquity of IP networks built over Ethernet, since in almost 100% of cases this combination usesARP.

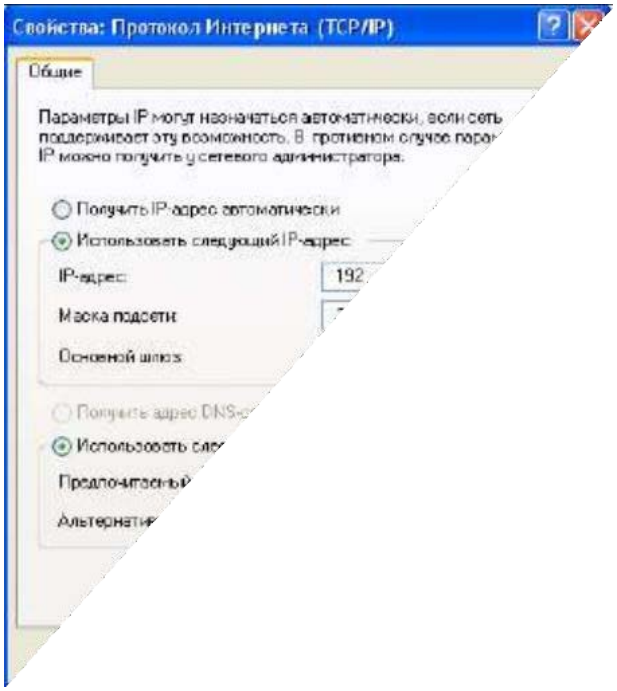
There are the following types of ARP messages: ARP request and response. ARP (ARP reply). The sending system requests the physical the address of the receiving system. The response (the physical address of the receiving node) comes in the form ARP response. Before transmitting a network layer packet across an Ethernet segment, the network the stack checks the ARP cache to see if the required one is already registered there information about the receiving node. If such a record V cache ARP No, That is being carried out ARP broadcast request. This request to devices on the network has the following meaning: "Does anyone know the physical address of the device that has the following IP- address?" When recipient With this IP address will accept this plastic bag, That must will reply: "Yes, this is my IP address. My physical address is: ..." After that The sender will update its ARP cache and will be able to transmit the information to the receiver. Entries in the ARP cache can be static or dynamic. The example given above describes dynamic recording cache. Can Also create static records V table ARP. This Can do at help commands:

arp -s <IP address> <MAC address>

ARP table entries created dynamically remain in the cache for 2 minutes. If during these two minutes there was a retransmission of data on this address, then the cache entry storage time is extended by another 2 minutes. This procedure Maybe repeat to those pores, Bye recording V cache will exist to 10 minutes. After this recording will removed from cache, And will sent repeated request ARP.

Instructions To execution work

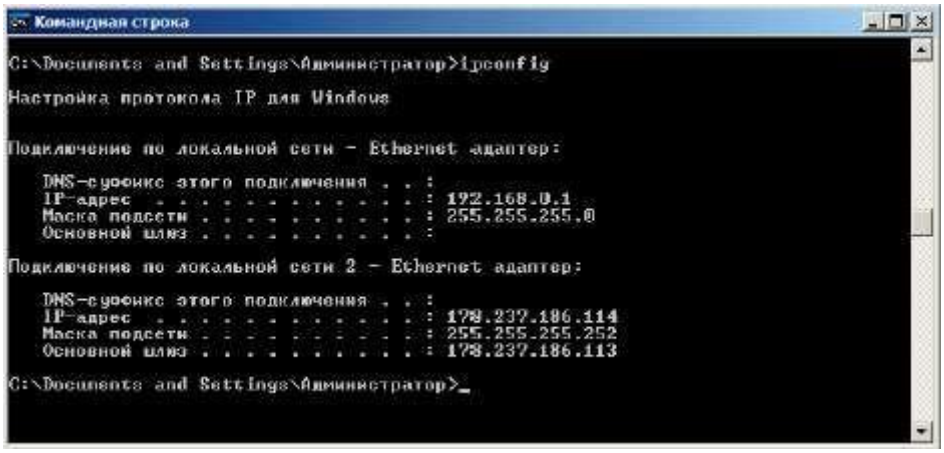
Task 1. Determine the parameters of the PC network adapter using the Start command. Settings-Panel management open window Panel management, then click on label Network connections. IN window Network connections select network connection and, by right-clicking, select the command from the context menu Properties.



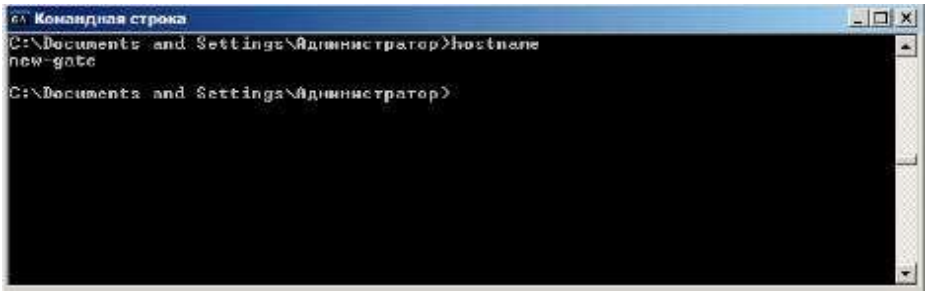
In the Local Area Connection Properties window, select the component from the list Protocol Internet TCP/IP And click on button "Properties". After this will open windowProperties: Protocol Internet (TCP/IP). Write it down IP address PC V report.

Exercise 2. Determine settings protocol IP yours computer.

For this launch program ipconfig. To get access To commandline, select the command Programs-Accessories-Command Prompt in the Start menu. window Command line enter the command ipconfig.



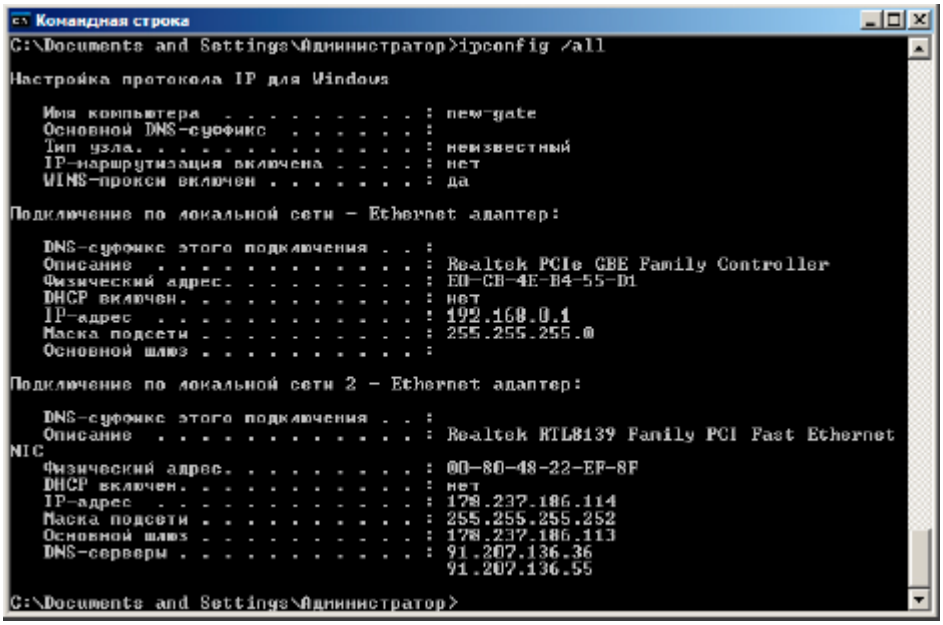
For Togo to define Name local computer, ask team Hostname.



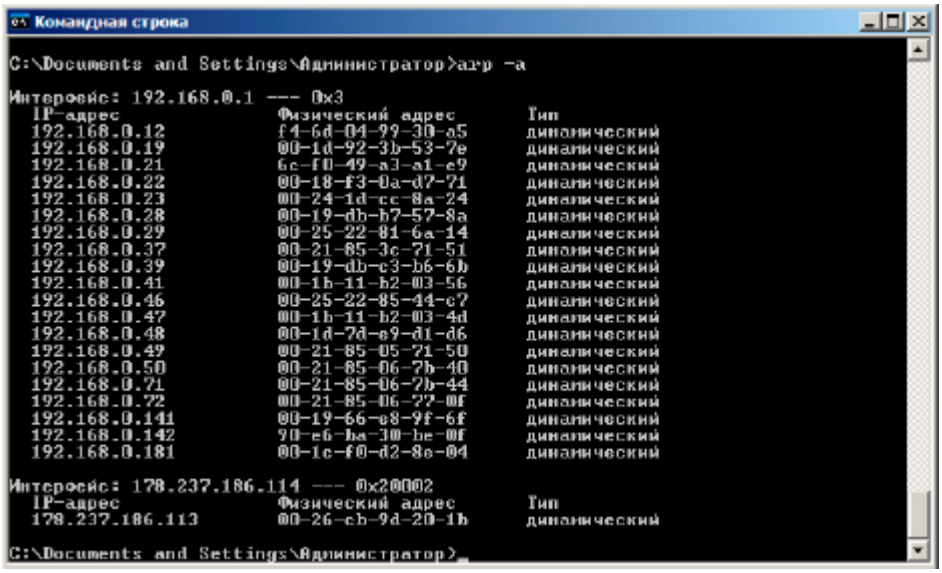
Enter into the report the addressing information of all network interfaces of the PC, as well as its symbolic Name.

Exercise 3. Receipt extended properties network connections PC.

IN window command lines dial team ipconfig /all. The result her execution is a table of extended properties of all PC network adapters, including their MAC- addresses. Data addresses are required reflect V reports.



For definitions MAC And IP addresses PC, located V one subnets With on the PC being examined, it is necessary to execute two console commands in sequence: ping [IP] And arp -a. The result execution should become table With data about IP And MAC addresses



Bring it in intelligence about addressing others PC subnets in reports.

Control questions

1. From what kind parts consists of an IP address computer (IPv4)?
2. What such MAC address PC ?
3. List main methods definitions IP And MAC addresses networkinterfaces.

4. Describe types messages protocol ARP.

Practical class No. 4. TCP/IP Stack Data Link Layer (Part 1).

Target And content:

Target
To study methods definitions hosts And subnet allocation

Content
1. Concept IP addressing.
2. Selection subnets.
3. Masks subnets.
4. Usage calculator Windows For solutions network tasks.

Theoretical justification:

What such IP addressing?

One of the most important topics when discussing TCP/IP is IP-addressing. *IP address* represents by yourself numerical identifier, assigned for every computer networks IP. He reflects location devices on the network. IP address is software, A Not hardware address

– last sewn up V computer or board network interface.

Hierarchical scheme IP addressing

IP address contains 32 bat information, which are separated on four one-byte (eight-bit) sections, otherwise called octets. There are three ways performances IP addresses:

- representation by decimal numbers separated by periods,For example, 130.57.30.56;
- binary performance, For example, 10000010.00111001.00011110.00111000;
- hexadecimal performance, For example, 82 39 1E 38.

Three forms of representation of the same IP address are shown here. A 32-bit IP address is hierarchical, not flat (non-hierarchical) structure. Can to use any scheme addressing, Buthierarchical – more attractive.

Good example non-hierarchical schemes addressing - numbering cards social insurance. IN these rooms No any division into sections, the contents of which would reflect the place of residence or others characteristics owner cards. Dignity flat the scheme is a large number of possible addresses, for example, space 32-bit addresses, V each positions which Maybe be 0 or 1, contains 2 or 4.2 billion addresses. The disadvantage of this scheme is that impossibility implementation routing, exactly By this reason A flat scheme is not used for IP addressing. If all addresses are different, routers Internet will have to remember addresses everyone cars, connected To the Internet, What Not will allow achieve effective routing, even at use only parts address space.

That's why For addressing chosen hierarchical scheme With three hierarchy levels: network, subnet, and host. For example, let's look at the structuretelephone number. Its first part (area code) describes the extensive geographic area. The second part (the prefix) narrows this area to a zone actions local telephone stations. Last segment (actually number phone) defines specific compound. At IP addressing Also is used scheme With three levels. Instead of Togo to consider a 32-bit combination as a single identifier in an address stand out parts for addresses networks and For addresses node.

Address networks definitely defines the network. IN IP addresses of all machines, connected or To one networks, indicated one And That same address networks. For example, V IP address 172.16.30.56 address networks can be 172.16.

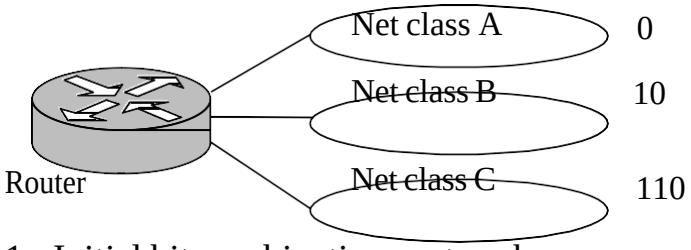
A node address is assigned to each machine on the network. Unlike an address network that describes a group of devices, the node address is unique and unambiguous identifies a specific machine on the network. The node address is also called the address host. IN given example address node has view 30.56.

The developers of the Internet decided to create classes of networks, and the network belongs to one class or another depending on its size. For For a small number of networks with a significant number of nodes, *class A was created. Class C* reserved for numerous networks with a small number of nodes. *Class B* networks include intermediate-sized networks. Method divisions IP addresses on fields addresses networks And node is determined the network's belonging to a particular class. Table 1.1 shows intelligence O three classes networks.

Table 1.1 - Characteristic classes networks

Class	Format	Started naya bit combina tiontion	Range decimal values first byte addresses networks	Maximal nye number networks	Maximume is the number of nodesV networks
A	Network.Node.Node. Node	0	1-127	127	16 777 214
B	Network.Network.No de.Node	10	128-191	16384	65 534
C	Network.Network.Net work.Node	110	192-223	2097152	254

For effective routing developers Internet define the mandatory initial part of the address for each of the classes. For example, knowing, What address networks class A Always it begins With 0, router Maybe speed up transmission package By needed route after recognition contents first bat addresses. On drawing 1.1 The correspondence between the network class and the contents of the initial bits is shown addresses.



Drawing 1.1 - Initial bit combinations networks

Some IP addresses are reserved for special uses, And administrator networks Not have the right attribute their nodes networks. Reserved addresses listed V table 1.2.

Table 1.2 - Reserved IP addresses

Addre ss	Purpose
Network address , consisting from zeros	Interpreted How current net" or "currentsegment"
Network address , consisting from units	Interpreted How "All networks."
Net 127	Reserved For ring tests. Indicateslocal knot And is used, When knot sends test plastic bag myself to myself without creation additional traffic
Node address , consisting from zeros	Interpreted How "current knot"
Node address , consisting from units	Interpreted How "All nodes" certain networks;For example, address 128.2.255.255 describes All nodes networks 128.2 (address class B).
Null IP address	Used by Cisco routers for designations route, selected By default.
IP address, consisting of units(or 255.255.255.255)	Broadcast address (address messages, directed to everyone nodes current networks)

Networks class A

In a Class A network IP address, the first byte is the network address, and in three subsequent bytes is located address node. Format IP addresses networks class A:

Network.Node.Node.Node.

For example, V IP address 49.22.102.70 address networks equal 49, A address node - 22.102.70. Each one this car networks should have address networks, equal 49.

Address networks class A has length 1 byte, and his first bit reserved (cm. table 1.1). This means, What Can create Not more
128 networks class A. So How every from seven remaining bits Maybe accept meaning 0 or 1, T. e. exists 2 or 128 various combinations. It was decided that the zero network address (0000 0000) is reservedFor designations route, selected By default (cm. table 1.2).Therefore, the actual number of Class A network addresses in use is128 - 1=127.

You can determine this number yourself. Start with the line withbinary zero And come down By lines down, turning attention on value of the first leftmost bit. The decimal number in the string where this the bit becomes 1 for the first time, equal to 127. In other words, class A network numbers are selected from the range from 0 to 127. Since address zero is reserved, the range becomes already: from 1 to 127. Table 1.2 indicates that the network with number 127 Also is special . Like this in this way, accurate number networksclass A equals 126.

3 bytes (24 bits) are allocated for the host address in the IP address of class A networks . they can accommodate 2^{24} or 16 777 216 different binary combinations or node addresses. Since addresses consisting only of zeros and only of units, reserved, exact number nodes in the network class And it makes up 16 777 214.

Networks class IN

In the IP address of class B networks, the first two bytes are occupied by the network address, and in The next two bytes contain the host address. The format of the IP network address class IN:

Network.Network.Node.Node

For example, V IP address 172.16.30.56 address networks equal 172.16, A addressnode - 30.56.

For addresses networks, consisting from 16 bit, there is 2^{16} possible combinations. Developers Internet decided, What address networks class IN

must start off With combinations 10. That's why free For formations addresses remain only 14 bit; This means, What Maybe exist 2 or 16 384 networks class IN.

Under address node V IP address networks class IN allotted 2 byte. Because addresses, consisting only from zeros And only from units, reserved, exact number networks class IN equals $2^{16} - 2 = 65\ 534$.

Networks class WITH

The first three bytes of an IP address for a Class C network are occupied by the network address, and nau byte remains For addresses node. Format Network IP addresses class C:

Network.Network.Network.Node

For example, in the IP address 192.168.100.102, the network address is 192.168.100, and address Node - 102.

The first ones three bat addresses networks class WITH occupies combination 110. Therefore, only 24 – 3 = 21 bits remain to form the address. thus, there may exist 2^{21} or 2 097 152 class networks WITH.

Additional classes networks

Another class of networks is class D. The address range of this class (from 224.0.0.0 to 239.255.255.255) is used For group mailings packages.

There is also a class E network with an address range from 240.0.0.0 to 255.255.255.255. These addresses reserved For use in future.

If You Not do you want complicate to myself life, Not assign nodesyour network addresses from classes D And E.

Subnets

If there are many computers in the organization or they are located far from each other friend, has meaning break big net on some more small ones And connect their through routers. TO merits such approachinclude:

- abbreviated network traffic. All will feel decrease traffic any type. At this networks remain of the same type. Without routers

traffic threatens almost fully slow down, work networks. A at their use big Part traffic remains V local networks; through router will be be transmitted only packages, intended consumers from others networks;

- Network performance optimization. This is a bonus for reduction network traffic;
- simplified control. IN group small networks, related Friend With friend, much easier identify And decide emerging problems, howV one big networks;
- simplified coverage large geographical spaces. Connections global networks are much slower and more expensive compared to with connections local networks. Unification numerous small networks does all system more effective.

If organization With numerous networks receives V Network the information center has only one network address, various problems arise problems. The first developers of the IP protocol took into account significantly a smaller Internet, consisting of dozens of networks and hundreds of hosts. their scheme addressing For each physical networks was envisaged separate address.

This approach led to several problems. Here's the first: the same address is assigned to several physical networks. However, organization Maybe demand separate address For each physicalnetworks. If all such requests were satisfied, the addressing problem was would solved.

Next problem refers to To application routers. If every router on the Internet had to know about every existing physical networks, tables routing incredible grew would. For support such tables were required would additional expenses on administration And increase physical

costs on routers (time cycle processor, memory, disk space And T. d.).

Undesirable consequence showed up would huge height network traffic, because routers exchange Friend With friend information O routing.

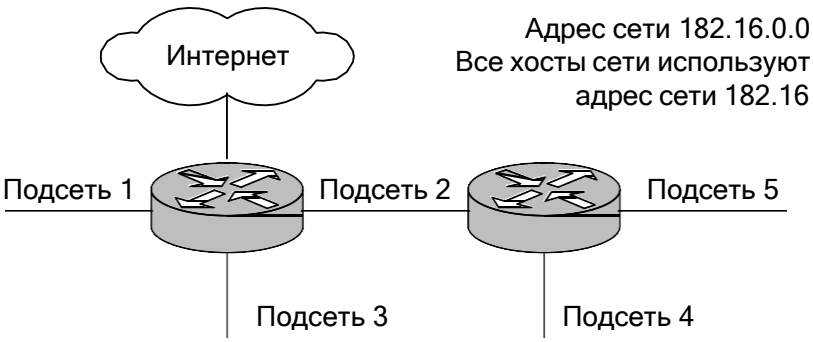
How same organize subnets? To V united networks IP highlight some more small ones logical subnets, Can take advantage of a feature of the software implementation of TCP/IP. The feature is that that some of the bits from the host address in the IP address are allocated to the so-called address subnets.

Methodology And order execution works:

Methodology

Selection subnets

Selection subnets is being implemented for check assignments some addresses subnets each car given physical networks. For example, on drawing 1.2 each car subnets 4 has address subnets, equal to 4.



Drawing 1.2 - Usage subnets

Let's look at the order in which the subnet address is placed in an IP address. The IP part addresses containing the network address cannot be changed, since all machines on the network share it. For example, all machines on the Acme network have an address networks, equal 182.16. That's why change Can only the second Part IP- addresses. IN scheme stations With subnets Part addresses hosta is being considered

How address subnets. On drawing 1.3 shown, How V IP address Maybe be built-in address subnets.

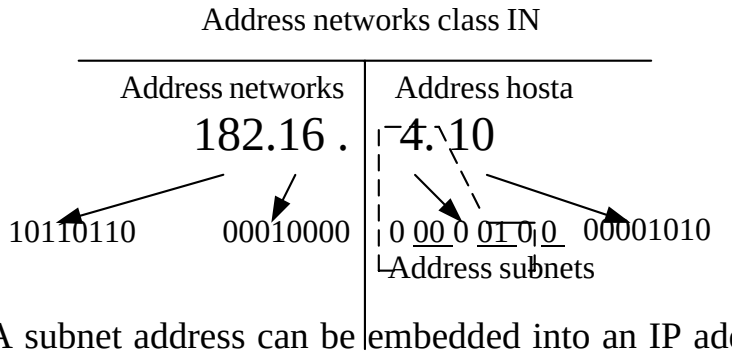
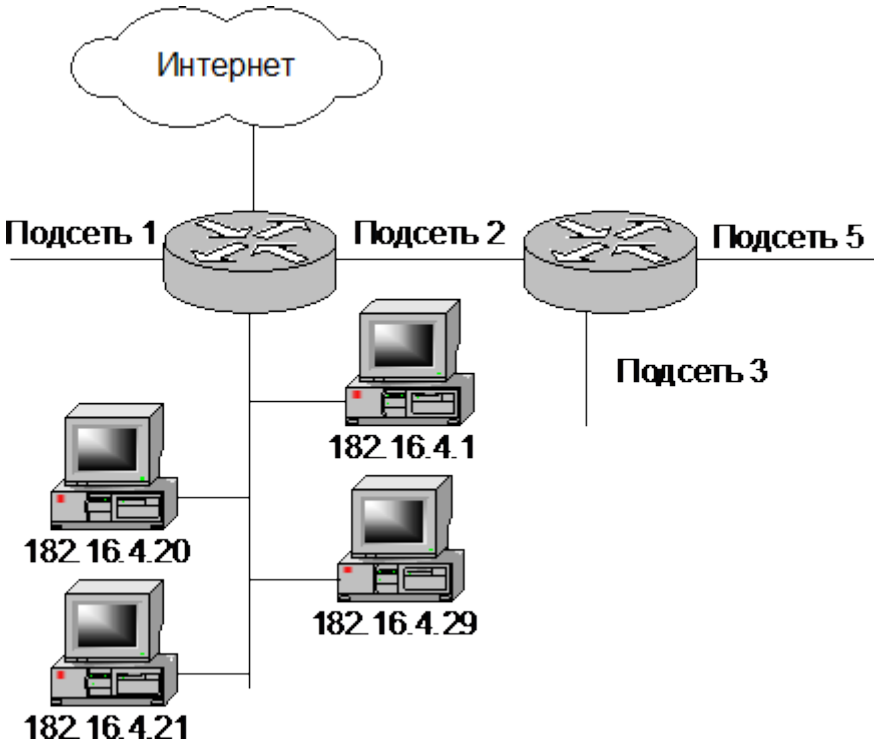


Figure 1.3 – A subnet address can be embedded into an IP address only in parts, related to the address hosta



Drawing 1.4 - Address networks And address subnets

Since the Acme network is a Class B network, the first two bytes of the IP-addresses contains address networks, together used by everyone cars networks, regardless of which subnets they belong to. The address of each cars subnets 4 must have V third byte number 0000 0100. Fourth byte (address host) contains unique number, identifying specific host. Like this in this way, V compound IP addresses are included three fields: address networks, address subnets And address host.

On drawing 1.4 shown, How are used addresses networks And subnets. This approach applicable To any subnets, allocated V composition networks.

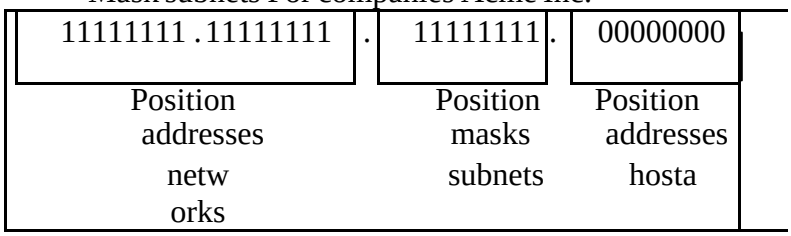
Masks subnets

When using a subnetted addressing scheme, each machine on the network must know what part of the host address is occupied by the subnet address. To do this, each car is being created mask subnets.

Coding discharges masks subnets

The units indicate the position of the network and subnet address.
Zeros marked position addresses hosts

Mask subnets For companies Acme Inc.



Drawing 1.5 - Mask subnets

Administrator network creates a 32-bit subnet mask consisting of from 0 And 1. Units V mask subnets mark positions, related To network and subnet addresses. Zeros are entered in the positions allocated for the address host. This idea illustrated on drawing 1.5.

In the example, the first two bytes of the subnet mask are filled with ones, since Acme networks belong to class B (format Network.Network.Node.Node). The third byte, usually related to the host address, is the address subnet. Therefore, all its bits are filled with ones. And only in the fourth byte stored unique address host.

Mask subnets Maybe be Also presented V decimal format. Binary combination 1111 1111 corresponds decimal number
255. Thus, the subnet mask of our example can be displayed in twoways. This idea illustrated on drawing 1.6

Двоичное представление
11111111.11111111.11111111.00000000

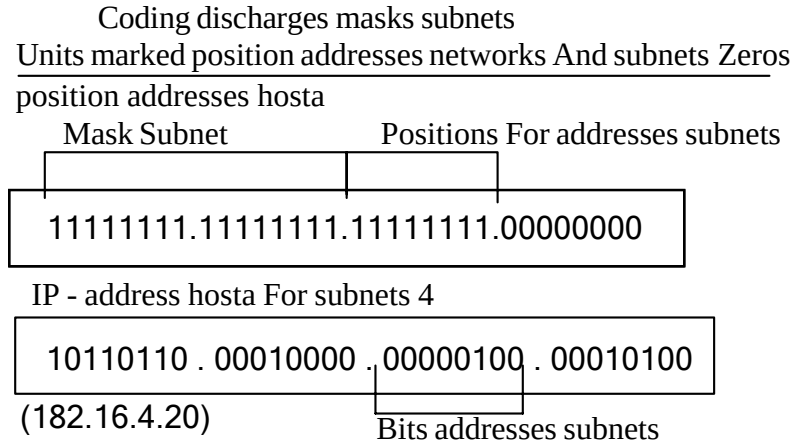
Десятичное представление:
255.255.255.0

Drawing 1.6 - View IP addresses With help masks subnets

At all not necessarily, to V compound networks entered subnets, T. e. The subnet mask may not be used. In such cases, they say that exists mask subnets, accepted By default. Masks, accepted By default values for different network classes (see Table 1.3) cannot be changed. Otherwise speaking, apply V quality masks subnets mask 255.0.0.0 Not is allowed. Host, to whom You you will try appropriate such mask, will consider it incorrect and will not allow this operation to be completed. Class A networks cannot change the first byte of the subnet mask, so it should start off With numbers 255. Except Togo, unacceptable mask 255.255.255.255, because this configuration means broadcast address. Mask subnets For networks class IN should start off 255.255 , A For networks class WITH - With 255.255.255.

Table 1.3 - Masks subnets, accepted By default

Class networks	Format addresses	Mask subnets
A	Network.Node.Node.Node	255.0.0.0
B	Network.Network.Node.Node	255.255.0.0
C	Network.Network.Network.Node	255.255.255.0



Drawing 1.7 - View IP addresses with help masks subnets

After Togo How administrator networks will create mask subnets For eachcars, software security protocol IP will browse IP-

addresses, using mask subnets For definitions addresses subnets, Corresponding operation presented on drawing 1.7.

IN this example By mask subnets programmatically is determined, What the third byte of the IP address no longer refers to the host address, but is occupied by the address subnets, equal 0000 0100.

If you use the third one to place the subnet address IP byte addresses class IN, That exercise And definition addresses subnets is relieved. For example, If V networks Acme Inc. necessary define subnet 12, V third byte addresses everyone cars of this subnets should insert 0000 1100.

When using the entire third byte of a Class B IP address for the address subnets can create quite a lot of subnets. Indeed, since A byte consists of eight bits, $2^8 = 256$ different addresses can be defined. Because address Not Maybe consist only from units or zeros, number The number of possible subnets is reduced to 254. Thus, in the Acme Inc. network You can allocate up to 254 subnets, each of which will contain up to 254 hosts.

Although V official specifications protocol IP application The zero subnet address is limited in some software products This address is still used. For example, adding special commands for Cisco router allows entering subnets with zero address, increasing the number of possible subnets to 255. However, by default this change impossible.

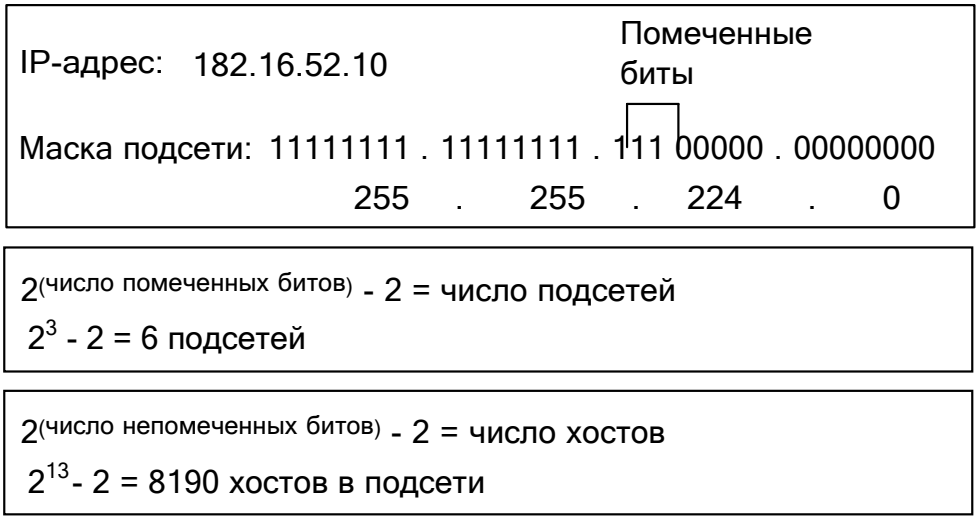


Figure 1.8 – Formulas for calculating the number of subnets and hosts Let us cite formulas For counting maximum numbers subnets And hosts V subnets:

$2^{\text{(number of marked bits in a mask subnets)}} - 2$ = maximum number subnets; $2^{\text{(number unmarked bits V mask subnets)}} - 2$ = maximum number hosts V subnets.

Marked are considered bits With single meaning, A *unmarked* - noughties bits. On drawing 1.8 given example applications these formulas.

Like this in this way, If number marked bits equals 3, according to The formulas given can be used to create up to six subnets. For addressing hosts have 5 bits left in the third byte and 8 bits in the fourth. With 13-bit addresses To subnets Can connect up to $2^{13} - 2 = 8190$ hosts.

At return to full use node address byte as subnet addresses (mask 255.255.255.0) possible number of nodes in each subnets will be reduced. Without subnetting address class IN may have 65,534 different values that are allowed to be used as addresses nodes.

If address subnets occupies full byte addresses node, remains only one byte for host addresses, i.e., up to 254 can be placed in a subnet hosts. When V some subnets will be required increase This number,

difficulties arise. To resolve them, it is necessary to either shorten the fieldsubnet addresses in the mask and thereby increase the length of the host address, or add secondary IP address To interface router, What Also will increase the number hosts in the subnet. However, a side effect such solutions will decrease quantities formed subnets.

Using Windows Calculator to Solve Network Problems

tasks

Network techniques are working on computers And network devices With binary, decimal And hexadecimal numbers. Required:

With help calculator Windows transform numbers V binary,decimal and hexadecimal systems numeration;

With help exponential functions determine number nodes, whichCan appoint addresses based on accessible numbers discharges.

Step 1: inclusion calculator Windows And definition hisoperating mode

a. From the Start menu, select **All Programs > Accessories** , andthen - " **Calculator** " rice 1.9.



Drawing 1.9 - External view calculator

An alternative method to launch the Calculator app is to openmenu " **Start** ", choose team " **Execute** ", enter **calc** And press key " **Enter** ". Try it both method.

b. After launch applications "Calculator" open menu " **View** ".c.

Determine, Which mode [Ordinary | Engineering] is active V given moment?

g. Select the "Standard" mode. This is the basic mode for simple calculations. Look, How many mathematical functions available V thismode? (Eight)

d. IN menu "View" select paragraph mode "Engineering".

Step 2: transition between systems numeration

a. Switch to **Engineering mode** . Pay attention to accessible modes systems numeration - Hex (hexadecimal), Dec(decimal), Oct (octal) And Bin (binary).

b. Look, which system numeration is used V given

moment? (Dec)

V. Please understand, What numbers (0 – 9) on digital keyboard active V decimal mode.

G. Install switch **Bin** (binary). Which numbers onnumeric keypad active V given moment? (0 and 1)

d. Why other numbers unavailable?

e. Install switch **Hex** (hexadecimal).

and. Make sure that symbols 0 - 9, a Also A, B, C, D, E And F on digital keyboard keys are currently active. In hexadecimal notation numeration (base 16) is used 16 numbers.

z. Install switch **Dec** . WITH help buttons mice clicknumber **1** and then number **5** on the numeric keypad. The field is entered decimal number 15. Install switch **Bin** .

And. What became With number 15 V text field at the top windows?

By switching modes, numbers are converted from one system to another. numbering to another. Switch back to **Dec mode** . The number in the window will return todecimal view. Select mode **Hex** .

l. Which hexadecimal number (0 - 9 or A – F) correspondsdecimal number 15?

m. Clean up window from numbers 15. Again go to V mode **Dec** . For input You can use not only the mouse but also the auxiliary digital key to enter numbers. keyboard and number keys. Using the auxiliary numeric keypad keyboards, located on the right from keys **Enter** , enter a number **22** .

If the number does not appear in the calculator field, press the **Num keyLock** " to enable the numeric keypad. After appearances numbers 22 V text field calculator With help keys Withusing the numbers at the top of the keyboard add **0** to the number 22 (then in the field should be displayed 220). Install **Bin** switch .

n. Which binary number corresponds decimal number 220?

O. Clean up window from numbers 220. IN mode binary systems numeration

enter next binary number: **11001100** . Install switch
Dec .

p. Determine, which decimal number corresponds binarynumber 11011100?

r. Transform next decimal numbers V binary. Make sure,What the results obtained are consistent given below numbers

Decimal number	Binary number
86	1010110
175	10101111
204	11001100
19	10011

With . Transform next binary numbers V decimal. Check it outreceived result.

Binary number	Decimal number
11000011	195
101010	42
111000	56
10010011	147

Step 3: transformation IP addresses nodes

a. Network computers typically have two addresses: an IP address and a MAC address. address Ethernet. For facilities users IP address usually seems to be Vas a group of decimal numbers separated by a decimal point, for example, 135.15.227.68. Each decimal octet in the address or mask can be convert to 8 binary digits. Remember that the computer understands only binary digits. If all 4 octet transform V binary form, How many discharges will it work? (IP address is 32-bit, 4x8).

b. IP addresses usually introduce themselves V view four decimal numbers, which accept values in within from 0 to 255 And separated point.
Transform 4 parts IP addresses 192.168.10.2 To binary view.

Decimal number	Binary number
192	11,000,000
168	10101000
10	1010
2	10

V. IN previous task pay attention attention on That, What number 10

is converted into only four digits, and 2 into two digits. Since in each any number from 0 to 255 can be specified for the IP address position, then for Each such number is usually provided using eight digits. in the previous example to represent the numbers 192 and 168 in binary form eight digits were required, but to represent the numbers 10 and 2, so many No digits are required. Usually, each converted to binary form The IP address number is followed by zeros (0) on the left to get eight binary numbers. Number 10 should be presented V view 00001010. Beforefour significant binary in numbers added four zero.

G. IN text field calculator V binary mode enter numbers **00001010** And install switch **Dec** .

d. Which one? decimal number corresponds 00001010?e.

They influence whether they are "leading" zeros on

number?

and. How should be presented number 2 (V previous example)eight digits?

Step 4: mask transformation IP subnets nodes

a. Subnet masks, such as 255.255.255.0, are also represented as decimal numbers With dividing dots. Mask subnets Always consists ofof four 8-bit octets, each of which is represented decimal number. Except for the decimal number 0 (all 8 binary digits are zeros) and the decimal number 255 (all 8 binary digits are units), each octet will have some number of ones on the left and some number of zeros on the right. Convert the 8 possible decimal values octets masks subnet to binary form.

Decimal number	Binary number
0	00000000
128	10000000
192	11,000,000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110

255	11111111

b. Transform four component masks subnets 255.255.255.0 Tobinary view.

Decimal number	Binary number
255	11111111
255	11111111
255	11111111
0	0 (8 zeros)

Step 5: transformation broadcast addresses

A. Network computers and devices use broadcast addresses for sending messages to entire groups nodes. Transform next broadcastaddresses.

Address	Binary number
Broadcast IP address 255.255.255.255	11111111 11111111 11111111 11111111
Broadcast MAC address FF:FF:FF:FF:FF:FF	11111111 11111111 11111111 11111111 11111111 11111111

Step 6: definition numbers nodes networks With help degrees numbers 2

a. Binary numbers are represented using two digits, 0 and 1. At calculation quantities possible nodes V subnets are used degrees numbers 2 because of binary performances. IN quality example Let's look at the subnet mask, which has six digits left in the IP part address corresponding to the node. In this case, the number of nodes in the network is 2 in 6- to the power minus 2 (since one number is required to represent the network, other - For achievements everyone nodes networks, those. For broadcast addresses). Always used number 2, as the work is underway in binary system numeration. Number 6 defines quantity discharges, corresponding to the nodes.

b. IN field calculator V mode **Dec** enter number **2** . Click button " **x^y** ", which corresponds to raising a number to a certain power. Enter the number **6.** Press the " = " button and then the " **Enter** " or " = " key onkeyboard - these are equivalent ways of obtaining the final result. In result will appear number 64. To subtract two, click button With

minus (-), then - button **2** , A V at the end - button " = ". In result will appear number 62.

This means, What Maybe be used 62 node.

V. WITH help described higher process determine number nodes, IfFor performances nodes is used following number discharges.

No. discharges For nodes	Number nodes
5	30
14	16382
24	16777214
10	1022

G. WITH help mastered method determine, what equals 10V 4th degrees.

d. Close calculator Windows.

Step 7: number identification networks And numbers nodes on basis masks subnets

a. The network IP address is 172.16.203.56 and the subnet mask is 255.255.248.0. Determine the network portion of the address and, based on the number remaining for the nodes discharges, calculate, how much is possible create nodes.

b. Get Started With transformations 4 octets decimal IP addresses V binary form, and then convert the decimal mask to binary form subnets. At transformation To binary form Not forget add leading zeros, to get 8 ranks For each octet.

IP address And mask subnets V decimal form	IP address And mask subnets V binary form
172.16.203.56	10101100. 00010000. 11001011. 00111000
255.255.248.0	11111111. 11111111. 11111000. 00000000

c. Align the 32 bits of the subnet mask with the 32 bits of the IP address and Compare them. The IP address digits corresponding to the ones digits in mask subnets, represent number networks. What binary And decimal number networks For this IP addresses? At first determine binary address (turn on all 32 discharge), A then transform his To decimal view.

Network address V binary form: 10101100. 00010000. 11001000. 00000000

Network address V decimal form: 172.16.200.0

G. How many discharges With units V this mask subnets?

_____21

d. How many discharges left to create nodes?

_____11

e. How many nodes Can create With remaining number of digits?

_____

2^11 = 2 048–2 = 2 046

Order execution works:

1) studying theoretical material laboratory work;
2) analysis original examples, given V this work;
3) execution tasks, proposed V work.

Tasks

1. In the network 172.16.0.0 it is necessary to allocate subnets so that Each subnet could connect up to 600 hosts. What mask? subnets follows choose, to allow height numbers subnets V future?

2. Network 172.16.0.0 contains 8 subnets. You need connect To subnets maximum possible number hosts. Which one? masksubnets should you choose?

3. IN networks 192.168.55.0 it is necessary to highlight maximum numbersubnets so that 25 hosts can be connected to each subnet. What mask? subnets follows choose?

4. Yours net class A contains 60 subnets. IN next two yearsyou need to organize another 40 subnets, and in such a way that each one of them, the maximum number of hosts could be connected. What mask subnets should you choose?

5. You have a class C network with the address 192.168.19.0 containingfour subnets. You need to set the maximum possible number of hosts on segment. Which one? mask subnets follows choose?

6. You have a class B network divided into 30 subnets. You wantadd 25 new subnets in the next two years. At the same time, you It will be necessary to connect up to 600 hosts to each segment. What mask subnets should you choose?

7. Network 192.168.1.0 needs to be divided into 9 subnets. necessary connect To to everyone segment maximum possible numberhosts. What mask? subnets should choose?

8. U you there is net class WITH With three subnets. To you necessary add 2 new subnets in the next two years. Each network must contain 25 hosts. What mask? subnets follows choose?

9. In your current Class C network address 192.168.88.0 necessary highlight maximum possible number subnets, V each fromwhich should be to 12 hosts. Which one? mask subnets follows choose?

10. You chose mask subnets 255.255.255.248. How many subnets And hosts You will you receive?

11. U you There is IP address 172.16.13.5 And mask subnets 255.255.255.128.Please specify Class addresses, address subnets And broadcast address.

12. U you There is 22-bit mask subnets. How many subnets And hosts You will you receive?

13. Transformation IP- And MAC addresses node

A. Click button " **Start** ", select team " **Execute** ",Type **cmd** and press **Enter** . In the command line enter **ipconfig /all** .

b. Note the IP address and physical address (also known as MAC-address).

IP address:

_____

MAC address:

_____

V. WITH help calculator transform four numbers IP addressesto binary view.

Десятичное число	Двоичное число

	Depends from computer
	Depends from computer
	Depends from computer
	Depends from computer

MAC address, or physical address, usually presented 12 hexadecimal digits, grouped in pairs and separated by dash (-). Physical addresses on computers under management Windows are usually displayed in the format xx-xx-xx-xx-xx-xx, where x is a digit from 0 to 9 or Latin letter from A to F. Every hexadecimal number in the address Can transform V 4-bit binary number, perceived computer. If All 12 hexadecimal numbers transform V binary form, How many discharges will it work? (MAC address is 48 bit, 12x4).

d. Transform every hexadecimal couple in binary form. For example, If group numbers CC-12-DE-4A-BD-88-34 corresponds physical address, convert the hexadecimal number to binary (11001100). Then transform To binary hexadecimal type number

12 (00010010) And So further. Make sure, What added necessary numberleading zeros to get 8 binary digits for each pair hexadecimal numbers.

Hexadecimal number	**Binary number**
	Depends from computer
	Depends from computer
	Depends from computer
	Depends from computer
	Depends from computer
	Depends from computer

Options tasks presented V next table:

Numbers options	Numbers tasks
1	1,3,5,13
2	2,4,6,13
3	1,7,5,13
4	3,8,9,13

5	2,10,12,13
6	4,7,11,13
7	1,6,12,13
8	8,9,10,13
9	3,6,4,13
10	2,5,10,13
11	4,8,12,13
12	1,9,11,13

Required decide tasks according to Yours option, and V tasks 1-12 write down results solutions V binary, decimal And hexadecimal systems numeration.

Content report And its form:

The report must be in a format consistent with the format of a simple abstract. Title sheet must include: Name disciplines, Name laboratory work, last name And initials handing over student, number groups, last name And initials host teacher. Main part of the work should contain:

A) answers on control questions, proposed V laboratorywork;

b) detailed consideration proposed examples laboratory work

V) description each stage execution tasks;G)

conclusions based on the work done work.

Exercise should be completed V in accordance With givenexamples.

Protection work
Protection work consists of:

1) V execution tasks And design report V in accordance With subparagraph "Content report and its form";

2) V answers on control questions By laboratory work;
3) V answers on additional questions.

Control questions

1. Concept about IP address.
2. Methods performances IP addresses.
3. Example hierarchical schemes addressing.
4. Characteristic classes networks.
5. Classes networks.
6. What such subnets? WITH Which goal They are used?
7. Reasons appearances subnets.
8. Selection subnets.
9. The main thing appointment masks subnets.
10. Masks subnets, accepted By default For classes networks.
11. Connection masks subnets With IP address.
12. Formulas For counting numbers subnets And hosts.
13. Examples definitions hosts And subnets.
14. Usage calculator Windows for solutions network tasks.

Practical class 5

TCP/IP Stack Data Link Layer (Part 2).

Target And content:

Target

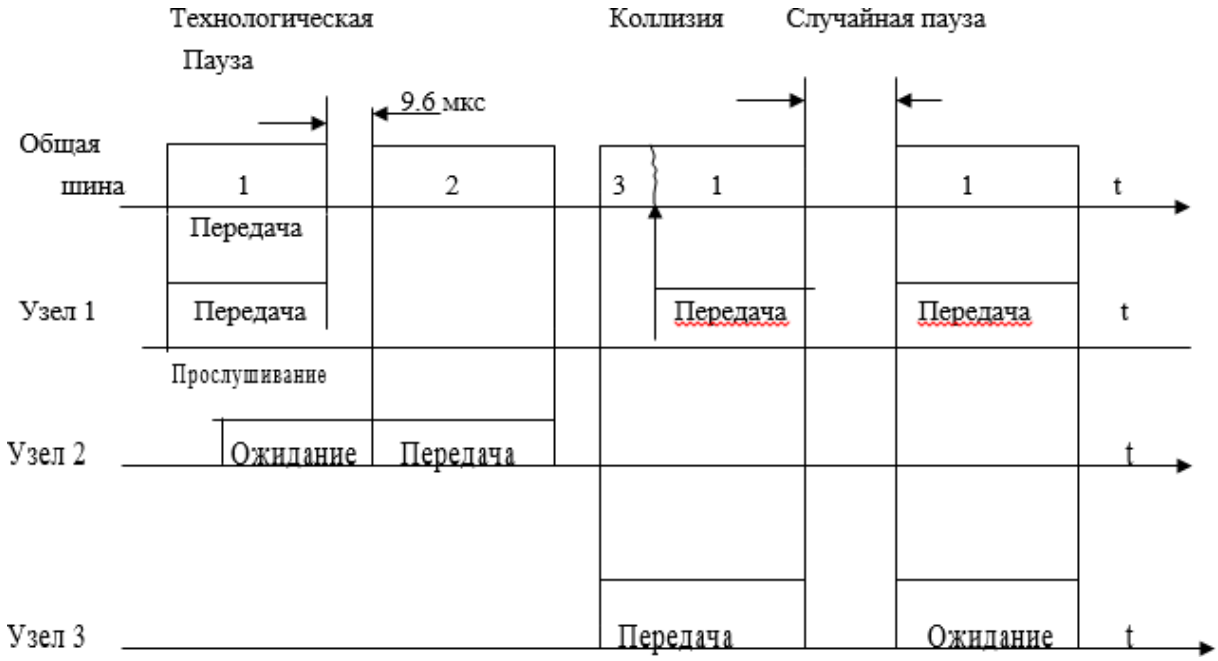
1. Construction local computing networks With using topologygeneral tire.
2. Construction With local computing networks using topology star.
3. Removal statistical characteristics, received projects local computing networks And their study.

Theoretical Part

Method random access CSMA/CD

Ethernet networks use a method of accessing the transmission medium called method collective access With identification load-bearing And detection collisions (CSMA/CD).

This method applies exclusively V networks with logical general tire (To which relate And radio networks, gave birth to this method). All computers such networks havedirect access To general tire, That's why she Maybe be used For transmissionsdata between any two network nodes. Simultaneously, all computers on the network have opportunity immediately (With taking into account delays distribution signal By physical Wednesday)receive data that any of the computers has started to transmit to the common bus (Fig. 3). Simplicity schemes connections - This one from factors, determined success standard Ethernet. It is said that the cable to which all stations are connected operates in collective modeaccess.



Stages access To environment

All data transmitted By networks, fit V frames certain structures And supplied unique address stations appointments.

To get opportunity transmit frame, station should make sure, What shared Wednesday free. This achieved listening basic harmonics signal,which Also it's called load-bearing frequency. Sign unemployment Wednesday is absence on her load-bearing frequencies, which at Manchester method coding equal 5-10 MHz, depending on the sequence of ones and zeros transmitted at a given time moment.

If Wednesday free, That knot has right begin transmission frame. This frame depictedin Fig. 3 first. Node 1 detected that the medium is free and began transmitting its frame. classical networks Ethernet on coaxial cable signals transmitter node 1 propagate in both directions, so that all network nodes receive them. A data frame is always accompanied by *preamble*, which consists of from 7 byte, consisting from values 10101010, And 8-go byte, equal 10101011(initial limiter frame). Preamble needed For occurrences receiver V bitwise And byte-by-byte synchronism With transmitter.

All stations connected to the cable can recognize the fact that a frame has been transmitted, and so a station that recognizes its own address in the frame headers records its contents in mine interior buffer, processes received data, transmits their up By to his own stack, and then sends a response frame down the cable. The source station's address is contained in the original frame, That's why receiving station knows, to whom need to send answer.

Knot 2 in time transmissions frame knot 1 Also tried begin transmission his own frame, however discovered, What Wednesday busy - on her present load-bearing frequency, - That's why knot 2forced wait, Bye knot 1 Not will stop transmission frame.

After endings transmissions frame All nodes networks obliged endure technologicala pause of 9.6 μs. This pause, called the interframe interval, is needed to bring network adapters V original state, A Also For prevention monopoly capture Wednesday one station. After endings technological pause nodes have rightstart transmitting your frame since the medium is clear. Due to propagation delays signal on the cable, not all nodes register the end of transmission at the same time frame knot 1 .

In the given example, node 2 waited for node 1 to finish transmitting the frame, and then pause V 9.6 ISS And started transmission his own frame.

Origin collisions

With the described approach, a situation is possible when two stations simultaneously p y- are hiding hand over frame data By general environment. Mechanism auditions Wednesday And pause betweenpersonnel do not guarantee against the occurrence of such a situation when two or more stations simultaneously decide, What Wednesday free, And they begin transmit their frames. They say, What in this case, a collision occurs **,** since the contents of both frames collide at a common cable And is happening distortion information - methods coding, used V Ethernet, Not allow highlight signals each stations from general signal.

Collision is a normal situation in the operation of the Internet networks . In the example shown on rice. 3, collision gave birth to simultaneous broadcast data knots 3 And 1 . For occurrence collisions Not Necessarily, to some stations started transmission absolutely simultaneously, such a situation is unlikely. It is much more likely that a collision occurs because one node starts transmitting before the other, but before the second node signals first Just Not they have time get there To to that time, When second knot decides begin transmission his own frame. That There is collisions - This investigation distributed character networks.

To correctly handle the collision, all stations simultaneously monitor emerging on cable signals. If transmitted And observable signals differ, That is fixed **collision detection** . For increases probabilities as soon as possible detection

collisions by all stations in the network, the station that detects the collision interrupts transmission his own frame (V arbitrary place, Maybe, And Not on border byte) And strengthens situation collisions by parcel V net special sequences from 32 bit,called **jam sequence** .

After this discovered collision transmitting station obliged stop transmission and pause for a short random interval of time. Then it Maybe again undertake attempted capture Wednesday And transmissions frame. Random pause is selected By to the next one algorithm:

Pause = L* (interval deferments),

where the backoff interval is equal to 512 bit intervals (in Ethernet technology , All intervals are measured in bit intervals; a bit interval is denoted as btand corresponds to the time between the appearance of two consecutive data bits on the cable;For speed 10 Mbps magnitude bitwise interval equal 0.1 μs or 100 ns);

L is an integer chosen with equal probability from the range [0, 2^N], Where N — number repeated attempts transmissions this frame: 1,2,..., 10.

After 10th attempts interval, from whom is selected pause, Not increases.
Like this in this way, random pause Maybe accept values from 0 to 52.4 ms.

If 16 sequential attempts transmissions frame cause collision, That transmitter must stop attempts And discard this frame.

From descriptions method access it is visible, What He wears probabilistic character, And probability successful receipt V your own order general Wednesday depends from network congestion, that is, from the intensity of the occurrence of demand at stations transmission of frames. When this method was developed in the late 1970s, it was assumed that The data transfer rate of 10 Mbps is very high compared to the needs computers in mutual data exchange, so the network load will always be small.This assumption remains sometimes true to this day, but there have already appeared applications that work in real time with multimedia information, which Very are loading segments Ethernet. At this collisions arise much more often. Atsignificant collision intensity, the useful bandwidth of the Ethernet network sharply drops because the network is almost constantly busy with repeated attempts to transmit frames. For reduction intensity occurrence collisions need to or decrease traffic, by reducing, for example, the number of nodes in a segment or replacing applications, or by increasingspeed protocol, For example, go to on Fast Ethernet. It follows note, What method accessCSMA/CD does not guarantee the station at all that it will ever be able to access environment. At small load networks probability such events small, But at with the network utilization rate approaching 1, such an event becomes very probable. This drawback of the random access method is the price to pay for its extreme simplicity, which made Ethernet technology the most inexpensive. Other access methods include tokenToken Ring and FDDI network access, the Demand Priority method of 100VG-AnyLAN networks are free from this shortage.

Time double turnover And recognition collisions

Clear recognition collisions by everyone stations networks is necessary condition correct work networks Ethernet. If any transmitting station Not recognizes collision and decides that the data frame has been transmitted correctly, then this data frame will be lost. Due to the overlap of signals during a collision, the frame information will be distorted and it will be rejected.host station (Maybe, because of discrepancies checksum). Rather in total,distorted information will be repeated transferred any protocol top level, for example, transport or application, working with the establishment of a connection. But retransmission of the message by the upper layer protocols will occur after a significant amount of time a longer time interval (sometimes even a few seconds) compared tomicrosecond intervals, which operates protocol Ethernet. Therefore, if collisions

Not will be reliably be recognized knots networks Ethernet, That This will come To noticeable decrease useful pass capabilities this networks.

For reliable recognition collisions should be carried out following ratio: $T_{min} \geq PDU$,

Where T_{min} is the transmission time of a frame of minimum length, and PDU is the time it takes signal collisions manages to spread to himself distant node networks. So How V the worst case signal must pass twice between most remote Friend from friend stations networks (one way passes undistorted signal, and on the way back the signal already distorted by the collision is propagated), then this time is called time double turnover.

When this condition is met, the transmitting station must have time to detect collision, which called transmitted her frame, more to Togo, How she will finish the transmission thisframe.

Obviously, What execution this conditions depends, With one sides, from lengths minimum frame And pass capabilities networks, A With another sides, from lengths cable network systems and the speed of signal propagation in the cable (for different types of cable this speed some differs).

All parameters protocol Ethernet selected like this in this way, to at normal work nodes networks collisions Always clearly were recognized. At choice parameters the above relationship, which connects the minimum, is also taken into account length frame And maximum distance between stations in the segment networks.

The Ethernet standard states that **the minimum length of the frame data field is is 46 bytes** (which together with the service fields gives a minimum frame length of 64 byte, and together with the preamble - 72 bytes or 576 bits). From here it can be determined limitation on distance between stations.

In 10-megabit Ethernet, the transmission time of a frame of minimum length is 575 bit intervals, therefore, the double rotation time must be less than 57.5 μs. The distance a signal can travel in this time depends on the type of cable. For thick coaxial cable the distance is approximately 13,280 m. Considering that for this time the signal must travel along the communication line twice, the distance between the two nodes is not should be more 6 635 m. IN standard magnitude this distances chosen significantlyless, with taking into account others, more strict restrictions.

One of these limitations is related to the maximum permissible signal attenuation. To ensure the required signal power when passing between the most remote from each other stations of the cable segment, the maximum length of continuous segment of thick coaxial cable, taking into account the attenuation it introduces, was chosen at 500 m. On a 500 m cable, the collision detection conditions will be met with greater reserve for frames of any standard length, including 72 bytes (double time The turnover of a 500 m cable is only 43.3 bit intervals). Therefore, the minimum The frame length could have been set even shorter. However, the developers of the technology did not began to reduce the minimum frame length, keeping in mind multi-segment networks, which are being built from several segments, united repeaters.

Repeaters increase the power of signals transmitted from segment to segment, As a result, signal attenuation is reduced and a much larger network can be used lengths, consisting from several segments. IN coaxial implementations Ethernet The developers limited the maximum number of segments in the network to five, which in turn The queue limits the total network length to 2,500 meters. Even in such a multi-segment networks condition detection collisions as before is being carried out With big in stock (let's compare received from conditions acceptable attenuation distance V 2500 m With calculated higher maximum possible By time distribution signal distance of 6635 m). However, in reality the time reserve is significantly less, because V multi-segment networks ourselves repeaters contribute V spreading

signal an additional delay of several tens of bit intervals. Smallstock was made the same way For compensation deviations parameters cable and repeaters.

IN result accounting everyone these And some others factors was thoroughly the ratio between the minimum frame length and the maximum possible one has been selected distance between stations networks, which provides reliable recognition collisions. This distance they call Also maximum diameter networks.

WITH increase speed transmissions frames, What has place V new standards, maximum distance between stations networks decreases proportionally increase the transmission speed. In the Fast Ethernet standard it is about 210 m, in In the Gigabit Ethernet standard it would be limited to 25 meters if the developers standard Not undertaken some measures By increase minimum size package.

Table 1 shows the values of the main parameters of the frame transmission procedure. standard 802.3, which Not depend from implementation physical environment. Important note, What Each variation of the physical medium of Ethernet technology adds to these limitations their own, often more strict restrictions, which Also should be carried out.

Table 1. Parameters level MAS Ethernet

Parameters	Values
Bitwise speed	10 Mbps
Interval deferments	512 bit interval
Interframe interval	9.6 ISS
Maximum number attempts transmissions	16
Maximum number increase rangepauses	10
Length jam sequences	32 bits
Maximum length frame (without preambles)	1518 byte
Minimum length frame (without preambles)	64 bytes (512 bit)
Length preambles	64 bit
Minimum length random pausesafter collisions	0 bits int.
Maximum length of random pauses after collisions	524000 bits. int
Maximum distance between stations networks	2500 m
Maximum number of stations V networks	1024

Methodology and procedure for performing
the workMethodology

1. Construction local computing networks With using topologygeneral tire.

For this necessary execute next actions:

1. Launch NetCracker Professional having chosen Programs==> NetCracker Professional 3.2 ==> NetCracker Professional from menu " Start ".
2. From menu File select paragraph New.
3. IN device browser find paragraph "GenericLANs".

4. Move required devices V working region, following nextinstructions:

a. Select Thin Ethernet Segment V under the window images and move to working region.

b. Change dimensions images devices V working areas By yoursat your discretion.

c. Enlarge size font signatures To device, having chosen from contextualmenu item "Properties".

5. Add four workers stations V working window areas.

a. Find paragraph LAN workstations», then Workstations And select folder Generic Devices».

c. Pull out Ethernet Workstation.It

will work following (drawing 2.1):

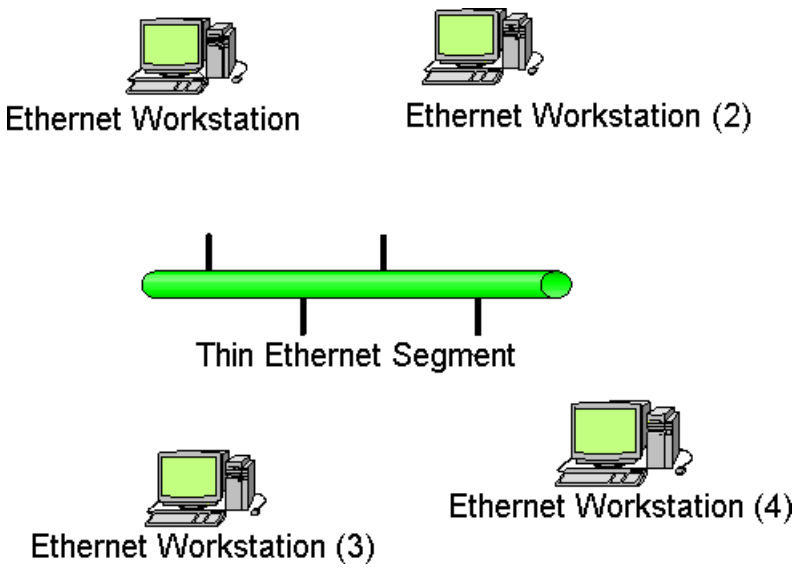


Figure 2.1 – External appearance of

workstationsWay definitions compatible

devices:

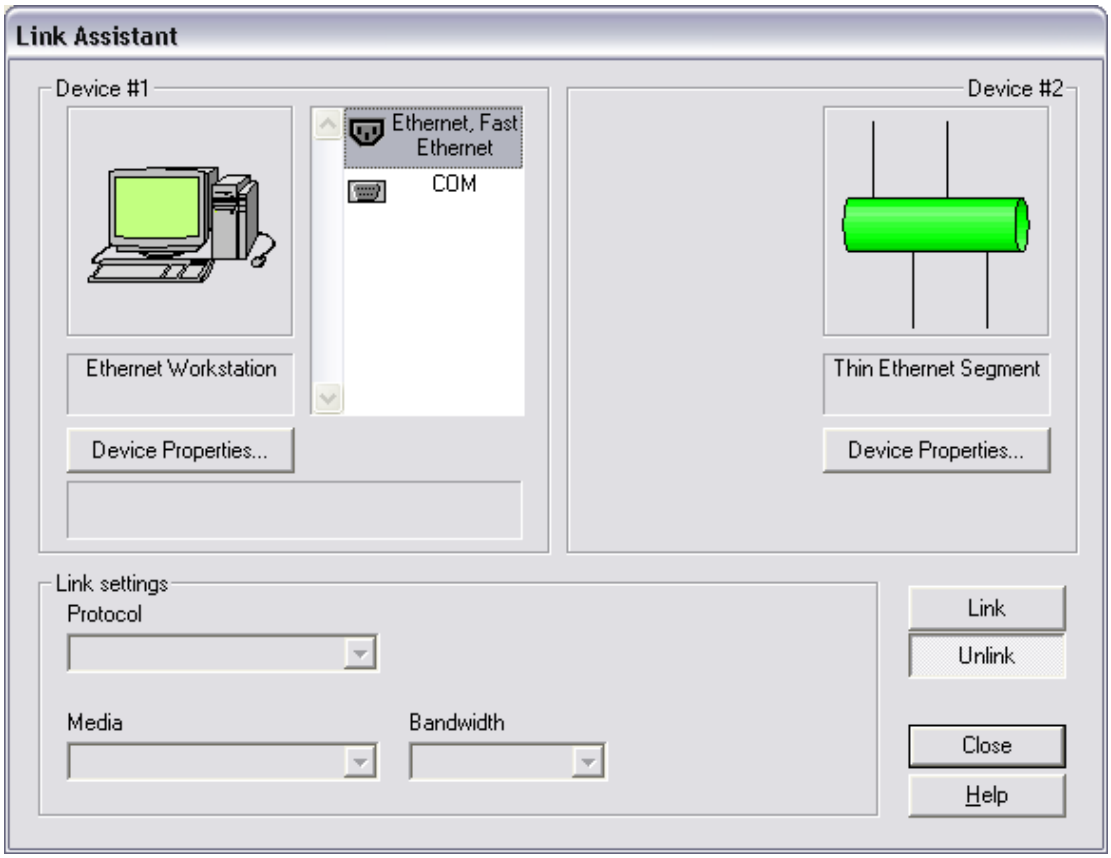
1. Click the mouse on device.

2. Select paragraph "Find compatible" (Find Compatible) from menu Objects (Objects).

7. Compound tires and workers stations.

a. IN mode panels press the button  .

b. Click left button mice at first on Ethernet Workstation, A Then onThin Ethernet Segment. This will appear dialogue (Figure 2.2):



Drawing 2.2 - External view panels Link Assistant

c. Click buttons "Link", then "Close", to install connection And close wind d. For fast installations connections hold on key Shift, click mouse on ow.

Ethernet Workstation, A Then on tire . It will appear connection without appeals To dialogic window.

8. Choice type Wednesday transmissions.

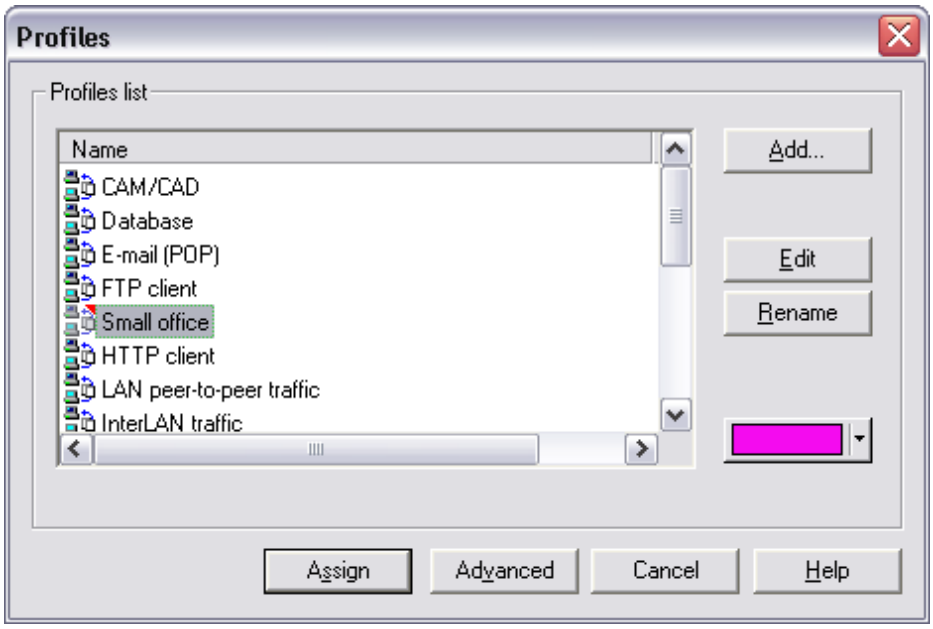
a. From the View menu, select Legends. Black color connections V yours project means coaxial line.

b. Close dialogue button "Close."

9. Choice type traffic between workers stations.

a. Click button Set Traffics .

b. Click left button mice on Ethernet Workstation, then on EthernetWorkstation (4) Will appear such a dialogue (picture) 2.3):



Drawing 2.3 - External view panels Profiles

c. Select type traffic Small Office» between workers stations.

d. Click button "Assign", to install given type traffic.

e. Repeat steps 9b-d, but now left-click first on Ethernet Workstation (4), A then on Ethernet Workstation.

f. Repeat steps 9b-e For Ethernet Workstation (2) And Ethernet Workstation (3).

10. Examination performance created project networks. Click on managing panels button "Start". Through segment will run packages between workers stations.

11. Regulation intensity interactions informational exchange.

a. Click button Animation Setup» , And V appeared dialoguemove regulator "Packet intensity».

b. Click the OK button. After a few seconds, the traffic intensity shouldchange.

12. Change speed movements packages.

a. Click button Animation Setup» , And V appeared dialoguemove regulator "Packet speed».

b. Click button OK. Through some seconds speed packages should change.

13. Change sizes images packages.

a. Click button Animation Setup» , And V appeared dialoguemove regulator "Packet size».

b. Click button OK. Size images of packages must change.

14. Take a look on used You devices And select bookmark Recently used» - "Used" V under the window images.

15. Location cards How background worker windows.

a. From contextual menu worker windows select Site Setup» - "Settings windo
ws." b. On bookmark Background put tick "Map".WITH help buttons Browse select file cards.

To understand, O what are you talking about, take a look on this one panel (Figure 2.4):



Drawing 2.4 - External view panels Site Setup

16. Coloring background. From contextual menu working window select Site Setup» - "Settings windows."

a. On bookmark Background take off tick "Map".

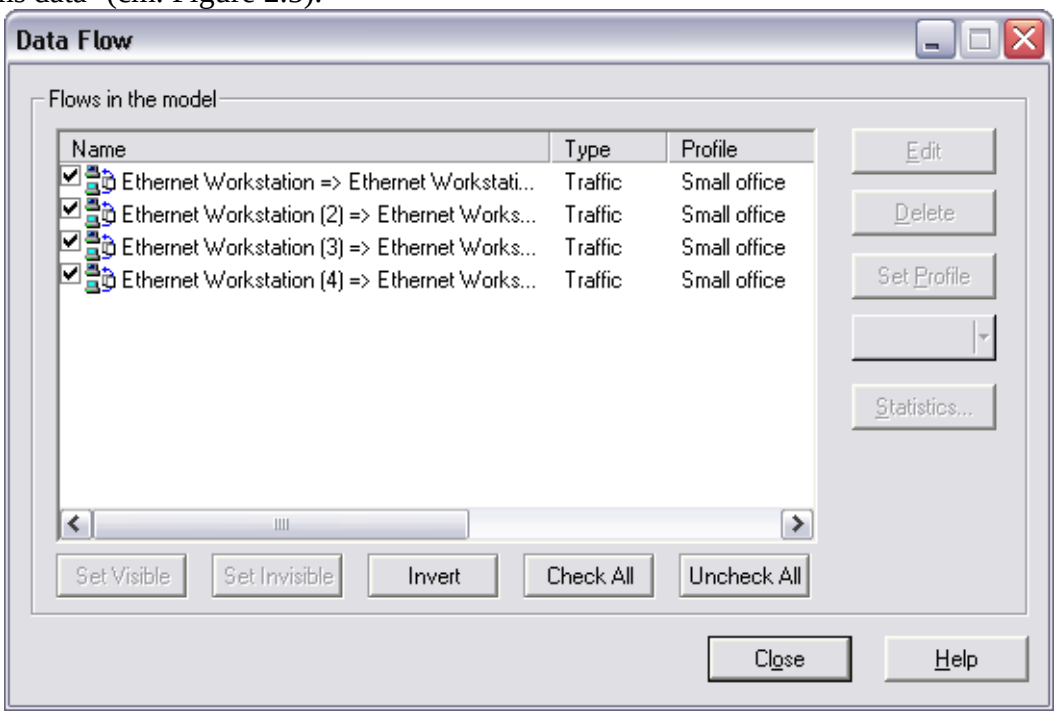
b. IN list "Page" select color By to taste.

c. IN list Non-printing select another color.

d. Click OK.

You can add color background And V window, containing already image cards.

17. Profiles traffic. From menu Global - "All", select paragraph "Data flow» - "Streams data" (cm. Figure 2.5).



Drawing 2.5 - External view panels Data Flow

IN appeared dialogue will be displayed profiles already selected You types traffic.

18. Increase networks.

a. Add to working window another Thin Ethernet segment Segment and more Multiple Ethernet Workstations. Connect them to the network by repeating steps 9b-e. For new workers stations.

b. Try it create compound between two segments Thin Ethernet Segment and Thin Ethernet Segment (2). As a result, you will receive the following message (see drawing 2.6)



Drawing 2.6 - External view windows at attempt connections two segments directlyFor connections of two segments V one net to you necessary put between them adapter.

c. Select standard cursor button Standard V mode panels.

d. IN browser devices find list "Media adapters and converters andtransceivers», then Generic Devices».

e. IN under the window images select "Ethernet Media" Converter", move onfree place in working order window.

f. Create compound between Thin Ethernet Segment And Ethernet Media Converter. Repeat process compound For Ethernet Media Converter And Thin Ethernet Segment (2).

g. Now You you can appoint traffic To example For Ethernet Workstation And Ethernet Workstation (6).

h. Launch project And check his performance.

2. Construction With local computing networks using topology star.

1) From menu File select item New.

2) IN browser devices find paragraph "Switches". Then expand points Workgroup, Ethernet, D-Link Systems.

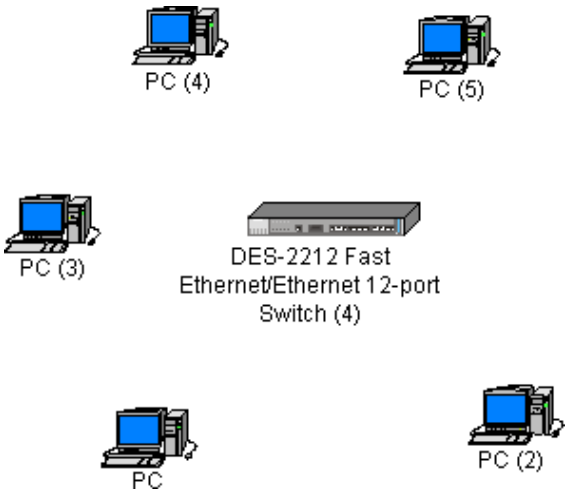
a) Move the DES-2212 Fast Ethernet/Ethernet 12-port to the workspace Switch having chosen his V under the window images.

b) Open the properties of this switch, the Ports tab, based on this switch You can create a network of 8 workstations using Ethernet network cards and 4 connections at use adapters Fast Ethernet.

3) Add several workers stations V working window areas.

a. Find paragraph LAN workstations», then "PCs" and select folder "Generic Devices».

c. Pull it out PC. Must it will work out following (drawing 2.7):



Drawing 2.7 - External view workers stations

4) Add network adapters V workers stations.

a. Collect paragraph LAN workstation".

b. Find LAN adapters», «Ethernet», « Generic Devices».

c. Add By alone Ethernet adapter V workers PC stations , PC(2), PC(3). AND By alone Fast Ethernet adapter in PC(4), PC(5).

d. Create a connection between the switch and the stations. When connecting pay attention attention on compatibility between various ports And network cards.

e. Assign traffic between workers stations How This was described V question 1, paragraph 9.

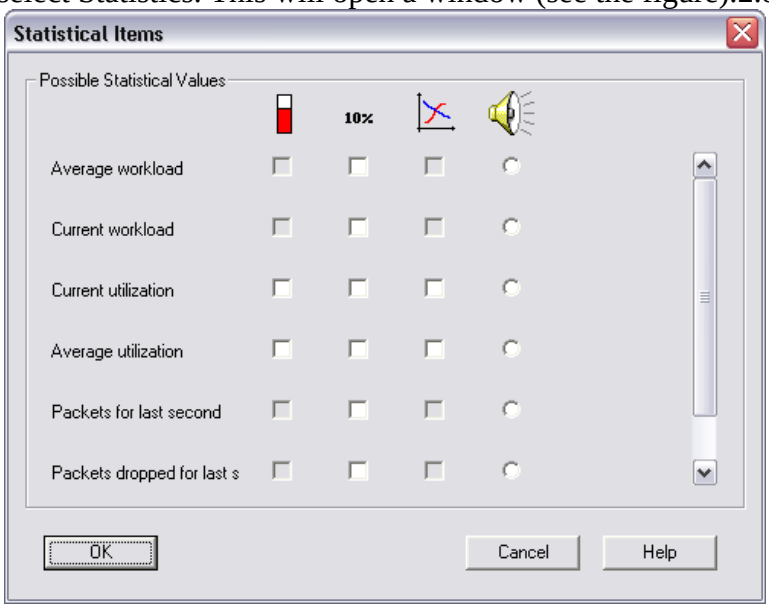
5) Add V working area still one switch. Select DES-5024 Fast Ethernet/Ethernet 24-port Modular Switch from "Switches", Workgroup, Ethernet, D-Link Systems.

a) Transfer more some workers stations, add To him adapters Andappoint traffic, repeating the actions points 3 And 4.

Received net will have topology star consisting from two segments.

3. Removal statistical characteristics, received projects local computing networks And their study.

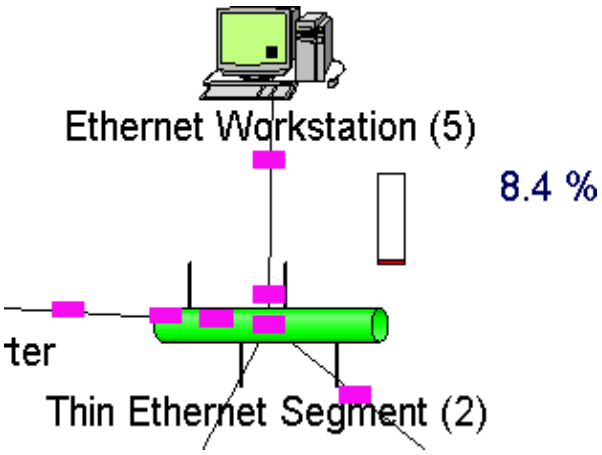
a. Right button mice click on any from lines connections And V In the context menu, select Statistics. This will open a window (see the figure).2.8)



Drawing 2.8 – External view windows statistics

b. Put it check marks, For example, against Current utilization V first column And against Average utilization in second. Click OK.

c. Now You you can see statistics selected you lines (cm. drawing 2.9)



Drawing 2.9 – Statistics

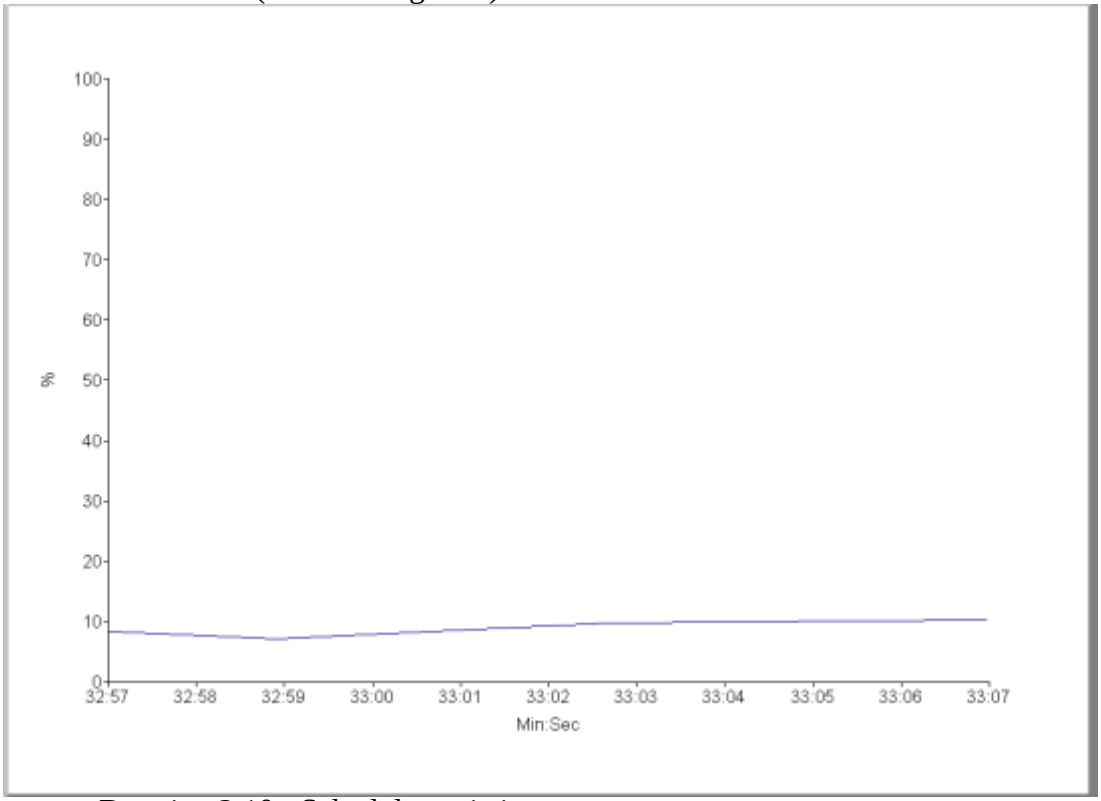
d. Try it change intensity transmissions packages And look, Whatit will work out.

IN NetCracker Also creation is possible graphs.

a. Right -click click on any from lines connections And V contextual menu select paragraph Statistics.

b. Put it tick, For example, against Average utilization V third column.Click OK.

c. On screen reflective graph work selected lines (cm. drawing 2.10).



Drawing 2.10 - Schedule statistics

a. From menu File select team Save.

b. By default Name file will Net1.net. You you can change his on such,what do you think? necessary. Extension .NET will be added automatically.

c. Close project, preliminary stopping his.

d. Build single-level network project according to Yours option tasks,guided by rules, set out higher.

Options tasks:

1. Build network project LAN Ethernet, having topology general tire.
2. Build network project LAN Ethernet, having topology star.
3. Build network project LAN Ethernet, having topology hierarchical star.
4. Removal of statistical characteristics obtained from local projects computing networks And their study.

Order execution works:

1) studying theoretical material laboratory work;
2) analysis original examples, given V this work;
3) execution tasks, proposed in laboratory work.

Control questions:

1. IN what kind topological structures is used method access To environment transmissionsdata CSMA/CD?
2. Name it stages access method CSMA/CD To environment data transfer.
3. Name it appointment preambles and her content.
4. For what necessary interframe interval and what his meaning?
5. What such collision? Describe her.
6. For what necessary jam sequence?
7. How is being formed random pause?
8. How is being carried out recognition collisions?
9. Name it minimum length fields data.
10. Name it parameters level MAS Ethernet.

Practical class 6

TCP/IP Stack Data Link Layer (Part 3).

Target And content:

Target

Learn the basic principles of configuring communicationsequipment Switch 2960.

Content

1. Registration on Switch.
2. Installation dates And time on switch
3. Installation passwords.
4. Change name V device Switch 2960
5. Installation IP addresses
6. Configuring ports

Theoretical justification:

Switch is a network device that performs filtering, distribution and creation of a frame stream based on the analysis of the recipient's address. Functions on channel level models OSI.

Methodology And order execution works:

Methodology

Registration on Switch

At registration on device Switch 2960 You you see invitation Exec interpreter in user mode, information about the device appears andmanaging menu:

```
Catalyst 2960 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-30-80-C7-BE-C0

PCA Number: 73-3122-04
PCA Serial Number: FAB033723WJ
Model Number: WS-C1912-A
System Serial Number: FAB0338S10A
Power Supply S/N: APQ032404SA
PCB Serial Number: FAB033723WJ,73-3122-04
-----------------------------------------.
1 user(s) now active on Management Console.
User Interface Menu
[M] Menus
[K] Command Line
Enter Selection:
```

Menus (Menu) - this item allows you to make a step-by-step selection configurations. At choice keys [M] additional appears menu:

```
Catalyst 2960 - Main Menu
[C] Console Settings
```

[S] System
[N] Network Management
[P] Port Configuration
[A] Port Addressing
[D] Port Statistics Detail
[M] Monitoring
[V] Virtual LAN
[R] Multicast Registration
[F] Firmware
[I] RS-232 Interface
[U] Usage Summaries
[H] Help
[K] Command Line
[X] Exit Management Console
Enter Selection: (Produce choice)

Let's consider second paragraph manager menu Command Line (Team line). It allows you to configure the device using controls commands, a list of which is easy to obtain. First, you need to select the [K] key. After the operation is completed, the Exec prompt will appear indicating that you are you located? V user mode (user mode).

Enter Selection:
CLI session with the switch is open.
To end the CLI session, enter [Exit].
>

For Togo to to know, which teams You you can fulfill necessary, producenext operation:
>?
Exec commands: Explanation each from teams presented V table 2.1.

Table 2.1 - Teams user regime

Name teams	Transcript teams
Enable	Turn on privileged commandsprivileged regime)
Exit	Exit from the EXEC (Complete) work interpreter Exec)
Help	Description of the interactive help system (Description dialogicreference systems)
Ping	Send echo messages (Send echo message)
Show	Show running system information (Withdraw bootable information O system)
Session	Tunnel to module (Module tunnel)
Terminal	Set terminal line parameters (Installation parameters terminal)

On this stage Can perform operations Not global scale, What characterizestable 2.1.

For Togo to produce global configuration necessary executeteam enable And go to V privileged regime (privileged) mode).
>enable
#
Also How And V user mode, list acceptable teams And receipt anyreference information, necessary produce input "?".
#?

Exec commands:
clear Reset functions
configure Enter configuration mode
copy Copy configuration or firmware
delete reset configuration
disable Turn off privileged commands
enable Turn on privileged commands
exit Exit from the EXEC
help Description of the interactive help system
menu Enter menu interface
ping Send echo messages
reload Halt and perform warm start
session Tunnel to module
show Show running system information
terminal Set terminal line parameters
vlan-membership VLAN membership configuration

Installation dates And time on switch

For this V privileged mode we use next command :Switch#clock set 12:29:30 20 October 2011
For viewing established dates we use teamSwitch #SH CLOCK
11:35:49.985 word ?? ??? 20 2011

Installation passwords

For installations passwords on manager console And entrance V privileged modenecessary produce as follows:
#config t
Enter configuration commands, one per line. End with CNTL/Z.
(config)#enable password level 1 kmlp
(config)#enable password level 15 mklp
(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
#
For installations password permitted secret necessary execute next commands:(config)#enable secret mklp9
(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
#disable
>en

Enter password:*****
#

Change name V device Switch 2960

For changes device name necessary execute in mode configurations "configure terminal» team hostname And enter other Name :
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.(config)#
hostname Switch_My
Switch_My(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Switch_My#

Comment: at execution any operations all changes V deviceare saved automatically.

Installation IP addresses

For installation IP addresses And gateway V mode configurations we are performing next command:

```
#conf t
Enter configuration commands, one per line. End with CNTL/Z.
(config)#hostname MySwitch_1
MySwitch_1(config)#ip host 172.16.10.16 255.255.255.0
MySwitch_1(config)#ip default-gateway 172.16.10.1
MySwitch_1(config)#^Z
```

To look information O settings switch we use team showrunning-config:

```
 Switch_My #sh running-config
Building configuration...

Current configuration : 1108 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password encryption
!
hostname Switch_My
!
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jJVK/
!
clock timezone word 23 23
!
IP host 172.16.10.16 255.255.255.0
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface Vlan1
 no IP address
 shutdown
!
IP default-gateway 172.16.10.1
!
!
line con 0
!
line vty 0 4
```

```
 password 123
 login
line vty 5 15
 login
!
!
End
```

Configuration ports

For choice configuration ports necessary execute next commands. In configuration mode, the command "interface" name and number is entered interface.

```
#config t
Enter configuration commands, one per line. End with CNTL/Z.
(config)#hostname My_switch
My_ switch( config)#interface Ethernet ?
<0-0> IEEE 802.3
My_switch(config)#interface Ethernet 0?
/
My_switch(config)#interface Ethernet 0/?
<1-25> IEEE 802.3
My_ switch( config)#interface Ethernet
0/1My_switch(config-if)#?
Interface configuration commands:
cdp Cdp interface subcommands
description Interface specific description
duplex Configure duplex operation
exit Exit from interface configuration mode
help Description of the interactive help system
no Negate a command or set it defaults
port Perform switch port configuration
shutdown Shutdown the selected interface
spantree Spanning tree subsystem
vlan-membership VLAN membership configuration
My_switch(config-if)#
My_ switch( config-if)#?
Interface configuration commands:
cdp Cdp interface subcommands
description Interface specific description
duplex Configure duplex operation
exit Exit from interface configuration mode
help Description of the interactive help system
no Negate a command or set it defaults
port Perform switch port configuration
shutdown Shutdown the selected interface
spantree Spanning tree subsystem
vlan-membership VLAN membership configuration
My_switch(config-if)#
```

Configuration descriptions interfaces

At establishment descriptions, necessary produce installation V mode configurations, choose port And execute team description And itself description.

My_switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
My_switch(config)#interface e 0/1
My_ switch(config-if)#description
finance_vlanMy_switch(config-if)#int f0/26
My_ switch(config-if)#description
trunk_to_Building_4My_switch(config-if)#

Information about interface Can get With help next teams.

My_switch#show int e0/1
Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0030.80C7.0180
MTU 1500 bytes, BW 100,000 Kbits
802.1 d STP State: Forwarding Forward Transitions: 1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: finance_vlan
Duplex/Flow Control setting: Half duplex
Enhanced Congestion Control: Disabled
Boot information Can get With help teams show run».My_switch#show run
Current configuration:
!
hostname My_switch
!
IP address 186.124.2.0 255.255.240.0!
!
Ethernet interface 0/1
description 'finance_vlan'
!
interface FastEthernet 0/26
description 'trunk_to_Building_4'
!
interface FastEthernet 0/27
line console
end

Application teams duplex

For configurations duplex applies team "duplex".

My_ switch(config)#int f0/26
My_switch(config-if)#duplex full
My_switch(config-if)#^Z

Table 2.2 - Command parameters duplex

Parameter	Description parameter
Auto	Automatic definition regime
Full	Produce installation V full-duplex mode
Full-flow-control	Usage full-duplex regime on 100 Mbps
Half	Usage half duplex regime on 10 Mbps

Cleaning memory is being carried out team delete

My_Switch#delete nvram

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.
Reset system with factory defaults, [Y]es or [N]o ?YES

After done operations is being carried out cleaning bootable information.

Order execution works:

1) studying theoretical material laboratory work;
2) analysis original examples, given V this work;
3) execution tasks, proposed V laboratory work.

Tasks

In the beginning necessary clear All information from Switch And execute specified belowoperations.

Set the IP address and gateway for the device, change the Switch name, install Allowed password for console and privileged mode, allowed secret. Ports Ethernet 0/1, Ethernet 0/2, Ethernet 0/3 install V half-duplex mode, A FastEthernet 0/26 V full-duplex mode, FastEthernet 0/27 V full-duplex mode on
100 Mbps, A All rest Ethernet ports V auto mode. Check Executing the set parameters. View information about the Switch. ViewAll subparagraphs menu devices.

After Togo How You make sure What All actions were completed Right, need to call teacher And introduce For control completed exercise.

Content report and its form:

The report should be in the format of a simple abstract. Title page the sheet should include: the name of the discipline, the name of the laboratory work, the last name and initials handing over student, number groups, last name And initials host teacher. Main Part laboratory work should contain:

a) answers to the control questions proposed in the laboratory work; b) a detailed examination of the proposed examples of laboratory work V) description each stage execution tasks;

G) conclusions By done work.

Exercise should be completed V in accordance With examples laboratory work.

Control questions And protection works:

Control questions.

1. IN What is it registration Switch?
2. Menu Switch.
3. Teams user regime.
4. Ports devices Switch.
5. Establishment passwords.
6. What means team interface?
7. What means team duplex.
8. Parameters teams duplex.
9. Cleaning And preservation bootable information.

Protection work

Protection work consists of:

1) V execution tasks And design report V in accordance With subparagraph "Content report And its form";

2) V answers on control questions about laboratory work;V

answers on additional questions

Practical class No. 7. TCP/IP Stack Data Link Layer (Part 4).

Theoretical Part

At first at the entrance V network device user sees command lineuser regime type:

Switch>

The commands available at the user level are a subset of the commands available in privileged mode. These commands allow display on the screen information without change of settings network devices.

To get access To full set teams, necessary at first activate privileged mode.

Press ENTER to start.

Switch>

Switch> **enable**

Switch#

Switch# **disable**

Switch>

From here on, the output of the network device will be given in normal font, and the input user **bold** font.

The transition to this mode will be indicated by the appearance in the command line invitations V view sign **#.** From privileged level Can receive information O settings systems And get access To regime global configuration And others special modes configuration, including modes configuration interface, subinterface, lines, network devices, route maps, etc. To exit the IOS system, you need to type on the keyboard team exit (exit).

Switch> **exit**

Regardless from Togo, How are turning to To network device: through console terminal programs, connected through null modem To COM port network devices, or within the framework session protocol Telnet, device Can translate V one from modes. Us are interested next modes.

Custom mode — This mode viewing, V which user Maybe only browse certain information about the network device, But Not Maybe Nothing change. IN this mode invitation has view type Switch>.

Privileged mode- supports teams settings And testing, detailed check network devices, manipulation With configuration files and access V mode configuration. IN this mode invitation has view type Switch#.

Mode global configuration — implements powerful one-line teams, which decide tasks configuration. IN this mode invitation has view type Switch (config) # .

IOS recognizes commands in any mode by the first unique characters. pressing tabulations iOS myself will complement team to complete name.

When entering any name mode in the command line commands and question marks (**?**) Comments about the command are displayed on the screen. When you enter one character, the result will be list of all mode commands. Many screens of lines can be displayed on the screen, so Sometimes down screen will appear clue - More -. For continuations follows press enter or space.

Global configuration mode commands define the system behavior in in general. In addition, the global configuration mode commands include commands transition V other modes configuration, which are used For creation configurations, requiring multi-line teams. For entrance V mode global configuration is used team privileged regime configure. At input this teams follows indicate source teams configuration: terminal (terminal), memory (non-volatile) memory or file), network (server tftp (Trivial ftp
-simplified ftp) V networks). By default teams are introduced With terminal consoles. For example

Switch# configure terminal

Switch(config)#(commands)

Switch(config)# exit

Switch#

Teams For activation private species configurations should precede teams global configuration. So For configurations interface, on opportunity which indicates invitation Switch (config-if)#, at first is introduced global team For definitions interface type And numbers his port:

Switch# **conf t**

Switch(config)# **interface** ***type port***

Switch(config-if)# ***(commands)***

Switch(config-if)# **exit**

Switch(config)# **exit**

For restrictions access To system passwords are used. Team **line console**
sets password on entrance on terminal consoles:

Switch (config)# **line console 0**

Switch (config -line)# **login**

Switch (config-line)# **password Cisco**

Team **line vty 0 4** sets password protection on entrance ByTelnet protocol:

Switch (config)# **line vty 0 4**

Switch (config-line)# **login**
Switch (config-line)# **password Cisco**
Team **enable password** limits access Toprivileged regime :

Switch#conf t
Switch(config)# enable password

passwordNext

Ctrl-Z
Switch# **ex**
…
Press RETURN to get started

Switch> **en**

Password: **password**
Switch#
Here password **password** - subsequence Latin symbols.

For installations on network interface IP addresses is used team **:**
Router(config-if)# **ip address** [ip - address] [subnet-mask] ,Router(config-if)#no shut

Team no shut (reduction no shutdown) is used For Togo, to would interface was active (without this teams Maybe arbitrary temporary disabling the interface). Reverse team - shut, will turn off interface.

Important have opportunity control correctness functioning And statesnetwork devices V any moment time. For this serve commands:

Team	Description
show version	Outputs on screen data O configurations hardwaresystemparts , software versions, names And sources configuration files And loaded images
show running-conf ig	Shows content active configurations
show interfaces	Shows data about everyone interfaces on device
show protocols	Outputs data O protocols third network level.

Table 1. Show command

Cisco Discovery Protocol (CDP)

CDP allows devices exchange basic configuration information. CDP will work without settings what no be protocol. By by default, CDP included on everyone interfaces. CDP works on second (channel)

level of the OSI model. Therefore, CDP is not a routable protocol and operates only With directly connected devices. Protocol CDP connects physical Wednesday transmissions data more low level With protocols more high network level. That's why devices, supporting different protocols third level, can learn Friend friend.

When the device starts, the CDP protocol starts automatically. After that, it can automatically detect neighboring devices that are also running protocol CDP. Among found devices will be Not only those, which are working With protocol IP.

CDP allows to administrators have access To data O friend network device, To to whom There is direct compound.

For conclusion information O neighboring devices, discovered By protocol CDP, is used family teams **show cdp.** It outputs next data By to everyone port And to everyone connected To him device: Identifiers devices, list addresses, identifier port, scroll functional opportunities, hardware platform devices.

Teams ping And traceroute

For diagnostics possibilities establishments connections V networks are used protocols type request-response or protocol echo packets. Results robots such protocol can help V assessment reliability paths To to another device, quantities delays V in general And between intermediate devices. For Togo to such the team worked, it is necessary that not only local network device knew, how to get to the destination, but also so that the device at the destination knows how get there to source.

Team ping sends ICMP (Internet Control Message Protocol) echo packets For connection verification. In the example below, the transit time of one echo- the packet has exceeded the specified value, as indicated by the dot (**.**) in the output information, and four package passed successfully, O how speaks exclamatory sign (!).

```
Switch> ping 172.16.101.1
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:
. !!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms
```

Symbol	Meaning
!	Successful reception echo response
.	Exceeded time expectations
U	Paragraph appointments out of reach
C	Overload networks
I	Execution teams interrupted administrator
?	Unknown type package

&	Plastic bag exceeded meaning parameter time life TTL package

Table 2. Results teams ping

The traceroute command shows the addresses of intermediate interfaces (hops) along the path. packages V paragraph appointments.

Switch> **traceroute 172.16.101.1**

Extended version teams ping supported only V privileged mode. To enter the advanced mode, you need to enter the prompt line Extended commands enter letter "y" (Yes)

Team in mode dialogue interrogates values parameters. Important note, What this team allows, being on one device, check connection between network interfaces on others devices.

Router# **ping**
Protocol [ip]:
Target IP address: **2.2.2.2**
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands[n]: **y**
Source address: **1.1.1.1**
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data [no]:
Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes[n]:

Team telnet

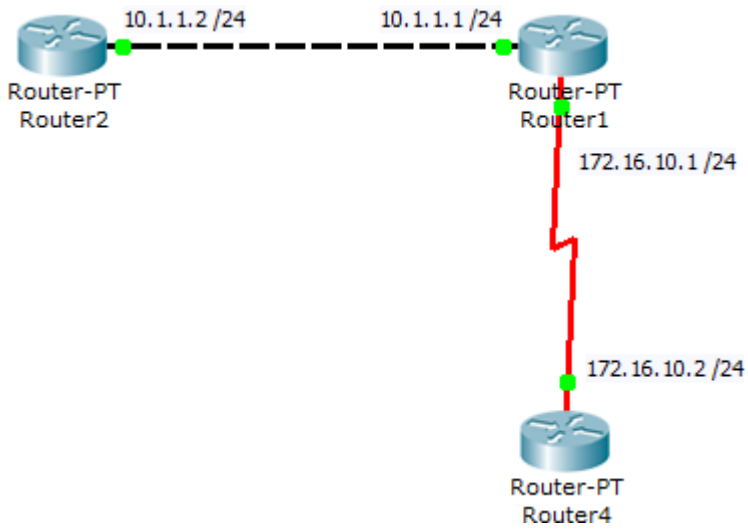
Virtual Protocol terminal telnet, incoming V compound protocols TCP/IP, allows you to establish a connection between the telnet client network device and the network telnet server device, which provides the ability to work in virtual mode terminal. Telnet is used for remote management of network device or to check application-level connectivity. Telnet connection established successfully allows you to control the remote device as if you were behind it console. Network devices Cisco capable support simultaneously to five input sessions protocol Telnet.

Practical Part

With **connection With network device Cisco**

Create the topology shown in the figure in Packet Tracer using The default router model is Generic. Name the devices as you see them. on drawing 1: Router1, Router2 And Router4.

Fig. 1



Black line means Ethernet compound. Red means consistent compound. For creation sequential connections we choose consistent point-to-point connection (serial cable). Select the second device. Decide which one router will fulfill functions DCE devices. This device asks synchronization. IN simulator For him will necessary define frequency synchronization.

Save topology.

Introduction With network device Cisco.

1. To select the Router1 network device, click on the icon in the program workspace.image needed. It will open window settings network devices. Here let's choose tab CLI For management device.

2. IN in the middle screen Network devices Router1 You you will

seeContinue with configuration dialog? [yes/no]:

Enter: “no” And click key <Enter>.You you

will see

Router>

You are now connected to the network device and are at the command prompt. user mode . Here "Router" is the name of the network device, and ">" means that you are you located? V mode user.

3. Now enter team enable, to get there V privileged mode.Router> **enable**

Router#

4. To return V mode user, Just print disable. From regimeuser введіте logout or exit, to leave network device.

Router#

disable

Router>

Router> **exit**

Router con0 is now available

Press RETURN to get started

Main teams network devices

1. Log in network device Router1

Router>

2. We we want see list everyone available teams V this mode. Enterteam, which is used For viewing everyone available commands:

Router> **?**

Key Enter press Not necessary.

3. Now log in V privileged modeRouter>enable

Router#

4. Browse list available teams V privileged modeRouter#?

5. Let's move on V mode

configurationsRouter#config terminal

Router(config)#

6. *Name hosta* network devices is used For local identification. When you log into a network device, you see *Host name* before the mode **symbol** (">" or "#"). This is the name can be used to determine the location. Install "Router1" as Name yours network devices.

Router(config)# **hostname Router1**

Router1(config)#

7. Password access allows to you control access V privileged mode. This Very important password, That's why What V privileged mode Can bring in configuration changes. Set a password access "password".

Router1(config)#enable password password

8. Let's test this password. Log out of the network device and try come in V privileged mode.

Router1>en

Password:*****

Router1#

Here are the signs: ***** - This your input password. These signs on screen Not are visible.

Main Show teams.

Go to V user mode team disable. Enter team For view all available show teams.

Router1> **show ?**

1. Team show version is used For receipt platform type network device, operating system version, operating system image file name, time work systems, volume memory, quantity interfaces And configuration register.

2. You can see the clock

Router1> **show clock**

3. In flash memory network devices is preserved image file operating room systems Cisco IOS. Unlike RAM, real flash devices memory saves image file even at failure nutrition.

Router1> **show flash**

4. X network devices By default saves 10 latest introduced teams

Router1> **show history**

5. Two teams will allow to you return To teams, introduced previously. Click onarrow up or <ctrl> P.

6. Two teams will allow to you go to To next team, saved V buffer.Click on arrow down or <ctrl> N

7. Can see list hosts And IP Addresses everyone their interfaces

Router1> **show hosts**

8. Next team will lead out detailed information O each interfaceRoute1r> **show interfaces**

9. Team Router1>

show sessions

will lead out information O each telnet sessions.

10. Team Router1>

show terminal

shows configuration parameters terminal.

11. Can see list everyone users connected To device byterminal lines

Router1> **show users**

12. Team Router1> **show**

controllers

shows state controllers interfaces.

13. Let's move on V privileged mode.

Router1> **en**

14. Enter the command For viewing everyone available show teams.

Router1# **show ?**

Privileged mode includes V myself All show teams user

regime And row new ones.

15. Let's look at the active configuration in the network device's memory. Required privileged mode. Active configuration automatically **Not** is preserved And will lost V in case of failure power supply.

Router1# **show running-config**

In the more line, press the space bar to view the next page. information.

16. Next team will allow to you see current state protocols third level.

Router# **show protocols**

Introduction V configuration interfaces.

We'll try understand, How include (to lift) interfaces network devices AndWhat necessary, to translate interface V state UP.

1. On network device Router1 let's go in V mode configurations

Router1# **conf t**

Router1 (config)#

2. Now we want tune Ethernet interface. For this we should come in Vmode configurations interface.

Router1(config)# **interface FastEthernet0/0**

Router1(config-if)#

3. Let's see All accessible V this mode teamsRouter1 (

config-if)# **?**

For exit V mode global configurations dial exit. Again log in Vmode configurations interface

Router1(config)# **int fa0/0**

We used abbreviated Name interface.

4. For each teams we can execute the opposing team, having placed before her word **no** . So the team

Router1(config-if)# **no shutdown**

includes this interface .

5. Let's add To interface description

Router1(config-if)# **description Ethernet interface on Router 1**

To see description this interface, go to privilegedmode And complete team show interface .

Router1(config-if)

#end Router1#show

interface

6. Now connect to **the Router 2 network device** and change its hostname.on **Router2**

Router# **conf t**

Router(config)# **hostname Router2**

Let's go in on FastEthernet 0 interface

.Router2(config)# **interface fa0/0**

Turn on interface .

Router2 (config-if)# **no shutdown**

Now that the interfaces on both ends of our Ethernet connection are enabled, screen will appear message O change interface states to active.

7. Let's move on to the configuration of serial interfaces. Let's go on Router1. Let's check, what device performs our router For consistent communication lines: end device DTE (data terminal equipment) or device connections DCE (data circuit)

Router 1# **show controllers S 2/0**

If we see - ..... DCE cable.....- , then our router is a device communication and it must set the synchronization frequency of the clock pulses used at transfer data. Frequency is taken from certain rows frequencies .

Router1#conf t Router1(

config)#int s2/0 Router1(

config-if)#clock rate ?Let's

choose frequency 64000

Router1(config-if)#clock rate 64000

And we raise interface

Router1(config-if)#no shut

8. Let's move on to router router4 And we'll give of the same name Name. Let's raise it on himserial2/0 interface.

Now that the interfaces at both ends of our serial connection areincluded on screen will appear message about the change states interface on active.

9. Let's check on each device, What configured us interfacesare in condition UP.

Router1# **sh int**

s2/0 Router1# **sh int**

e0/0 Router2# **sh int**

e0/0 Router4# **sh int**

s2/0

CDP

1. On router router1, let's introduce team For conclusion states everyone interfaces, on which works CDP.

router1#show cdp interface

We should see, What both interface raised and they send CDP packages.

```
FastEthernet0/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial2/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

2. Once we have verified that the network device is sending and receiving CDP updates, we We can use CDP to obtain information about directly connected devices. Enter team

router1# **show cdp neighbors**

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Router4      Ser 2/0          138            R       PT1000      Ser 2/0
Router2      Fas 0/0          142            R       PT1000      Fas 0/0
```

We done All Right. We see, What our router router1 connected With interface Fas 0/0 **(Port ID)** of router **(Capability)** router2 **(Device ID)** series 1000 **(Platform)** through interface Fas 0/0 **(Local Intrfce)** And With interface Ser 2/0 router router4 series 1000 through interface Ser 2/0.

3. On router1, enter the command for more detailed information about neighborsrouter1# **show cdp neighbors detail**

This team shows By alone device for once. She is used For display of network layer address information. Currently, this layer at us Not configured That's why field Entry address(es) empty. Team Also outputs information O versions IOS.

10. On router1, enter the command to find out information about the device "router4"

router1# **show cdp entry Router4**

This command gives the same information, as well as show cdp neighbor detail, But for onespecific devices. Remember that names hosts are sensitive To register.

11. On device router1 enter team, to see, How often router1sends neighbors updates CDP And How for a long time at neighbors They should be stored.

router1#show cdp

```
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

For savings stripes transmission low-speed devices CDP Can turn off

router1 (config)# **no cdp run**

and turn it back on for the entire device

router1 (config)# **cdp run**

12. Sometimes it is necessary to disable CDP for a specific interface, for example at his narrow strip transmission or V purposes security. On device router1, turn it off CDP on the interface FastEthernet 0/0.

router1 (config)# **interface fa0/0**

router1 (config-if)# **no cdp**

enablerouter1 (config)# **Ctrl-Z**

router1# **show cdp interface**

IN received conclusion You Not you will see information about FastEthernet 0/0.

Setting up IP addresses interfaces

1. Let's connect To device **Router1** and we will install IP address Ethernet interface

Router1(config)# **interface fa0/0**

Router1(config-if)# **ip address 10.1.1.1 255.255.255.0**

2. Now let's appoint interface S0/0 IP address 172.16.10.1 255.255.255.0, without leaving configurations interface

Router1(config-if)# **in s0**

Router1(config-if)# **ip ad 172.16.10.1 255.255.255.0**

Let us note, What on consistent compound dot dot Always stands out wholesubnet.

3. Let's switch over To device **Router2** And let's appoint interface FastEthernet 0/0 IP address 10.1.1.2 255.255.255.0

Router2(config)# **interface fa0/0**

Router2(config-if)# **ip address 10.1.1.2 255.255.255.0**

4. Let's connect To device **Router4** And let's install IP address Ethernet interface Serial 2/0.

Router4(config-if)# **ip address 172.16.10.2 255.255.255.0**

5. On each device take a look yours active configuration And make sure thatthere appeared appointed IP addresses.

Router1# **show running-config** Router2# **show running-config**Router3# **show running-config**

6. Look at the detailed IP information for each interface and make sure that configured interfaces have migrated V state UP

Router1# **show IP interface** Router2# **show IP interface** Router4# **show IP interface**

7. Brief information Can get with the show ip interface brief command , for example

Router1# **show IP in bri**

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	10.1.1.1	YES manual up	up
FastEthernet1/0	unassigned	YES manual up	down
Serial2/0	172.16.10.1	YES manual up	up

Router2# **show IP in bri**

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.1.1.2        YES manual up                    up

FastEthernet1/0        unassigned      YES manual up                    down

Serial2/0              unassigned      YES manual administratively down down
```

Router4# **show IP in bri**

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual administratively down down

FastEthernet1/0        unassigned      YES manual administratively down down

Serial2/0              172.16.10.2     YES manual up                    up
```

8. Let's connect To device **Router1.** You should successfully ping directly connected FastEthernet 0/0 interface on device Router2.

Router1# **ping 10.1.1.2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms
```

Let's try ping interface Serial 2/0 on device Router4Router1# **ping 172.16.10.2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
```

Successfully.

9. Let's come back on Router2. You should successfully ping address 10.1.1.1 directly connected FastEthernet 0/0 interface on device Router1. Let's come back on Router4. You should successfully пропінгувати address 172.16.10.1 directly connected interface Serial 2/0 on device Router1. Let's try ping interface FastEthernet 0/0 on the device Router1.

Router4# **ping 10.1.1.1**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Failure. Let's try ping address 10.1.1.2 FastEthernet 0/0 interface onRouter2 device.

Failure.

10. Let's get back to Router2. Let's try ping address 172.16.10.1 interface

Serial 2/0 on Router1. Failed. Let's try pinging 172.16.10.2.interface Serial 2/0 on device Router4. Failure.

The failures occurred because we did not configure the routersrouting.

11. Come in on Router1 device **.** Determine paths passages packages onRouter2

Router1# **traceroute 10.1.1.2**

And Router4

Router1# **traceroute 172.16.10.2**

You should see By alone hop.

12. Do it team extended ping from addresses 10.1.1.2 To address 172.16.10.2Router1# **ping**

…

Target IP address: **172.16.10.2**

…

Extended commands [n]: **y**

Source address: **10.1.1.2**

…

Telnet

Be Be careful: simulator has limited support telnet.

1. Log in to the Router1 device. We need the network device accepted telnet sessions and was password protected. Each so-called line in network device potentially represents an active telnet session that device Maybe support. Our network devices support to 5 lines, appointed on virtual terminals vty. We we use all 5 lines

Router1(config)# **line vty 0 4**

Router1 (config-line)#

2. Now we will inform network device, what do we need will be needed password entrance Vsystem.

Router1(config-line)#l **ogin**

Router1(config-line)# **password password**

3. Log in on Router2 device And let's install telnet connection With deviceRouter1. For this We we use IP address his interface FastEthernet 0/0

Router2# **telnet 10.1.1.1**

4. We will see request enter password. Enter your password password And click <enter>.Notice that the network device name has changed to “Router1” because we installed telnet connection With Router1. Team

Router1> **show user**

```
* 67 vty 0                 idle                 00:00:00 10.1.1.2
```

will show, What compound implemented from addresses 10.1.1.2 devices router2 .

Now press control-shift-6 simultaneously for a second, then release and press x key immediately . Notice that the network device name has changed back to “Router2”. Now you again device Router2.

Router 1> **< Control > + < Shift > + <6> Then < x >**
Router2#

6. Enter the show sessions command. This will allow you to see all active telnet-sessions. To resume a telnet session, specify the session number you want resume (V ours case There is only one With number 1) And enter the command resume 1.

Router2# **Show sessions**

```
Conn Host                Address             Byte  Idle Conn Name
*  1 10.1.1.1            10.1.1.1               0     1 10.1.1.1
```

Router2# **resume 1**
Router1#

7. Now Name hosta again changed on Router1. Click combination control-shift-6 And key x, to return back on Router2.

Router1# **<Control> + <Shift> + <6> Then <x>**
Router2#

8. Close the session

Router2#disconnect 1

```
Closing connection to 10.1.1.1 [confirm]
```

Save project V in general And configuration each router in separateness (Vtext file).

Control questions

1. Which There is modes input teams V command line?
2. How switch between modes input teams V command line?
3. Which one? role plays key tabulations at input teams?
4. How to enter global configuration modes, activate private viewconfigurations And go out from these modes?
5. How navigate V previously introduced teams And repeat their?
6. What such CDP, For what He serves And How them use ?.
7. Which one? information returns the command ping?
8. Can whether being on one device in pairs ping All devices Vnetworks?
9. For what serves team traceroute?
10. For what serves team protocol telnet?
11. How ask Name host?
12. Which one? information Can look teams show V usermode?
13. Which one? information Can look teams show V privilegedmode, but it is forbidden look V user mode?
14. What the device can act as serial routerlines connections?

15. On what device at sequential connection is possible install frequency synchronization?
16. How raise interface And define it state?
17. How appoint IP address on interface And make sure, What He appointed?
18. Why can Not pass pings between devices?19. How suspend And resume telnet session? 20. How to close telnet compound?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute V PacketTracer practical Part.
4. Get it option And complete V PacketTracer exercise For independent work
5. Submit the result of the assignment to the teacher for independent work. work. Show your router configuration files. Showto him, What computers ping according to table 4.
6. Demonstrate work telnet.
7. Make out report. Content report Look below.
8. Protect report.

Exercise For independent work

1. Get it mine option

Option	i11-i31	i12-i21	i22-i32
1, 9	serial	Serial	serial
2, 10	serial	Serial	Ethernet
3, 11	serial	Ethernet	serial
4, 12	serial	Ethernet	Ethernet
5, 13	Ethernet	Serial	serial
6, 14	Ethernet	Serial	Ethernet
7, 15	Ethernet	Ethernet	serial
8, 16	Ethernet	Ethernet	Ethernet

Table 3.

Select the appropriate devices in the designer and create the topology shownon drawing 2. Ourselves appoint devices names. Raise it on each device interfaces used. Check their status. On each device, using teams CDP show cdp neighbors, receive information O neighboring devices. Save screenshots teams CDP.

2. Assign interfaces addresses, according to option (v=1-16) from table 3. All masks equal 255.255.255.0. For example, For options 7 (v=7) we have

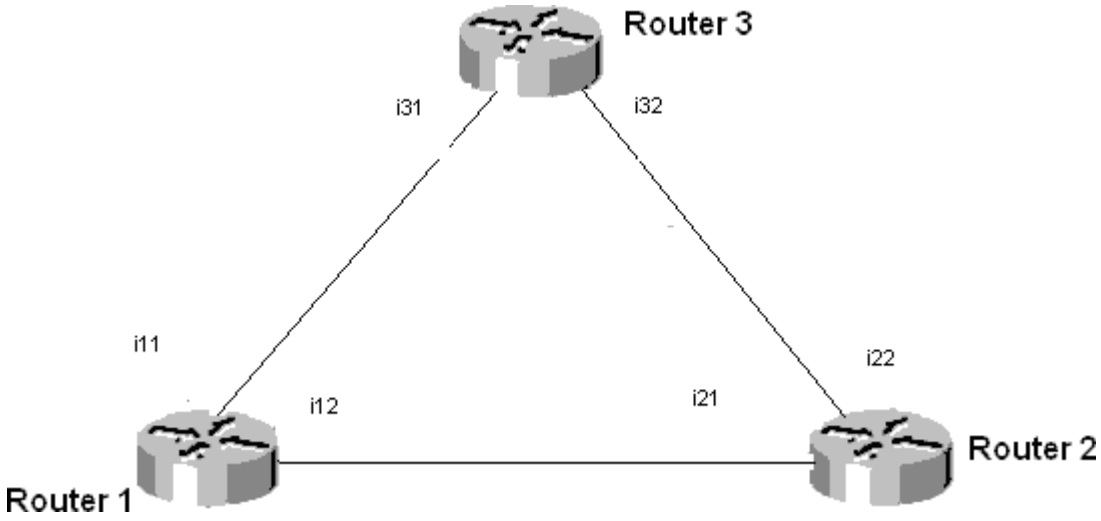
Device	Interface	Address
Router1	i11	**7.1.1.2**

Router3	i31	**7.1.1.2**
Router1	i12	**7.1.2.1**
Router2	i21	**7.1.2.2**
Router2	i22	**7.1.3.1**
Router3	i32	**7.1.3.2**

Table 4.

Option	i11, i31	i12, i21	i22, i32
1	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
2	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
3	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
4	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
5	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
6	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
7	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
8	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
9	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.2.1, v.1.2.2
10	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
11	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
12	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
13	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
14	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
15	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
16	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2

Table 5.



Rice 2.

3. Check it out, What addresses appointed. On each device complete team showIP interface brief . Save screenshots.

4. If made All Right You you can ping from any computercertain (But Not All) interface addresses others computers.

From\To	I11	I12	I21	I22	I31	I32

Router1	Yes	Yes	Yes *	No	Yes *	No
Router2	No	Yes	Yes	Yes	No	Yes *
Router3	Yes	No	No	Yes	Yes	Yes

Table 6.

Do it This. Save screenshots For pings connections, marked V Table 4 familiar *.

5. Run an extended ping on Router1. Save three screenshots of the pings: from i12 To i21, from i11 To i31 And from i22 To i32.

6. Set up on Router1 Telnet. Ask password.

7. Go to Router2. Telnet to Router1. Run the show command. user. Pause the session. Resume the session. Kill sessions. Save a screenshot. consoles Router2.

8. Save topology.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshot topology from drawing 1
2. Configurations three routers from .txt files, created at executionpractical parts.
3 Screenshot topology from drawing 2
4. All screenshots, specified V **Task For independent work**
5. Configurations three routers from .txt files.

Practical class No. 8. TCP/IP Stack Data Link Layer (Part 5).

ARP (Address Resolution Protocol)

When the sender has determined the IP address of the receiver, it looks in its ARP table. to find out the MAC address of the receiver. If the source detects that the MAC and IP addresses the receiver is present in the ARP table, it establishes a correspondence between them and uses his during encapsulation IP packets in channel frames level. MAC addresses frames channel level are taken from ARP tables. After this frame By physical channel is being sent from sender To to the addressee.

If the sender has an IP packet for the recipient with the IP address of the ADR and this address is not in the ARP table, then the sender sends an ARP broadcast over the network the following request: Tell the MAC address of the network interface with the IP address ADR. The request is accepted by all network devices in the network segment, and only the device, having the IP address of the ADR, responds to it by sending MAC information to the sender address his own network interface With IP address ADR. Sender writes down couple
<MAS address, IP address ADR > V my ARP table.

Routing

Protocols routing - This rules, By which is being carried out exchange information O paths transmissions packages between routers. Protocols characterized by time convergence, losses and scalability. At present time is used some protocols routing. Every protocol has strong And weak sides.

One of the main tasks of a router is to determine the best path to to the specified addressee. The router determines paths (routes) to the addressees or from static configuration entered by the administrator, or dynamically based on route information, received from others routers. Routers exchange route information With help protocols routing. The router stores routing tables in RAM. Route table This is a list of the best known available routes. The router uses this table for deciding where to route a packet. To view the routing table You should use the show ip route command. Even if on some router X Not were asked none teams routing, Then He All equals builds table routes For directly connected To him networks, For example:

```
. . .
C192.168.4.0/24 is directly connected, Ethernet0
  10.0.0.0/16 is subnetted, 3 subnets
C10.3.0.0 is directly connected, Serial0
C10.4.0.0 is directly connected, Serial1
```

C10.5.0.0 is directly connected, Ethernet1

Route on directly connected networks is displayed on interface router, To to whom they attached. Here /24 means mask 255.255. 255.0, A /16 - 255.255.0.0.

Table routes displays network prefixes (addresses networks) on weekend interfaces. When X receives plastic bag, designed For 192.168.4.46, He is looking for prefix 192.168.4.0/24 in the route table. According to the table, the packet will be directed to interface Ethernet0. If X will receive a package For 10.3.21.5, He will direct his on Serial0.

This table shows four route For directly connected networks. They have the label C. Router X drops all packets destined for networks not listed in the route table. To route packets to other destinations necessary V turn on the table additional routes. New routes can be added two methods:

Static routing - administrator manually defines routes To networks appointments.

Dynamic routing – routers follow rules defined by routing protocols for exchanging route information and selecting the best one paths.

Static routes Not are changing ourselves router. Dynamic routes are changing ourselves router automatically at receipt information O change routes from neighboring routers. Static Routing consumes few computing resources and is useful in networks that are not have several paths To to the addressee appointments. If from router To router There is only one path, That often use static routing.

For configurations static routing V routers Cisco use two versions teams IP route

First version

IP route DestinationNetworkAddress MaskNetworkPurpose Interface

Team indicates router, What All packages, intended For DestinationNetworkAddress-DestinationNetworkMask follows guide on mine interface Interface. If the interface Interface - type Ethernet, That physical (MAC) addresses outgoing packages will be broadcast (Why?).

Second version

IP route DestinationNetworkAddress MaskNetworkPurpose Address

Team indicates router, What All packages, intended For DestinationNetworkAddress-DestinationNetworkMask should be directed to the interface that you have. from which the IP address is reachable. Typically, the Address is the address of the next hop paths To DestinationNetworkAddress. Day off interface And physical addresses outgoing packets are determined by the router according to its ARP tables based on the IP address Address. For example

IP route 10.6.0.0 255.255.0.0 Serial1 (1)
IP route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

The first example maps the network prefix 10.6.0.0/16 to the local interface router Serial1. The following example maps the network prefix 10.7.0.0/16 to IPaddress 10.4.0.2 next hop By paths To 10.7.0.0/16. Both these teams will add static routes V table routing (label S):

S 10.6.0.0 via Serial1
S 10.7.0.0 [1/0] via 10.4.0.2

When interface falls, All static routes, displayed on this interface, are deleted from tables routes. If router Not Maybe morefind the address of the next hop along the path to the address specified in the static route, then route excluded from tables.

Note that for Ethernet type networks it is recommended to always use form (2) teams IP route. Ethernet interface on router, How rule, connected With several Ethernet interfaces of other devices on the network. Specifying in the ip route command IP addresses will allow router Right form physical address weekend package By your own ARP tables.

Routing By default.

It is not necessary for every router to maintain routes ko to everyone possible networks appointments. Instead of this router stores route Bydefault or gateway last shelters (last resort). Routes By default used when the router cannot map the destination network line V table routes. Router must use route By default for sending packets to another router. Next router will have a route to this destination network or have its default route to to the third router And etc. IN final account, plastic bag will routed on router, having route to the network appointments.

Route By default Maybe be statically introduced administrator or dynamically received from protocol routing.

Since all IP addresses belong to the network 0.0.0.0 with a mask of 0.0.0.0, then in the simplest if necessary use team

IP route 0.0.0.0 0.0.0.0 [address next hop | day off interface]

Manually setting the default route on each router is suitable for simple networks. IN complex networks necessary organize dynamic exchange routes By default.

Interface loop

On network devices Can create network interfaces Not related With real channels for data transmission and assign IP addresses with masks to them. Such interfaces they call loops (loopback). Loops useful for phased design

networks. If you connect to any real network interface of the router in the future will connected subnet, That V beginning on router is being created loopback, is configurable V plan interactions With the rest plots networks And only then is replaced by the actual interface. The loop interface appears after the interface command. loopbackN or abbreviated int lN, where N is a non-negative integer – loop number. For example

Router(conf)> **int l0 1.1.1.1 255.0.0.0**

Team trace

The trace command is an ideal way to find out where messages are being sent. data on the network. This command uses the same ICMP protocol technology as the command ping, but instead of checking the end-to-end connection between the sender and the recipient, it verifies every step along the way. The trace command uses the router's ability generate messages about error at excess package his own established Time To Live (TTL) This command sends several packets and outputs on the screen the data on the round trip time for each of them. The advantage teams trace consists of V volume, What she shows another one reached router on the way to the destination. This is a very powerful tool for localization.refusals on paths from sender To to the recipient. Options answers utilities trace

Symbol	Meaning
!H	Probing plastic bag was accepted router, But Not redirected, Whatusually It happens because of list access
P	Protocol out of reach
N	Net out of reach
U	Port out of reach
*	Exceeding borders expectations

Table 1.

Practical Part

Download topology And configuration from practical parts previous work.

ARP

1. Join us To router Router1 With And take a look his ARP tableRouter1# **show arp**

It contains only one line about the MAC address of its Ethernet interface with IP address

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1               -   00D0.58B7.80A1  ARPA   FastEthernet0/0
```

10.1.1.1.

2. Connect to router2 and look at its ARP table. It contains only one line about the MAC address of its Ethernet interface with IP address 10.1.1.2

3. Ping Ethernet interface router Router1Router2#ping 10.1.1.1

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.2                -   00D0.BA88.005C  ARPA   FastEthernet0/0
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1                0   00D0.58B7.80A1  ARPA   FastEthernet0/0
Internet  10.1.1.2                -   00D0.BA88.005C  ARPA   FastEthernet0/0
```

4. Look at your ARP table again. It already contains two lines. recording O Ethernet MAC address interface Router1 With IP address 10.1.1.1.

5. Connect to router1 and look at its ARP table. contains already two lines

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1                -   00D0.58B7.80A1  ARPA   FastEthernet0/0
Internet  10.1.1.2                2   00D0.BA88.005C  ARPA   FastEthernet0/0
```

Appeared recording O MAC address Ethernet interface router Router2 With IP address 10.1.1.2. Why, we didn't send any IP packets from Router1? Because Router1 For answer on ping from Router2 must was know O MAC address Ethernet interface Router2 With IP address 10.1.1.2, And He formed ARP plastic bag For his receipt.

Static routes

IN last work We Not could from routers Router2 and Router4 pingsome interfaces because of absence routing. We'll fix it position.

1. Join us To router router2. We Not could ping addresses 172.16.10.1 And 172.16.10.2. Take a look table routes

Router2# **show IP route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
```

We see directly annexed networks. No route To networks 172.16.10.0/24. Let's add a route to the network 172.16.10.0/24 via the address 10.1.1.1 of the nearest hop on the way to this networks:

Router2(config)# **ip route 172.16.10.0 255.255.255.0 10.1.1.1**

Here And further 172.16.10.0/24 - This abbreviated recording - definition subnets 172.16.10.0 with mask 255.255.255.0. The mask 255.255.255.0 contains 24 units, which is is designated /24.

2. Successfully Let's ping the serial interface of

Router1Router2# **ping 172.16.10.1**

Again take a look table routes

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.10.0 [1/0] via 10.1.1.1
```

3. But us Not will succeed ping serial interface Router4.

Router2# **ping 172.16.10.2**

Why? Because, What ICMP ping packets not know, How them return back from Router4,So How on Router4 Not registered routes.

4. Join us To router router4. Take a look table routesRouter4# **show IP route**

No route To networks 10.1.1.0/24. Let's add route To networks 10.1.1.0/24 through

```
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

address172.16.10.1 nearest hop on paths To this networks:

Router4(config)# **ip route 10.1.1.0 255.255.255.0 172.16.10.1**

Again take a look table routes.

```
     10.0.0.0/24 is subnetted, 1 subnets
S       10.1.1.0 [1/0] via 172.16.10.1
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

5. That's all now network interfaces online pinged from each network devices.Check it out This.

Routing By default.

Network devices Router2 and Router4 have only one output to the external world: through interfaces with addresses 10.1.1.1 and 172.16.10.1, respectively. Therefore, it is possible Not determine on which subnets We we route packages And use routing By default.

1. In the beginning let's delete old routes.

Router2(config)# **no IP route 172.16.10.0 255.255.255.0 10.1.1.1**

Router4(config)# **no IP route 10.1.1.0 255.255.255.0 172.16.10.1**

2. AND let's appoint routes By default.

Router2(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.1**

Router4(config)# **ip route 0.0.0.0 0.0.0.0**

172.16.10.1

3. Take a look table routes on everyone devices.Router2#

sh IP route

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
```

Router4# **sh IP route**

```
Gateway of last resort is 172.16.10.1 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
S*   0.0.0.0/0 [1/0] via 172.16.10.1
```

4. All network interfaces V networks ping from each network devices.Check it out This.

Loopback

1. Let's define interface loop on device Router4

Router4(conf)# **int loopback 0 1.1.1.1 255.255.255.0**

2. Let's write it down on device Router1 route on net loops

Router1(conf)# **IP route 1.1.1.0 255.255.255.0 172.16.10.2**

3. Let's join To device Router2 And let's ping created loopRouter2# **ping 1.1.1.1**

Save the project as a whole and the configuration of each router inseparate file.

Control questions

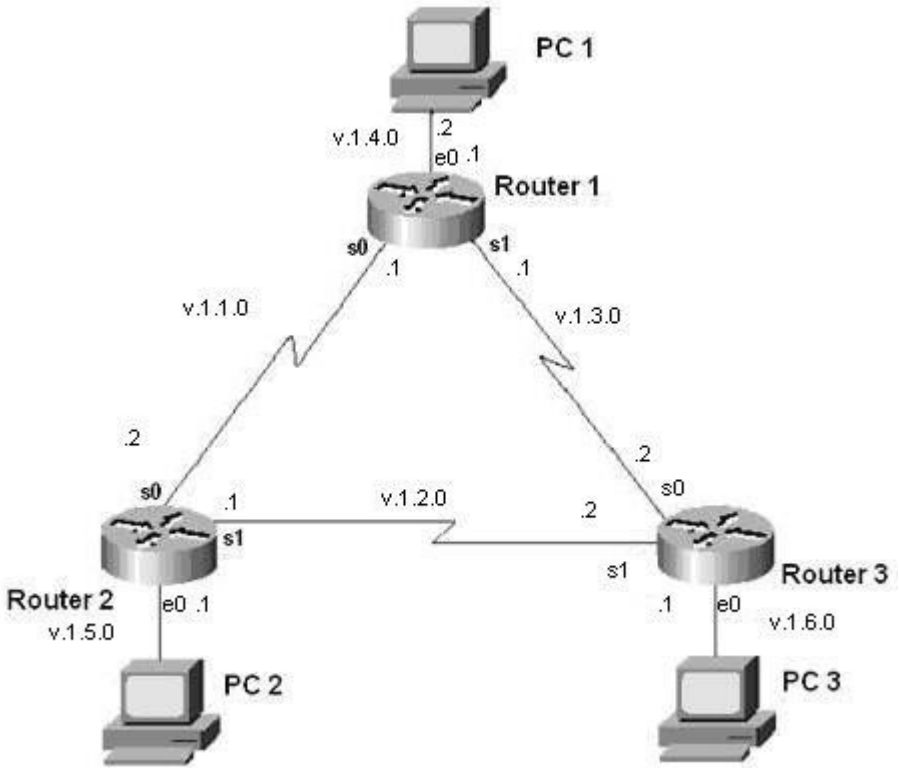
1. How sender recognizes MAC address recipient?
2. How look ARP table?
3. When V ARP table appear new lines?
4. What's happened table routes?
5. If administrator Not tuned none routes, That What she willcontain?
6. How static routing is different from dynamic?
7. Which two forms tasks static routing You do you know?
8. How V team routing is determined net destination?
9. Why For networks type Ethernet recommended Always use form (2)teams routing?
10. Explain values fields V teams routing.
11. is it recommended to use an address as **the Address field?** nexthop By paths to the network appointments.
12. When is used routing By default?
13. When use interface loop?
14. How works team tracings?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute V Packet Tracer practical Part.
4. Get it option And complete V Packet Tracer task For independentwork.
5. Show your teacher the results of completing points 8 and 9 of the assignment for independent work.
6. Make out report. Content report Look below.
7. Protect report .

Exercise For independent work

1. Build V Packet Tracer topology, presented on drawing. Usenecessary routers.



Drawing 1

IN ours networks six subnets. You you see, What every the router is connected to threesubnets.

2. On each router raise used interfaces And lookneighbors team show cdp neighbors. To do screenshots.

3. Assign interfaces networks addresses according to drawing 1 And table 1 V which v - This number options. All masks 255.255.255.0. Don't forget appoint gateways By default For computers according to the table 1..

	v.1.1.0	v.1.2.0	v.1.3.0	v.1.4.0	v.1.5.0	v.1.6.0
Router1	S0:v.1.1.1		S1:v.1.3.1	E 0 :v.1.4.1		
Router2	S0:v.1.1.2	S1:v.1.2.1			E 0 :v.1.5.1	
Router3		S0:v.1.2.2	S1:v.1.3.2			E 0 :v.1.6.1
PC1				E 0 :v.1.4.2		
PC2					E 0 :v.1.5.2	
PC3						E 0 :v.1.6.2

Table 1

4. Check it out fact appointments addresses by way execution on each routershow running-config and show ip interface brief commands. For computers, use team ipconfig.

5. Check the correctness of the address assignment by performing the following on each router teams ping To direct to neighbors. For example, on routerRouter1 complete

Router1#ping v.1.1.2

Router1#ping v.1.3.2

Router1#ping v.1.4.2

6. Let's put it before by yourself task connect between by yourself computers PC1, PC2 And PC3.To do this, we will configure static routing on the routers. We'll assign routes to remote Ethernet networks to each router. To solve thisthe task of routing packets to remote serial networks connections Not necessary.

U each router There is By two on deleted Ethernet networks. Total necessaryprescribe six static routes.

To reach a remote Ethernet network v.1.5.0/24 from router1, packetsCan direct on IP address 1.1.1.2 nearest external interface on paths to this one net.

This will do team

router1(config)#ip route 1.1.5.0 255.255.255.0 1.1.1.2

Ask rest five teams routing.

7. On each router look table routing team showIP route. Do screenshots.

8.On each router do it screenshots extended pingsA) on router router1 from

PC2 to PC3

b) on the router router2 from PC1 to PC3V)

on router router3 from PC1 To PC2

For example, the result of an extended ping on router1 from PC2 to PC3For For options 1 (v=1) has view

```
router1#ping
Protocol [ip]:
Target IP address: 1.1.6.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:1.1.5.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

9. On each computer, take screenshots of the execution of trace commands. tracert of other computers. There are six screenshots in total. For example, a tracert from PC1 toPC2 For options 1 (v=1)

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.1.2 20 msec 16 msec 16 msec
 3 1.1.5.2 20 msec 16 msec *
```

10. Save project.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshot topology created at execution practical parts .
2. Configurations three routers from .txt files, created at executionpractical parts.
3. Screenshot topology from drawing 1 With addresses your own version
4. Table 2 With addresses his own options
5. Configurations three routers from .txt files, created at executiontasks For independent work.
6. All screenshots, specified V task For independent work

Practical class No. 9. TCP/IP Stack Data Link Layer (Part 6).

Theoretical Part

Static routing is not suitable for large, complex networks because Networks typically include redundant links, multiple protocols, and mixed topologies. Routers V complex networks should fast adapt To changes topology And choose best route from many candidates.

IP networks have hierarchical structure. WITH points vision routing net is being considered How totality autonomous systems. IN autonomous subsystems large networks For routing on rest autonomous systems wide are used routes By default.

Dynamic routing can be accomplished using one and more protocols. These protocols often are grouped according to Togo, Where They are used. Protocols for operation within autonomous systems are called internal interior gateway protocols (IGP), and protocols for working between autonomous systems they call external protocols gateways (exterior gateway IGP protocols (EGP) include RIP, RIP v2, IGRP, EIGRP, OSPF, and IS-IS. EGP3 and BGP4 protocols are related to EGP. All these protocols can be divided into two class: distance vector protocols And protocols states connections.

Routers use metrics to evaluate or measure routes. When There are many routes from the router to the destination network, and they all use one routing protocol, then the route with the lowest metric is considered as best. If different routing protocols are used, then for route selection is used administrative distances, which are appointed routes operating room system router.

RIP uses hop count as its metric. EIGRP uses complex combination factors, including strip transmission channel And his reliability.

The results of the routing protocols are entered into the route table, which is constantly changing as the network situation changes. Let's consider a typical line in route table, related To dynamic routing

R 192.168.14.0/24 [120/3] via 10.3.0.1 00:00:06 Serial0

Here R defines the routing protocol. So R stands for RIP, O stands for OSPF, and so on. Recording [120/3] means, this route has administrative distance 120 and metric

3. These numbers router uses For choice route. Element 00:00:06 determines the time when this row was updated. Serial0 is local interface, through which the router will forward packets to the network 192.168.14.0/24 via the address 10.3.0.1.

For Togo to dynamic protocols routing exchanged information O static routes, follows realize additional configuration.

Distance vector routing

This routing is based on the Bellman-Ford algorithm. Through certain moments time router transmits neighboring routers all my table routing. Such simple protocols How RIP And IGRP Just distribute information O tables routes through All interfaces router V broadcast mode without clarifications precise addressesspecific neighboring router.

Neighboring router, receiving broadcasting, compares information with its current route table. Routes to new networks are added to it or routes to known networks with the best metrics. Non-existent ones are removed.routes. Router adds their own values To metrics received routes. New table routing again is spreading By neighboring routers (cm. Fig. 1).

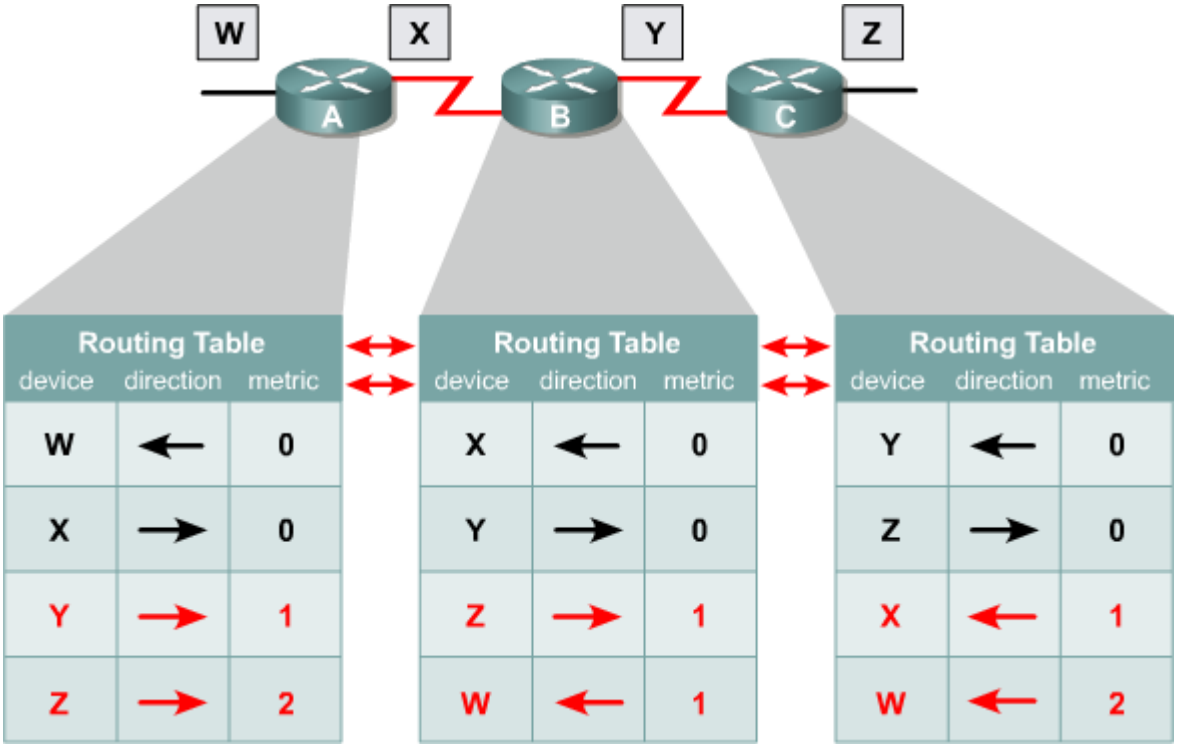


Fig. 1. Distance vector routing.

Protocols states connections

These protocols offer better scalability. and convergence by comparison with distance vector protocols. The protocol is based on Dijkstra's algorithm, which often they call algorithm "the shortest path - first" (shortest path first (SPF)). The most typical representative is the OSPF (Open Shortest Path First) protocol. First).

Router beret V consideration state connections interfaces others routers V networks. Router builds a complete database of all states connections V his own areas, That There is has enough information For creation his own

displays networks. Every router then on one's own performs SPF- algorithm on its own network mapping or link state database for determining the best path, which is entered into the route table. These paths to others networks form tree With top V in the form of local router.

Routers notify O condition their own connections to everyone routers V areas. Such a notice they call LSA (link-state advertisements).

IN difference from distance vector routers, routers states connections can to form special relationship with your own neighbors.

There is an initial influx of LSA packets to build the state database connections. Further route updates are performed only when the connection status changes or, If state Not changed V flow certain interval time. If the connection status has changed, That partial update is being forwarded immediately. It contains only states connections that have changed, but Not all table routes.

The administrator who is concerned with the use of communication lines finds these partial And rare updates effective alternative distance vector routing that broadcasts the entire routing table at regular intervals time.

Protocols states connections have more fast convergence And the best usage stripes transmission By comparison With distance vector protocols. They surpass distance vector protocols For networks any sizes, however have two main disadvantages: elevated requirements To computing power routers And complex administration.

Convergence.

This process simultaneously And joint, And individual. Routers They share information among themselves, but recalculate their tables independently. routing. For Togo to individual tables routing were accurate, all routers must have the same idea of topology networks. If routers Deal O topology networks, That has place their convergence. Fast convergence means fast recovery after connection breaks and other changes in the network. About routing protocols and the quality of network design are being judged main way By convergence.

When routers are located V process convergence, net receptive To routing problems. If some routers have determined that a certain connection absent, That other wrongly they think this connection present. If This happens, then the individual route table will be inconsistent, which can lead to discarding packages And loops routing.

Impossible, to All routers V networks simultaneously discovered changes V topology. IN dependencies from used protocol, Maybe pass many time Bye All processes routing V networks will converge. On This influence the following factors:

Distance V hops to points changes topology.
Number routers, using dynamic protocols.Bandwidth And loading channels
connections.
Loading routers .
Effect some factors Maybe be reduced at thorough design

netw
orks.

Configuration dynamic routing

There are two main methods used to configure dynamic routing: commands: router i network. Team router launches process routing And has form:

Router(config)# **router protocol [keyword]**

where Protocol is any of the routing protocols: RIP, IGRP, OSPF, etc., keyword – additional parameters.

Then necessary teams network:

Router (config -router)# **network network number [keyword]**

Where network number - identifies directly connected net, added to the routing process, keyword -additional parameters network- number allows the routing process to determine which interfaces will be taken participation in sending And reception update packages route information.

For viewing information O protocols routing is used team show IP protocol., which outputs values timers processes routing And network information related to routing. This information can used to identify a router suspected of supplying bad route information

Table contents IP routing output by the command show ip route. She contains records of all networks and subnets known to the router and indicates the methodreceipt this information.

Protocol RIP

Key protocol characteristics RIP:
routing on basis vectors distances;
metrics at choice paths to view quantities transitions (hops);maximum
permissible number of hops- 15;

By default packages updating route information are sent V modebroadcasting every 30 seconds.

Choice protocol RIP yak protocol routing is being carried out command:Router(config)#
router rip

Team network assigns IP network address which router hasdirect connection.

Router(config-router)# **network network number**

Process routing connects interfaces With corresponding addresses Andbegins processing packages V given networks.

IN shown on Fig. 2 example teams network 1.0.0.0 And network 2.0.0.0 askdirectly connected to router Cisco A networks.

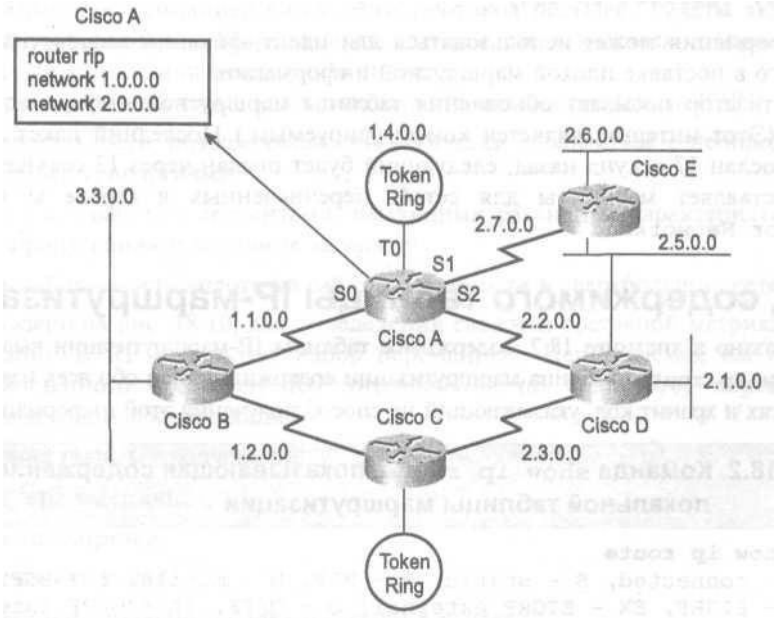


Fig.2.

Team debug IP rip outputs content packages updating route information protocol RIP V volume view, V which these data are sent And are accepted.

Protocol IGRP

IGRP represents by myself protocol routing By vector distances developed company Cisco. This protocol sends packages updating route information at 90-second intervals, which contain information about networks For specific autonomous systems. This protocol characterizes versatility to automatically handle complex topologies, and flexibility V work With segments, having different characteristics By strip bandwidth and delay values. The metric he uses does not have the inherent protocol RIP restrictions By quantity transitions. She includes next components: Width stripes transmission; Size delays; Level downloads; Reliability channel; Size maximum transmission block V channel.

Choice protocol IGRP V quality protocol routing is being carried out With help commands:

Router (config)# **router igrp autonomous-system**

Where parameter Autonomous system they call number autonomous systems And He identifies computing process IGRP- routing. Processes V routers networks With the same number autonomous-system will be collectively use the route information.

The network command specifies the directly attached networks that are subject to inclusion V given routing process:

Router(config-router)# **network network number**

IN shown example on Fig. 3 on router Cisco A launched a routing process that organizes IGRP routing in an autonomous system with a number 109. IN routing will be participate networks 1.0.0.0 And 2.0.0.0.

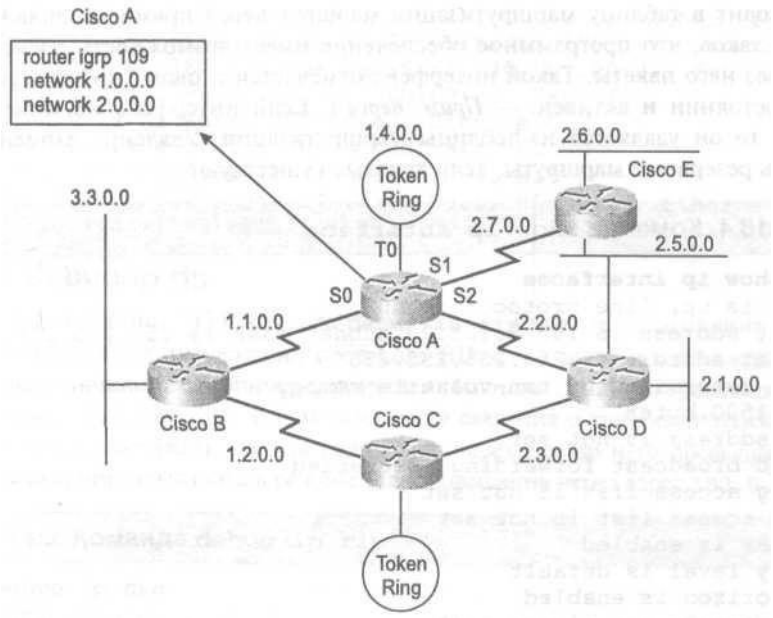


Fig.3.

The debug ip igrp transactions and debug ip igrp events commands display the contents of packets. updating route information protocol IGRP V volume view, V which these data is being sent And accepted

Protocol OSPF

OSPF is dynamic, hierarchical link state protocol used for routing within autonomous systems. It is based on open standards and was designed How replacement RIP protocol. He is development early versions protocol routing IS-IS. OSPF - stable protocol, supportive least-weight routing and load balancing. Shortest path in the network is calculated By algorithm Dijkstra. Cisco supports my version standard OSPF.

How only router configured on work With OSPF, He begins process exploring the environment, going through several initialization phases. At the beginning, the router uses Hello For definitions their own neighbors And creation relationships For exchange update route information With them. Then router begins phase ExStart initial exchange between bases routes. Next is a phase exchange, V

which appointed router sends route information And receives confirmation from ours new router. IN flow stages downloads, newrouter compiles table routes. By at the end calculations the router enters the full state, in which it is an active member networks.

For launch OSPF routing serves team Router(config)#

router ospf N,

Where N-number computing process OSPF. IN difference from IGRP He Maybe be various For different routers autonomous systems. OSPF region Area is being organized team

Router(config-router)# **network network number area Area**

And defines autonomous system.

IN OSPF network number has special format. For pluggable V process Network routing uses an inverse mask. So, the network 212.34.0.0 255.255.0.0 place V region 7 OSPF routing follows give team

Router(config-router)# **network 212.34.0.0 0.0.255.255 area 7**

Team show IP ospf interface For each interface outputs all OSPF information: IP address, region, number process, identifier router, price, priority, type networks, timer intervals.

Team show IP ospf neighbor shows important information, concerning states neighbors.

Practical Part

1. Download V simulator topology And configuration, used practical parts laboratory work №2.

2. If made All Right You you can ping from any routers addresses directly united interfaces others routers. On each device, using commands CDP show cdp neighbors detail, receive IP neighboring addresses devices And ping their.

3. In Lab 2 we were unable to ping the long-distance interfaces. Router2 was unavailable net 172.16.10.0/24, A from Router4 was unavailable net 10.1.1.0/24. IN laboratory work No. 3 With help static routing We decided problem. IN this work For solutions problems we use different forms dynamic routing.

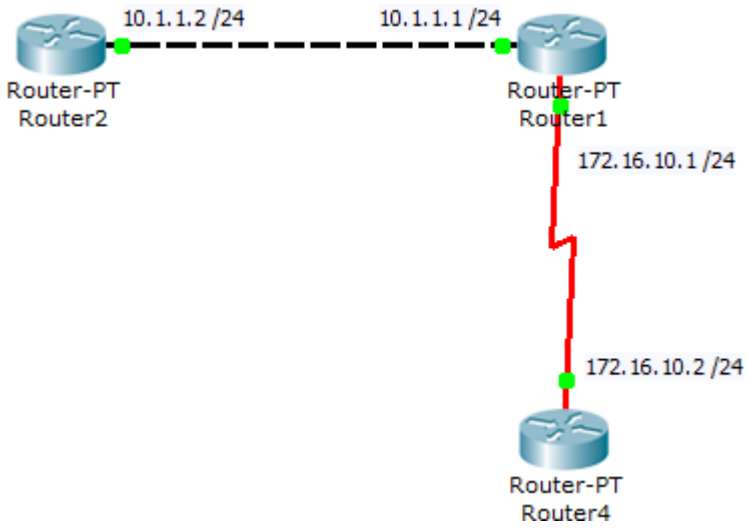


Figure 4.

.

4. Let's see tables routesRouter2# **sh IP route**
No route on net 172.16.10.0/24. That's why V this one net from Router2 Not they are coming pings.Router4# **sh IP route**
No route to net 10.1.1.0/24.
That's why V this one net from Router4 Not they are coming pings.

RIP
1. Let's turn it on RIP on everyone routers
Router1(config)# **router rip**
Router1(config-router)# **network 172.16.10.0**
Router1(config-router)# **network 10.1.1.0**

Router2(config)# **router rip**
Router2 (config-router)# **network 10.1.1.0**

Router4(config)# **router rip**
Router4 (config-router)# **network 172.16.10.0**

2. On each router, we'll use the show running-config command to see how the routers are understood our commands. We see that the 10.1.1.0/24 network is perceived as the 10.0.0.0/8 network, and the 172.16.10.0/24 perceived How net 172.16.0.0/16. It's related With classes IP addresses.

3. Using the show ip protocols command, we'll see what parameters the protocol works with. RIP. For example, For Router1 we have

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial2/0             1     2 1
  FastEthernet0/0       1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.16.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
Distance: (default is 120)
```

Translate message.

4. Let's see tables routesRouter2# **sh**

IP route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
R    172.16.0.0/16 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0
```

Eat route on network 172.16.10.0/24 via the interface Ethernet on address 10.1.1.1.

Pings V this one net from Router2 they will go. Check it out

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Let's move on on another router

Router4# **sh IP route**

```
R    10.0.0.0/8 [120/1] via 172.16.10.1, 00:00:22, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Eat route on network 10.1.1.0/24 through interface Serial on address 172.16.10.1.Pings V this one net from Router4 they will go. Check it out

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

5. Team debug IP rip We'll see How routers exchangeroute information. For example, For Router1 we have recurring every 30 seconds messages

6.

Router1# **debug IP rip**

```
RIP: sending update to 255.255.255.255 via Serial0 (172.16.10.1)
 subnet 10.1.1.0, metric 1

RIP: sending update to 255.255.255.255 via Ethernet0 (10.1.1.1)
 subnet 172.16.10.0, metric 1

RIP: received update from 172.16.10.2 on Serial0

RIP: received update from 10.1.1.2 on Ethernet0
```

Let's turn it off tracing

Router1# **no debug IP rip**
Save configuration.

EIGRP

Let's stop on everyone routers RIP team

Router(config)#no router rip.

1. Let's turn it on EIGRP on everyone routers, forming autonomous system With number 100

Router1(config)# **router eigrp 100**
Router1(config-router)# **network 172.16.10.0**
Router1(config-router)# **network 10.1.1.0**

Router2(config)# **router eigrp 100**
Router2 (config-router)# **network 10.1.1.0**

Router4(config)# **router eigrp 100**
Router4 (config-router)# **network 172.16.10.0**

2. On each router team show running-config We'll see How The routers understood our commands. We see that the 10.1.1.0/24 network is recognized as a network. 10.0.0.0/8, and the network 172.16.10.0/24 is perceived as the network 172.16.0.0/16. This is due to classes IP addresses.

3. Using the show ip protocols command, we'll see what parameters the protocol works with. EIGRP. For example, For Router1 we have

```
Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
    172.16.0.0/16 for FastEthernet0/0
      Summarizing with metric 20512000
    10.0.0.0/8 for Serial2/0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
     172.16.0.0
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.10.2     90            8321604
    10.1.1.2        90            8350639
  Distance: internal 90 external 170
```

Translate message.

4. Let's see tables routesRouter2# **sh**

IP route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
D    172.16.0.0/16 [90/20514560] via 10.1.1.1, 00:08:37, FastEthernet0/0
```

There is a route to the network 172.16.10.0/24 via the Ethernet interface to the address 10.1.1.1.Pings V this one net from Router2 they will go. Check it out

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Let's move on on another router

Router4# **sh IP route**

```
D    10.0.0.0/8 [90/20514560] via 172.16.10.1, 00:12:30, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Eat route on network 10.1.1.0/24 through interface Serial on address 172.16.10.1.Pings V this one net from Router4 they will go. Check it out

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

7. Teams debug IP eigrp transactions And debug IP eigrp events take a look How routers exchange route information.

Save configuration.

OSPF

Let's stop on everyone routers EIGRP teamRouter(config)# **no**

router eigrp 100

1. Let's turn it on OSPF on everyone routers. We will give process OSPF number 100.Let's form OSPF region 0

Router1(config)# **router ospf 100**
Router1(config-router)# **network 172.16.10.0 0.0.0.255 area 0**
Router1(config-router)# **network 10.1.1.0 0.0.0.255 area 0**

Router2(config)# **router ospf 100**
Router2(config-router)# **network 10.1.1.0 0.0.0.255 area 0**

Router4(config)# **router ospf 100**
Router4(config-router)# **network 172.16.10.0 0.0.0.255 area 0**

2. Team show running-config shows, What routers understood ourteams V volume same view, How We their And asked.

3. Team show IP protocols We'll see With what parameters works protocolOSPF. For example, For Router1 we have

```
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.10.0 0.0.0.255 area 0
    10.1.1.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2             110      00:01:40
    172.16.10.2          110      00:01:45
  Distance: (default is 110)
```

Translate message.

4. Let's see tables routesRouter2# **sh**

IP route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.10.0 [110/782] via 10.1.1.1, 00:08:26, FastEthernet0/0
```

Eat route on network 172.16.10.0/24 via the interface Ethernet on address 10.1.1.1.

Pings V this one net from Router2 they will go. Check it out

Router2# ping 172.16.10.1
Router2# ping 172.16.10.2

5. Let's move on on another router

Router4# **sh IP route**

```
     10.0.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/782] via 172.16.10.1, 00:03:26, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Eat route on network 10.1.1.0/24 through interface Serial on address 172.16.10.1.Pings V this one net from Router4 they will go. Check it out

Router4# ping 10.1.1.1
Router4# ping 10.1.1.2.

8. Teams show IP ospf interface, show IP ospf database And debug IP igrp neighborthey will show to you all information O parameters protocol OSPF.

Save configuration.

Control questions

1. What such autonomous system.
2. What such metrics?
3. Which exist two class protocols dynamic routing.
4. Explain work distance vector protocols.
5. Explain work protocols states connections.
6. How to know, which protocols routing launched on router?
7. IN how advantages And flaws distance vector protocols Andprotocols states connections?
8. What such convergence protocols routing?
9. Which parameters influence on speed convergence?

10. How to run and configure the RIP routing protocol on a router? 11. How to run and configure the EIGRP routing protocol on a router?12. How on start the router And tune protocol routing OSPF?

13. How look content packages updating route informationRIP protocol?
14. How look content packages updating route informationprotocol EIGRP?
15. Could you clarify what is meant by an autonomous system in EIGRP?
16. In how difference V format teams router For EIGRP And OSPF? 17. In how difference V format teams network for RIP, EIGRP And OSPF?

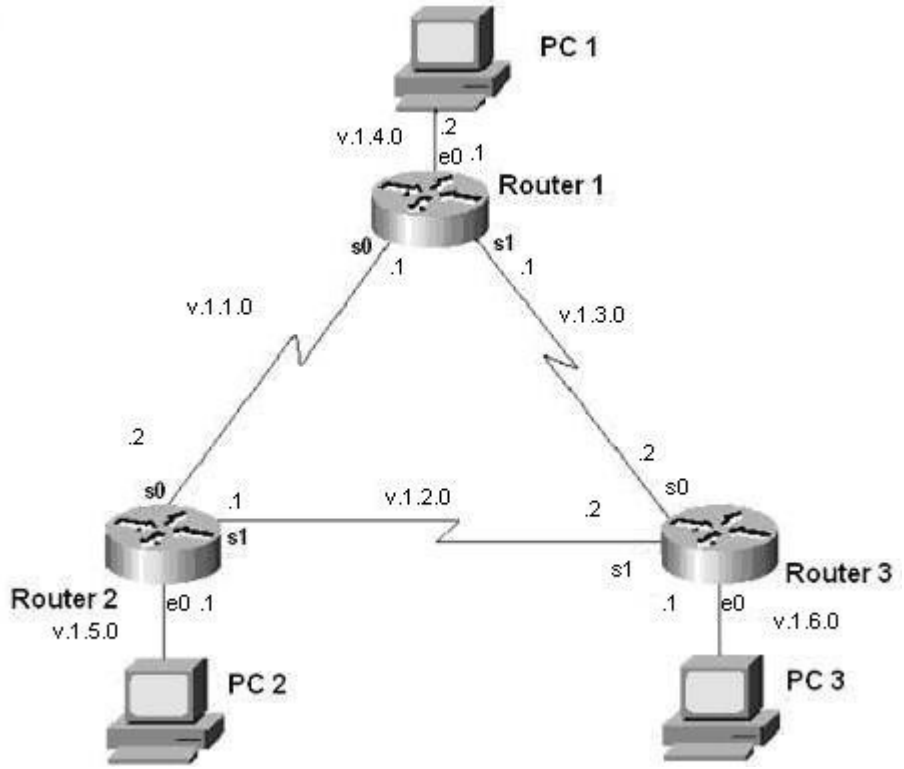
Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute V Packet Tracer practical Part.
4. Using the option from the previous lab, complete the following in Boson:exercise For independent work.
5. Show me to the teacher result execution points 7, 10, 14 And 18 tasksFor independent work.
6. Make out report. Content report Look below.

7. Protect report.

Exercise For independent work

1. Use the topology of your version from the previous lab, presented on drawing 5.



Drawing 5.

Our network has six subnets. You can see that each router is connected to three subnets.

2. Edit manually saved configuration previous successfully completed laboratory works: remove V rtr files routers teams static routing.

3. Download edited configuration V simulator.

4. On each router check right downloads configurations teams show cdp neighbors and show IP interface brief.

If the serial interface does not come up, check with **the show running command. config** that is on the DCE side interface serial communication is given **the clock command rate!** If Not given, That ask her.

5. Set up on each router dynamic routing By protocol RIP.

6. On each router, view the routing table using the show command. IP route. Take screenshots. For example, for router1 for option 1 (v=1) we have

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:01:43, Serial1
R       1.1.5.0/24 [120/1] via 1.1.1.2, 00:06:30, Serial0
R       1.1.2.0/24 [120/1] via 1.1.1.2, 00:03:35, Serial0
```

7. On each computer complete teams tracing tracert others computers. Take screenshots. Six screenshots in total. For example, a trace from PC1 on PC2 For options 1 (v=1) has view
We see, What path For packages from PC1 on PC2 (1.1.5.2) lies sequentially through Router1

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.1.2 20 msec 16 msec 16 msec
 3 1.1.5.2 20 msec 16 msec *
```

(Ethernet 1.1.4.1) And then through Router2 (serial0 1.1.1.2)

8. Let's turn it off on router router1 consistent interface serial 0Router1(config)# **interface serial 0**
Router1(config-if)# **shutdown**

9. Through couple minutes, When V networks will pass updates route information, on each router view the routing table with the command Show ip route. Take screenshots. For example, for router1, for option 1 (v=1) we have
We see, What table changed: disappeared net 1.1.1.0/24 And All packages Now are routed on

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.2.0/24 [120/1] via 1.1.3.2, 00:07:26, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:08:41, Serial1
R       1.1.5.0/24 [120/2] via 1.1.3.2, 00:07:44, Serial1
```

address 1.1.3.2 through interface Serial1.

10. On each computer complete teams tracing tracert others computers. Take screenshots. Six screenshots in total. For example, a trace from PC1 on PC2 For options 1 (v=1) has view

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.3.2 20 msec 16 msec 16 msec
 3 1.1.2.1 20 msec 16 msec 16 msec
 4 1.1.5.2 20 msec 16 msec *
```

We see that now the path for packets from PC1 to PC2 (1.1.5.2) goes sequentially through Router1 (Ethernet 1.1.4.1), then through Router3 (serial0 1.1.3.2) and then through Router2 (serial1 1.1.2.1).

11. Save configuration.

12. Turn it off RIP And set up on each router dynamic routing By protocol IGRP.

13. On each router, view the routing table using the command Show ip route. Take screenshots. For example, for router1, for option 1 (v=1) we have

14. Check it out, What You All done Right. On each computer run commands tracert

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
I       1.1.6.0/24 [100/651] via 1.1.3.2, 00:02:38, Serial1
I       1.1.5.0/24 [100/651] via 1.1.1.2, 00:04:26, Serial0
I       1.1.2.0/24 [100/651] via 1.1.1.2, 00:08:28, Serial0
```

others computers.

15. Save configuration.

16. Turn it off IGRP And set up on each router dynamic routing By protocol OSPF.

17. On each router, view the routing table using the command Show ip route. Take screenshots. For example, for router1, for option 1 (v=1) we have

18. Check it out, What You All done Right. On each computer perform tracing

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
O       1.1.5.0/24 [110/65] via 1.1.1.2, 00:00:39, Serial0
O       1.1.2.0/24 [110/65] via 1.1.3.2, 00:00:22, Serial1
O       1.1.6.0/24 [110/65] via 1.1.3.2, 00:00:26, Serial1
```

commands tracert others computers.

19. Save configuration.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshot topology, created at execution practical parts.

2. Configurations of three routers from .txt files created during execution practical part for each routing protocol. Total content 9 (nine) files.

3. Screenshot topology from drawing 5 With addresses your own version

4. Table 2 previous laboratory work With addresses his own options

5. Configurations of three routers from .txt files created during execution exercise For independent work For each protocol routing. Total content 9 (nine) files.

6. All screenshots, specified V task For independent work

Practical class №10. Network Layer Protocols (Part 1).

Theoretical Part

Scalable net requires schemes addressing allowing height. However as a result uncontrolled growth networks can arise row unforeseen consequences. As nodes and subnets are added to the enterprise network, shortage free addresses And will be required change schemes existing addresses. This Can avoid by way thorough planning scalable address systems networks enterprises.

Unfortunately, the TCP/IP architects could not predict exponential growth. Internet, and V present time sharp costs distribution problem addresses.

When TCP/IP was introduced in the 1980s, it was based on a two-level addressing scheme. The high-order part of the 32-bit IP address determined the network number (address), and the low-order part number host. Address networks necessary For interactions networks. Routers use the network part of the address to organize communication between hosts from different networks.

For facilities human perception IP address is being recorded V view four decimal numbers separated by periods. The 32-bit address is divided into four groups by eight bit, called octets. Every octet is being recorded V decimal view And is divided dots. For example

10101100000111101000000000010001 <-> 10101100 00011110 10000000 00010001 <-> 172 30 128 17 <-> 172.30.128.17

The question arises: how to distinguish the network address and the host address from any IP address? beginning use TCP/IP For solutions this question was used class addressing system. IP addresses were divided into five disjoint classes. The breakdown implemented according to values several first bit V first octet.

If the first bit in the first octet is zero, then it is a Class A address. Class B addresses are beginning from binaries 10. Addresses class WITH are beginning With binary 110.

IN addresses class A address networks is located V first octet. IN class IN For The first and second octets are used for network addressing. In class C, the network addressing is used the first, second, and third octets. The use of classes D and E is specific And Here Not is being considered.

In modern networks, classes are often ignored and classless IP is used. scheme, founded on masks subnets.

From here on we will use masks in the form of a sequence of binary ones, turning into a sequence of binary zeros with a total length of 32 bits. Masks accepted record V decimal form like IP addresses

11111111111111110000000000000000 <->11111111 1111111 0000000 0000000 <-> 255 255 0 0 <-> 255.255.0.0

The subnet mask is a necessary addition to the IP address. If the bit in the IP address corresponds single bat V mask, That this bit V IP address represents number networks, and if the bit in the IP address corresponds to the zero bit in mask, then this bit is in the IP address represents the host number. So for the mask 255.255.0.0 and the address 172.24.100.45, the network number will 172.24.0.0, A For masks 255.255.255.0 number networks will 172.24.100.0.

Other form records masks - /N, Where N - number units V mask. This form used only in combination with an IP address. For example, for the mask 255.255.0.0 and the address 172.24.100.45 they write 172.24.100.45/16.

All class A addresses have a mask of 255.0.0.0, class B addresses have a mask of 255.255.0.0, and class C addresses have a mask of 255. 255. 255.0. The converse is not true, since How at definition class are used first bits V first octet of the address.

If organization has network class IN (mask 255.255.0.0), That she Maybebreak this one net on subnets, using mask 255.255.255.0. For example, If address 172.24.100.45 belongs to an organization, then the class B network number will be 172.24.0.0, and the intra-corporate subnet number will be 172.24.100.0. Note that the received subnets Not will be be networks class WITH.

If the number of zeros in the mask is M, then the number of available host addresses in the subnet equals 2M-2. That is, it is not recommended to use two addresses in a subnet. One of these addresses in which the last M bits are zero is called a subnet address, and the second from these addresses at whom latest M bit equal unit it's called broadcast address. So For addresses 172.24.100.45/24 address subnets equal 172.24.100.0, and the broadcast address is 172.24.100.255. The number of addresses in the subnet equals 2^8-2 =254.

Addresses class A And IN make up near 75 percent address space. The number of class A and B networks is approximately 17,000. The acquisition of a class A network B, A those more class And in present time is very problematic. Addresses class WITH make up about 12.5 percent address space. Number of networks class WITH approximately equals 2.1 million. TO unfortunately net class WITH limited 254 addresses, which does not meet the needs of large organizations that cannot acquire class addresses A or IN.

Classful IP addressing, even with the use of subnets, cannot satisfy requirement By scalability For Internet communities.

Already in the early 90s, almost all class B networks were distributed. Adding to The Internet of new Class C networks led to a significant increase in route tables and overload routers. Usage classless addressing allowed V significant measure decide problems that have arisen.

CIDR

Modern routers use form IP addressing called classless cross-domain routing (Classless Interdomain Routing (CIDR)),

which ignores classes. IN systems, using classes, router determines the class of the address and then splits the address into network octets and host octets based on in this class. In CIDR, the router uses mask bits to determine the address network parts And numbers host. Border divisions addresses Maybe pass in the middle octet.

CIDR significantly improves IP scalability and efficiency in the following ways: points:

- flexibility;
- economical usage addresses V highlighted range;
- improved aggregation routes;
- Supernetting is the combination of contiguous network addresses into a new supernet address, determinable mask.

CIDR allows routers to aggregate or summarize information about routes. They do This by way use masks instead of classes addresses For determining the network portion of an IP address. This reduces the size of route tables, since is used only one address And mask For performances routes ko many subnets.

Without CIDR And aggregations routes router must contain individual information For everyone subnets.

Let's consider net class A 44.0.0.0/8, V which is being considered 8 subnets

Network number	The first octet	Second octet	Third octet	Fourth octet
44.24.0.0/16	00101100	00011000	00000000	00000000
44.25.0.0/16	00101100	00011001	00000000	00000000
44.26.0.0/16	00101100	00011010	00000000	00000000
44.27.0.0/16	00101100	00011011	00000000	00000000
44.28.0.0/16	00101100	00011100	00000000	00000000
44.29.0.0/16	00101100	00011101	00000000	00000000
44.30.0.0/16	00101100	00011110	00000000	00000000
44.31.0.0/16	00101100	00011111	00000000	00000000

Table 1.

The first two octets (16 bits) represent the subnet address. Since the first 16 bits the addresses of each of these eight subnets are unique, then the classful router sees eight unique networks and must create a route table row for each of them. these subnets.

However, these eight subnet addresses have one thing in common: the first 13 bits are the same. CIDR-compliant router Maybe summarize routes To this eight subnets, using general 13-bit prefix V addresses: 00101100 00011. For performances this prefix in decimal form let's supplement his on the right zeros

10101100 00011000 00000000 00000000 = 172.24.0.0.

13-bit mask subnets has view

11111111 11111000 00000000 00000000 = 255.248.0.0.

Therefore, one address and one mask defines a classless prefix, which summarizes routes To eight subnets: 172.24.0.0/13.

Supernetting

Supernetting is the practice of using a bit mask to group multiple classful networks as a single network address. Supernetting and route aggregation There are different names for the same process. However, the term supernetting is more often used when Aggregated networks are under common administrative control. Supernetting beret bits from network portions masks, A subnetting beret bits from portions masks, related To host. Supernetting And aggregation routes is inverse concept By attitude To subnetting.

Since class A and B networks are almost exhausted, organizations are forced request from providers some networks class WITH. If company receives block continuous addresses in class C networks, then supernetting can be used and all addresses in companies will be lie V one larger network or supernets.

Let's consider company ABC, which required addresses For 400 hosts. At class addressing company should request at central Internet services InterNIC class B network. If a company gets such a network, there will be tens of thousands of addresses in it will not be used. The alternative is to get two Class C networks, which gives254*2= 504 addresses For hosts. Flaw this approach consists of V necessity support routing For two networks.

With a classless address system, supernetting allows ABC Company to obtain necessary address space With minimal quantity unusedaddresses And without increases size tables routing. Using CIDR, ABC requests a block of addresses from its Internet provider, not from the central Internet services InterNIC. Provider defines needs ABC And highlights address space from his own address space. Provider beret on myself control address space V his own internal classless system. All external Internet routers contain only summary routes to the provider's network. Provider myself supports routes, more specific For their own clients, including ABC. This approach significantly reduces the size of route tables for all routers V Internet.

Let ABC receive two class C networks from the provider, the addresses in which are continuous: 207.21.54.0 and 207.21.55.0.

207.21.54.0	110001111	00010101	00110110	00000000
207.21.55.0	110001111	00010101	00110111	00000000

Table 2.

From the table it can be seen that the addresses have a common 23-bit prefix 11001111 00010101 0011011. Complementing prefix on the right zeros 11001111 00010101 00110110 00000000, we will receive supernet from 23- bit mask, 207.21.54.0/23.

Provider provides net companies ABC external to the world How net 207.21.54.0/23.

CIDR allows providers to efficiently distribute and aggregate contiguous spaces IP addresses.

VLSM

Mask variable lengths (Variable-Length Subnet Mask (VLSM)) allows organizations use more than one subnet mask within the same network address space. Implementation VLSM often they call subnets on subnets."

Let's look at subnets created by borrowing the first three bits in the host portions addresses class WITH 207.21.24.0

Subnet	Address subnets
0	207.21.24.0/27
1	207.21.24.32/27
2	207.21.24.64/27
3	207.21.24.96/27
4	207.21.24.128/27
5	207.21.24.160/27
6	207.21.24.192/27
7	207.21.24.224/27

Table 3.

We got eight subnets, each of which can contain no more than 30 hosts.

Each connection is via serial interface requires two addresses for myself and a separate subnet. Using any of the /27 subnets for this will result in a loss addresses. To create a subnet which of the two addresses is better fits 30 bit mask. This is just what you need for a serial connection. Let's break one of subnets 207.21.24.192/27 by eight subnets, using 30 bit mask.

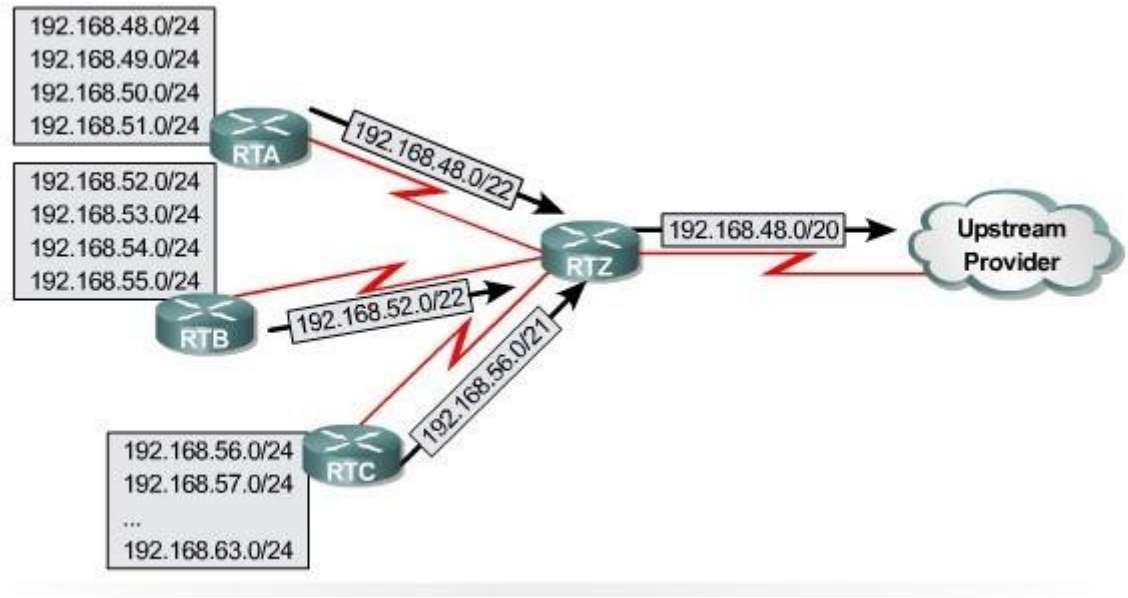
0	207.21.24.192/30
1	207.21.24.196/30
2	207.21.24.200/30
3	207.21.24.204/30
4	207.21.24.208/30
5	207.21.24.212/30
6	207.21.24.220/30
7	207.21.24.224/30

Table 4.

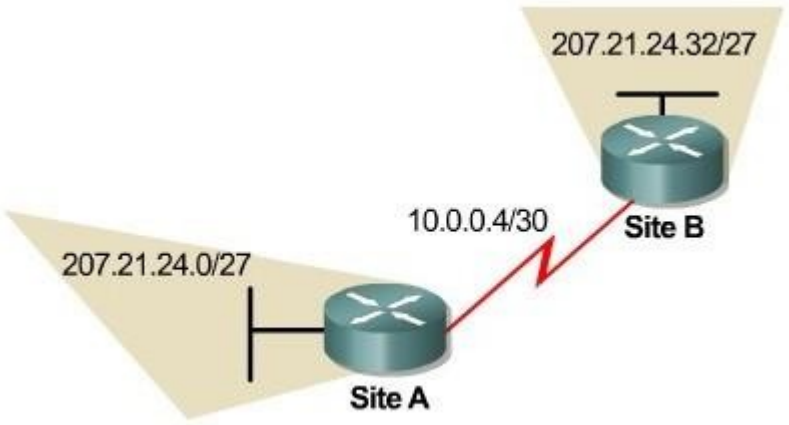
That is, each of the remaining seven /27 subnets can be used for addressinghosts in seven local area networks. These local area networks can be connected into a global network with help Not more than eight sequential connections from ours eight networks.

To ensure that routing is performed correctly in VLSM networks, routers should exchange information O masks V subnets.

Using CIDR and VLSM not only prevents wasted addresses, but also contributes aggregations routes or summation. Without summation routes The Internet would have stopped developing by the end of the 90s. The figure illustrates how summation reduces load on routers.



Rice. 1



Rice. 2

This complex hierarchy of networks and subnetworks is summed up at various points so that the whole the network as a whole looks from the outside like 192.168.48.0/20. For the summation to work correctly routes follows thoroughly approach to the appointment addresses: summable addresses should have identical prefixes.

Torn subnets

Broken subnets are networks from one main network, separated by a network in a completely another address range. Classful routing protocols RIP version 1 and IGRP do not support bursting networks, So How routers Not exchange masks subnets. If in Figure 1, Site A and Site B are running on RIP version 1, then Site A will be receive routing information updates from site B on the network 207.21.24.0/24, not in networks 207.21.24.32/27.

RIP v2 and EIGRP summarize addresses at class boundaries by default. Usually such summation desirable. However V case torn subnets Not desirable. Cancel class autosummation Can team no auto-summary.

Practical Part

Configuring VLSM And let's test functionality on two protocols routing RIP versions 1 And RIP versions 2.

Let's consider net class WITH 192.168.1.0/24. Required highlight minimum By 25 addresses for two local networks and reserve the maximum number of addresses for further development.

For support 25 hosts V each subnets required minimum five bit V eight-bit host portion of the address. Five bits will give a maximum of 30 possible addresses. hosts (25 = 32 - 2). If five bits are to be used for hosts, then the other three bits in the last octet of the address can be added to the 24-bit mask of our network class WITH. Hence, 27-bit mask Maybe be used For creation following 8 subnets:

0	192.168.1.0/24	4	192.168.1.128/24
1	192.168.1.32/24	5	192.168.1.160/24
2	192.168.1.64/24	6	192.168.1.192/24
3	192.168.1.96/24	7	192.168.1.224/24

Table 5.

To further maximize the address space, the 192.168.1.0 /27 subnet is againis divided on 8 subnets With using 30-bit masks:

0	192.168.1.0/30	4	192.168.1.16/30
1	192.168.1.4/30	5	192.168.1.20/30
2	192.168.1.8/30	6	192.168.1.24/30
3	192.168.1.12/30	7	192.168.1.28/30

Table 6.

These subnets can be used for serial point-to-point connections. dot And minimize losses addresses, since each subnet contains only two addresses.

Let's build and configure the network shown in Figure 3. For a Vista router let's take model 2501, A For the rest two model 805. We use Switch 2950.

1. Raise it up interfaces And check net team **show cdp neighbors.**
2. Assign addresses according to drawing. Check it out appointment team **show IP interface brief.**

3. For computer HostA we have ambiguity V appointment route By default: or on address 192.168.1.33 Ethernet interface router SanJose1, or on address 192.168.1.34 Ethernet interface router SanJose2 **.** Select arbitrary, For example

hostA# **ipconfig /dg 192.168.1.33**

4. We will configure routing on all three routers protocol RIP with disabled autosummation addresses. This will allow passage information O subnets.

Router(config)# **router rip**
Router(config-router)# **version 2**
Router(config-router)# **no auto-summary**
Router(config-router)# **network 192.168.1.0**

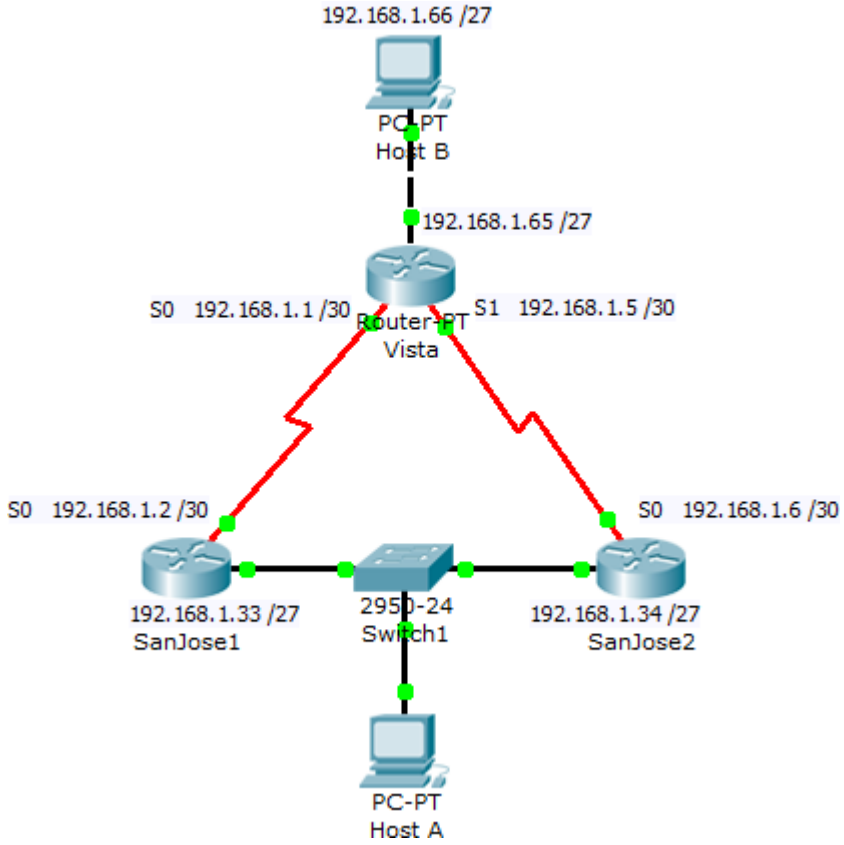


Fig. 3

5. Must see, What on router Vista There is route on local net192.168.1.32/27, Where the computer is located hostA.

Vista# **show IP route**

```
C       192.168.1.0/30 is directly connected, Serial2/0
C       192.168.1.4/30 is directly connected, Serial3/0
R       192.168.1.32/27 [120/1] via 192.168.1.6, 00:00:15, Serial3/0
                        [120/1] via 192.168.1.2, 00:00:24, Serial2/0
C       192.168.1.64/27 is directly connected, FastEthernet0/0
```

Note, What V table withdrawn only one route on net 192.168.1.32/27 -on address192.168.1.2 through interface Serial0, Although There is more one route on network 192.168.1.32/27 -

via the 192.168.1.6 address of the Serial1 interface. In a real router, we would see both these route. Simulator outputs one route, But exchanged route information By both of them interfaces Serial0 And Serial1:

Vista# **debug IP rip**

```
RIP: sending update to 255.255.255.255 via Serial0 (192.168.1.1)
 subnet 192.168.1.64, metric 1
 subnet 192.168.1.4, metric 1
 subnet 192.168.1.32, metric 2

RIP: sending update to 255.255.255.255 via Serial1 (192.168.1.5)
 subnet 192.168.1.64, metric 1
 subnet 192.168.1.0, metric 1

RIP: sending update to 255.255.255.255 via Ethernet0 (192.168.1.65)
 subnet 192.168.1.0, metric 1
 subnet 192.168.1.4, metric 1
 subnet 192.168.1.32, metric 2

RIP: received update from 192.168.1.2 on Serial0
     192.168.1.32 in 1 hops
     192.168.1.4 in 2 hops

RIP: received update from 192.168.1.6 on Serial1
     192.168.1.32 in 1 hops
     192.168.1.0 in 2 hops
```

Vista# **no debug IP rip**

Do it screenshots.

6. Must see, What on router SanJose1 There is route on localnet 192.168.1.64/27, Where is located computer hostB.

```
C       192.168.1.0/30 is directly connected, Serial2/0
R       192.168.1.4/30 [120/1] via 192.168.1.34, 00:00:18, FastEthernet0/0
C       192.168.1.32/27 is directly connected, FastEthernet0/0
R       192.168.1.64/27 [120/1] via 192.168.1.1, 00:00:18, Serial2/0
```

Do it screenshot.

7. Must see that on router SanJose2 Also There is route onlocal net 192.168.1.64/27, where is located computer hostB.

```
R       192.168.1.0/30 [120/1] via 192.168.1.33, 00:00:09, FastEthernet0/0
C       192.168.1.4/30 is directly connected, Serial3/0
C       192.168.1.32/27 is directly connected, FastEthernet0/0
R       192.168.1.64/27 [120/1] via 192.168.1.5, 00:00:26, Serial3/0
```

Do it screenshot.

Ping your computer hostA from the computer hostB And vice versa. Do it 2 screenshot.

Note, What simulator implemented So, What given example works And withoutinput teams version 2 And no auto-summary.

Control questions

1. For what needed mask?

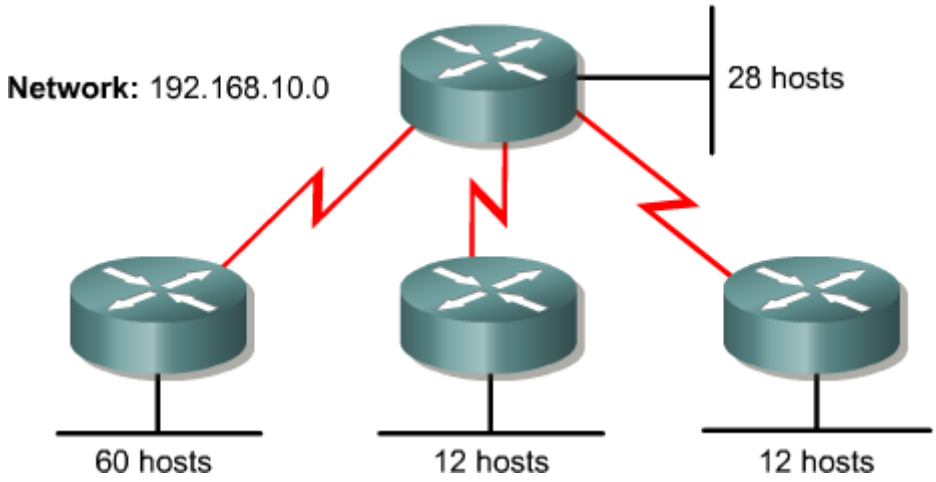
2. What's happened CIDR?
3. What such VLSM?
4. How at use classes IP addresses V IP address highlight address hostaAnd address subnets?
5. How without use classes IP addresses V IP address allocate an address hosta And subnet address?
6. What equals number available addresses V subnets?
7. Based on the number of nodes in the subnet specified by the teacher, determineminimum mask.
8. Which forms records masks You do you know?
9. Why consistent compound highlight V separate subnet?
10. What mask is recommended to use for a serial network ?connections And Why?
11. How CIDR And VLSM contribute thrifty use addressspace?
12. What such Supernetting?
13. What such aggregation routes And How she contributes reduction tablesroutes on routers?
14. What such torn subnets, And which protocols routing their Notsupport?
15. Which peculiarities work simulator at implementation protocol RIP?

Order execution And surrender work

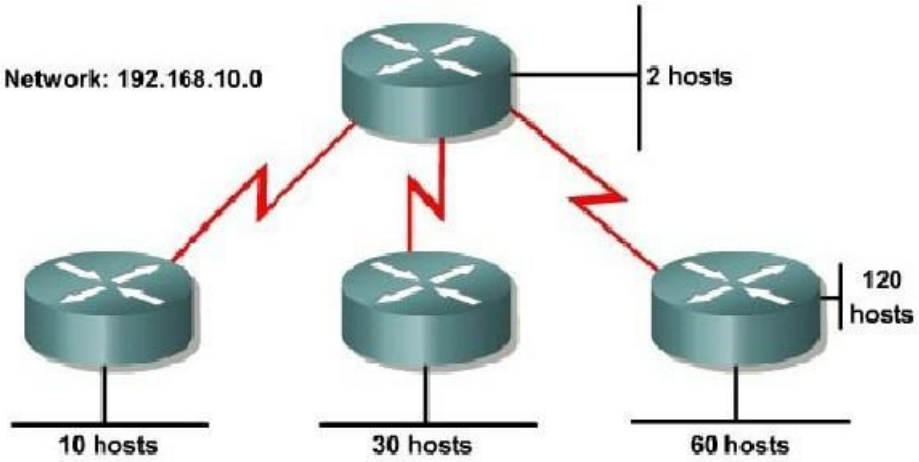
1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute V Packet Tracer practical Part.
4. Do it V Packet Tracer exercise For independent work.
5. Show me to the teacher result execution point 11 tasks Forindependent work.
6. Make out report. Content report Look below.
7. Protect report.

Exercise For independent work

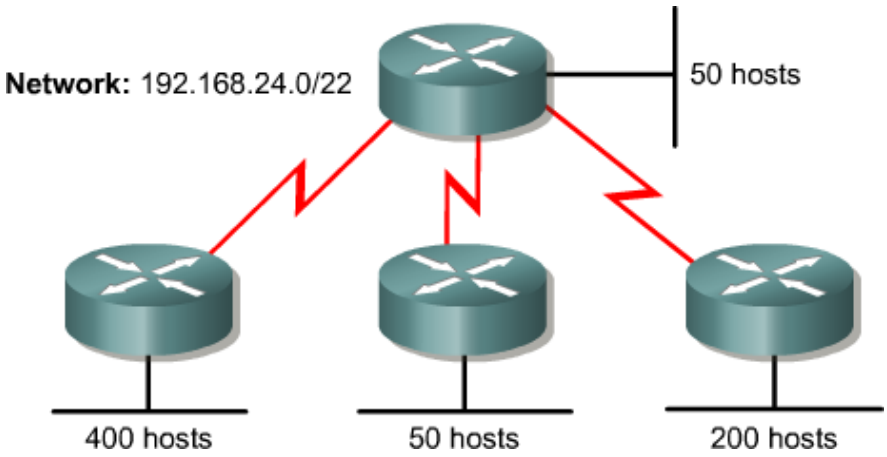
Design next four networks, according to received option. Cm. rice. 4,5, 6 And 7.



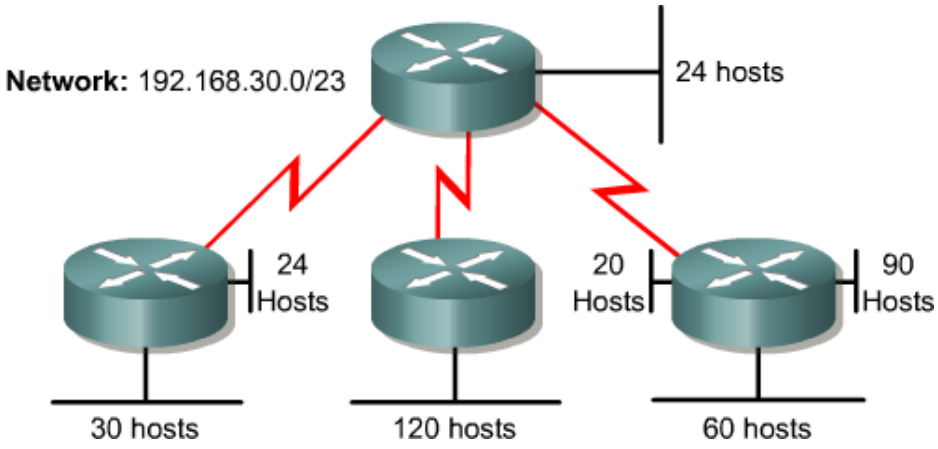
Rice 4. Option 1.



Rice 5. Option 2



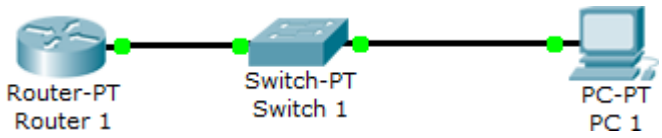
Rice 6. Option 3.



Rice 6. Option 4.

Order solutions options

1. In the designer, select the correct routers with the required number and type interfaces. Use multi-slot devices that have expandable number interfaces. IN simulator They have addresses species Ethernet 2/0, What means interface 0 V slot 2.
2. Create topology. Local net , seems to be V view switch with one computer



3. . Do it screenshot topology.
4. Assign each subnet a correct mask with a minimum number of zeros.Remember, What mask for sequential connections equal /30.
5. Decide which addresses you will assign to your network interfacesrouters And computers.
6. Apply V graphic editor on yours topology appointed addresses Andmasks.
7. IN simulator appoint addresses on network interfaces routers Andcomputers.
8. Check it out right appointments addresses teams **show IP interface brief** (router) or **ipconfig** (computer).
9. Configure dynamic routing on each routerprotocol RIP second versions.
10. On each router withdraw table routing And do itscreenshot.
11. You should ping from any computer any another computer.
12. By desire You you can V routers use interfaces loop loopback For modeling local networks With subsequent their replacement on An Ethernet interface that connects a router to a single computer. through switch.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshot topology, created at execution practical parts.
2. Configurations everyone routers from .txt files, created at executionpractical parts.
2. Screenshot topology your option With addresses And masks.
4. Configurations everyone routers from .txt files, created at executiontasks For independent work.
5. All screenshots, specified V task For independent work

Practical class №11. Network Layer Protocols (Part 2).

Theoretical Part.

An access control list (ACL) is a sequential list. rules that are used to allow or deny the flow of packets within a network basis information, given inside list. Without list access All packages within the network are allowed without restrictions for all parts of the network. The access list can be used to control the spread and obtain information about changes route tables and, most importantly, to ensure **security** . Security policy in particulars includes protection from external attacks, restrictions access between departments organizations And distribution downloads networks.

List access allows use router How internetwork screen, firewall, to prohibit or restrict access to the internal network from the external network, for example, the Internet. A firewall is typically placed at the connection points between two networks.

Standard ACL

When using standard ACLs, the only criteria for determining The IP address of the source of a packet is the indicator of whether a packet is allowed or denied. The format element list access next

Router(config)# **access-list No. permit | deny source address source-mask,**

where # is an integer – the access list number, source-address denotes the source address package, source mask - mask V inverse form, imposed on address, permit - allow passage package, deny - ban passage package. Number No. determines whether an access list element belongs to a specific access list with number #. The first access-list command defines the first element of the access list, the secondthe command defines the second element of the access list, etc. The router processes each access list defined in it by elements from top to bottom. That is, If the source address of the packet, taking into account the mask, satisfies the condition of the list element, then further elements list router Not processes. Hence, For To avoid unnecessary processing, elements that define more general conditions should be Place at the beginning of the list. Several routers can be defined within a router. access lists. The standard list number must be in the range 1–99. The mask in The access list is specified in inverse form, for example, the mask 255.255.0.0 looks like 0.0.255.255.

Routers Cisco assume What All addresses, Not mentioned V list access V obvious view, are prohibited. That There is V at the end list access present invisible element

Router(config)# **access-list # deny 0.0.0.0 255.255.255.255**

So, if we want to allow only traffic from address 1.1.1.1 and deny all the rest traffic enough V list access place one element

Router(config)# **access-list 77 permit 1.1.1.1 0.0.0.0.**

Here supposed, what are we organized list access With number 77.

Let's consider the possibility of using standard access lists for a range addresses. Let's take the range 10.3.16.0 – 10.3.31.255 as an example. To obtain the inverse masks can be subtracted from the higher address of the lower one and get 0.0.15.255. Then the example element list Can ask team

Router(config)# **access-list 100 permit 10.3.16.0 0.0.15.255**

For Togo, to list access started fulfill my he did the job must be applied To interface With help teams

Router(config-if) **#ip access group access list number in or out**

The access list can be applied either as an input (in) or as a day off (out). When You apply list access How input, That router receives input plastic bag And checks his input address With elements list. Router permits package be routed on interface appointments, If plastic bag satisfies permissive elements list or throws away plastic bag, If He corresponds conditions prohibiting elements list. If You apply list access How day off, That router receives input plastic bag, routes his on interface appointments And only Then processes input address package according to elements of the access list of this interface. The router then either allows the packet leave interface or throws away his according to permissive And prohibitive elements list respectively. So, created previously list With number 77 applies To interface Ethernet 0 router How input list of commands

Router(config)# **int Ethernet 0**

Router(config-if) **#ip access group 77 in**

The same list applies to the router's Ethernet 0 interface as an output list With using commands

Router(config-if) **#ip access group 77 out**

Canceled list on interface with help teams **no**

Router(config-if)# **no IP access group 77 out**

Let's move on to creating more complex access lists. Consider the network in the figure.1. Allow all packets coming from network 10.1.1.0 /25 (10.1.1.0 255.255.255.128), but We will deny all packets coming from the network 10.1.1.128 /25 (10.1.1.128 255.255.255.128). We we also want to deny all packets coming from the network 15.1.1.0 /24 (15.1.1.0 255.255.255.0), except for packets from a single host with the address 15.1.1.5. All other packets We we allow. List we'll give number 2. Subsequence teams For execution delivered tasks will next

Router(config)# **access-list 2 deny 10.1.1.128 0.0.0.127**

Router(config)# **access-list 2 permit 15.1.1.5 0.0.0.0**

Router(config)# **access-list 2 deny 15.1.1.0 0.0.0.255**

Router(config)# **access-list 2 permit 0.0.0.0 255.255.255.255**

Note the absence of a permitting element for the network 10.1.1.0 255.255.255.128. Its role performs last element **access list 2 permit 0.0.0.0 255.255.255.255.**

Let's make sure, What We completed delivered task.

1. Allow All packages, outgoing from networks 10.1.1.0 255.255.255.128.

The last one line V list access satisfies to this criterion. No there is no need to explicitly allow this network in our access list as in the list there are no lines matching this network except the last allow line permit 0.0.0.0 255.255.255.255.

2. Ban All packages, outgoing from networks 10.1.1.128 255.255.255.128.

The first line in the list fulfills this criterion. It is important to note the type of inverse masks 0.0.0.127 For this networks. This mask indicates, What We Not should take V consideration latest seven bit fourth octet addresses, which appointed For addressing in this subnet. The mask for this network is 255.255.255.128, which says that latest seven bit fourth octet determine addressing in this networks.

3. Deny all packets originating from network 15.1.1.0 255.255.255.0 except packages from the only one hosta With address 15.1.1.5

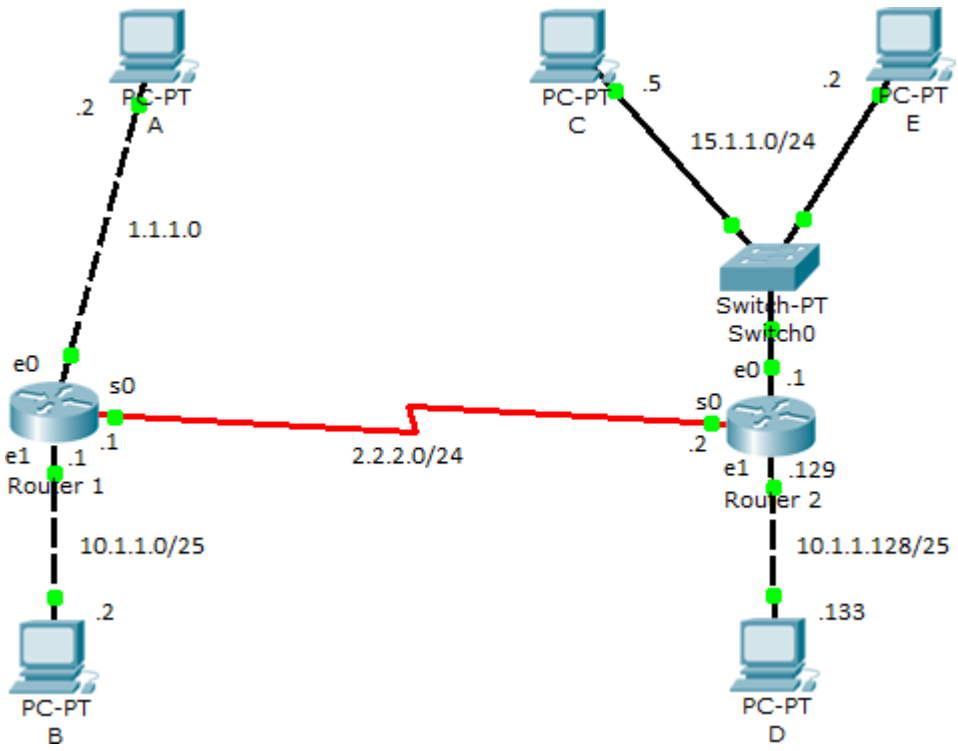


Figure 1.

This requirement is satisfied by the second and third lines of our access list. It is important to note that the access list implements this requirement in a different order than it is defined. It is important to remember that the access list is processed from the topdown and at the first match, packet processing stops. We first require deny all packets coming from network 15.1.1.0 255.255.255.0 and only then allow packages With address 15.1.1.5. If V teams, defining list access We,

let's rearrange the second And third teams, That all net 15.1.1.0 will prohibited to permissions of host 15.1.1.5. That is, the address 15.1.1.5 will be immediately banned from the beginning common criterion deny 15.1.1.0 0.0.0.255.

4. Allow all rest packages

The last one team permits All addresses, which Not correspond first threeteams.

Like this in this way, we have next subsequence actions For incarnationsaccess list.

1. Define criteria And restrictions For access.

2. Implement them using the access-list command by creating an access list withcertain number.

3. Apply list to a certain interface or How incoming, or Howoutgoing.

Let's focus on the last point. In general, the standard access list should be placed as close as possible to the destination, not to the source of the packets. Although can be exceptions. So How standard list access works only With original addresses, That Not Always possible detailed configuration. Required make every effort to avoid the occurrence of undesirable access configurations. If list placed nearby source packages, That Very likely, What access To devices, on which Not is being carried out none configuration access, will difficult.

Let's specify the security policy for the network in Figure 1. Our goal is to create policy for computer A (address 1.1.1.2 network 1.1.1.0/24), which from all devices local network 15.1.1.0 /24, which includes computer C (15.1.1.5), will allow access to computer A only himself computer WITH. We Also we want create politics, prohibiting remote access To computer A from any devices local networks
10.1.1.128 / 25 computer D (10.1.1.133). All the rest traffic We we allow. On In Figure 1, computer PC5 (15.1.1.5) plays the role of an arbitrary computer other than From the representative local networks 15.1.1.0/24.

The placement of the list is critical to the implementation of such a policy. Let's take the created previously list With number 2. If list do weekend on sequential interface router 2, then the task for computer A will be completed, however will arise restrictions on traffic between others local networks. Similar we'll get the same situation if we make this list an input on the serial interface router 1. If we put this list as output on Ethernet A interface router 1, That the task will be completed without any side effects effects.

Extended ACL

So standard ACL You you can indicate only address source, A mask Notis mandatory. IN extended ACL You should indicate And address receiver And address source With masks. You can add additional protocol information For

source and destination. For example, for TCP and UDP it is allowed to specify the port number, and For ICMP, you can specify the message type. As with standard ACLs, you can help options log realize log.

General form teams For formations lines list extended access

access list access-list-number {permit | deny} protocol source source-wildcard [operator source-port] destination destination-wildcard [operator [destination-port] [precedence precedence-number] [tos [tos] [established] [log | log-input] ,

where access-list-number -100-199|2000-2699, protocol - ip, icmp, tcp, gre, udp, igrp, eigrp, igmp, ipinip, nos and ospf. For source-port or destination -port can be use number port or his designation bgp, chargen, daytime, discard, domain, echo, finger, ftp, ftp-data, gopher, hostname, irc, klogin, kshell, lpd, nntp, pop2, pop3, smtp, sunrpc, syslog, tacacs-ds, talk, telnet, time, uucp, whois and www. Operator is eq (equal to), neq (not equal to), gt (greater than), lt (less how), range (two are specified) port for definitions range).

As well as For standard ACL extended ACL follows tie to the interface or For incoming on traffic interface

Router(config-if)# IP access group №ACL in

or For coming out from interface traffic

Router(config-if)# IP access group №ACL about ut

Here №ACL - number list.

Examples elements extended ACLAllow

SMTP from everywhere to the host

Router(config)# access list 111 permit tcp any host 172.17.11.19 eq 25

Allow telnet from everywhere on host

Router(config)# access list 111 permit tcp any host 172.17.11.19 eq 23

Extended ACL allows Very thin tune rights access.

Named ACL

TO named ACL are turning to By name, A Not By number, What gives clarity And convenience For appeals. For creation named ACL is present team

Router(config)# IP access list extended ACL_name

And further teams For creation elements list exactly this unnamed list

Router(config-ext-nacl)# permit|deny IP_protocol source_IP_address wildcard_mask [protocol_information] destination_IP_address wildcard_mask [protocol_information] [log]

For completion creation list follows give team exit.

Name named list sensitive To register. Teams For creation unnamed list similar to commands for creating numbered list items list, but the creation process itself is different. You must use the keyword ip before the main ACL operator and thus enter the configuration mode specifically for of this named list. In this mode, you start with keywords permit or deny And shouldn't enter access list V beginning each lines.

Binding named ACL To interface is carried out by the team

Router(config)# interface type [slot_№]port_№

Router(config-if)# IP access group ACL_name

in|out

ACLs are processed from top to bottom. The most frequently occurring traffic should be processed V beginning list. How only processed list plastic bag satisfies element list, processing this package stops. Standard ACLs should be placed closer to the destination where the traffic should be filtered. Output (out) extended ACLs should place as close to the source as possible filtered packages, A entrance follows put closer To point appointments, Where traffic must be filtered.

Named ACLs permits to you myself edit. For this necessary dial team, which was used For his creation

Router(config)# IP access list extended ACL_name

Use the vertical arrow keys to find the line in the list you want to want to change. Change it using the horizontal arrows. Press enter. New The line will be added to the end of the list. The old one will not be deleted. To delete it, you should enter no V beginning lines.

To edit numeric ACLs, you must destroy it and recreate it or change list offline And download V device With help.

Practical Part.

1. Let's load it V simulator topology, depicted on drawing 2.

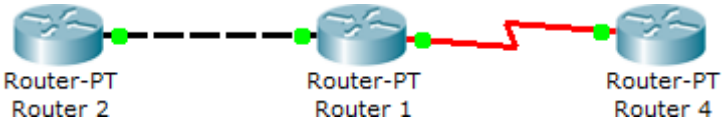


Figure 2.

Let's appoint addresses interfaces (mask 255.255.255.240) according to table. Not forget about it DCE device sequential connections ask synchronization.

	Router2	Router1	Router4
Etherne t	24.17.2.2	24.17.2.1	
Serial		24.17.2.17	24.17.2.18

We will make it happen configuration RIP routing

For Router1

Router1(config)# **router rip**
Router1(config- router)# **version 2**
Router1(config- router)# **network 24.0.0.0**
On Router2 Router2(config)#

router rip Router1(config-

router)# **version 2**

Router2(config- router)# **network 24.0.0.0**
And on Router4 Router4(config)#

router rip Router1(config-

router)# **version 2**

Router4(config- router)# **network 24.0.0.0**

Check it out my net With help teams ping And, V in particular, What You you canping interface Ethernet0 (24.17.2.2) router 2 of router 4

Router4# **ping 24.17.2.2**

Let's create a standard access list that will not allow pinging.router 2 from router 4. For this we block the only one address 24.17.2.18 router 4 And let's resolve the rest traffic. List let's create onrouter 2 teams

Router2(config)# **access-list 1 deny 24.17.2.18 0.0.0.0**
Router2(config)# **access-list 1 permit 0.0.0.0 255.255.255.255**

Let's apply list To interface Ethernet router 2Router2(config)#

interface FastEthernet0/0

Router2(config-if) **#ip access group 1 in**

Let's check, What list access launched. For this let's take a look workingconfiguration

Router2# **show running-config**

We we can also see that list applied To interface, using team“show IP interface”. Find V output information With line “Innbound access list is 1”.

Router2# **show IP interface**

Team “show access-lists” will show us content created list access.Router2# **show access lists**

```
Standard IP access list 1
    deny host 24.17.2.18
    permit any (4 match(es))
```

Let us note, What host 24.17.2.18 equivalent 24.17.2.18 0.0.0.0. Now at attemptping interface Ethernet0 (24.17.2.2) router 2 from router 4

Router4# **ping 24.17.2.2**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 24.17.2.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5), round-trip min/avg/max = 1/2/4 ms
```

We will receive line “UUUUU”, which means, What list access workscorrectly.

2. Let's create And let's load it in simulator topology on drawing 2,

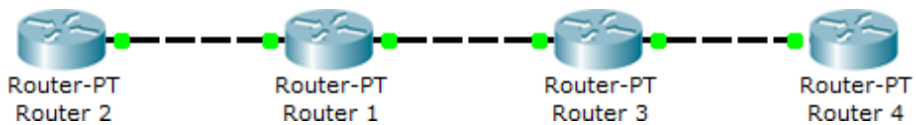


Figure 3.

Let's appoint addresses interfaces (mask 255.255.255.0) according to table

	Router2	Router1	Router3	Router4
Ethernet 0	160.10.1.2	160.10.1.1	175.10.1.2	180.10.1.2
Ethernet 1		175.10.1.1	180.10.1.1	

We will make it happen configuration OSPF routing

For Router1

Router1(config)# **router ospf 1**
Router1(config- router)# **network 160.10.1.0 0.0.0.255 area 0**
Router1(config- router)# **network 175.10.1.0 0.0.0.255 area 0**
For Router2 Router2(config)#

router ospf 1

Router2(config- router)# **network 160.10.1.0 0.0.0.255 area 0**
end
For Router3
Router3(config) # **router ospf 1**
Router3(config- router)# **network 175.10.1.0 0.0.0.255 area 0**
Router3(config- router)# **network 180.10.1.0 0.0.0.255 area 0**
For Router4
Router4(config) **#router ospf 1**
Router4(config- router)# **network 180.10.1.0 0.0.0.255 area 0**
For checks ping extreme pointsrouter2#ping

180.10.1.2

router4#ping 160.10.1.2

Let's create a standard access list to filter traffic coming to interface ethernet0 of router1 and allows traffic from subnet 175.10.1.0(router3) And blocks traffic from others devices.

router1(config)# **access-list 1 permit 175.10.1.0 0.0.0.255**
Check that it was created.

router1# **show access list**

```
Standard IP access list 1
    permit 175.10.1.0 0.0.0.255
```

Attach list How input To interface Ethernet 1router1(config)#

interface FastEthernet1/0

router1(config-if) **#ip access group 1**

inCheck it out accession team router1#

show running-config

Check it out connection between 3 And 2 routers And between 4 And 2 .
router3# **ping 160.10.1.2**
router4# **ping 160.10.1.2**
The connection between 3 And 2nd routers should be, A between 4 and 2 - No.

Let's change it list access And let's resolve traffic from subnets 180.10.1.0 (router4) And we block traffic from others devices.

router1(config)# **no access list 2**
router1(config)# **access list 2 permit 180.10.1.0 0.0.0.255**
Check it out, What He

changedrouter1# **show access-**

```
Standard IP access list 1
    permit 180.10.1.0 0.0.0.255
```

list

Attach list How input To interface Ethernet 1router1(config)#

interface FastEthernet1/0

router1(config-if) **#ip access group 1**

inCheck it out accession team router1#

show running-config

Check it out connection between 3 and 2 routers And between 4 and 2.
router3# **ping 160.10.1.2**
router4# **ping 160.10.1.2**
The connection between 4 And 2nd routers should be, A between 3 and 2 - No.

3. Make it happen And check configuration IP For networks on drawing 1 And apply OSPF For organizations dynamic routing.

For router 1router1(config)#

router ospf 1

router1(config-router)# **network 2.2.2.0 0.0.0.255 area 0**
router1(config-router)# **network 1.1.1.0 0.0.0.255 area 0**
router1(config-router)# **network 10.1.1.0 0.0.0.127 area 0**
For router 2Router2(config)#

router ospf 1

Router2(config-router)# **network 10.1.1.128 0.0.0.127 area 0**
Router2(config-router)# **network 15.1.1.0 0.0.0.255 area 0**
Router2(config-router)# **network 2.2.2.0 0.0.0.255 area 0**
Check it out performance networks: You should from any devices ping any interface. Or more simply: all computers A, B, C, D, PC5 must be mutually paired ping.

Let's create list access from theoretical parts
3.1 On Let's create router 1 list access router1(config)#

access-list 2 deny 10.1.1.128 0.0.0.127 router1(config)#

access-list 2 permit host 15.1.1.5 router1(config)# **access-**

list 2 deny 15.1.1.0 0.0.0.255 router1(config)# **access-list 2**

permit 0.0.0.0 255.255.255.255

And applicable his To interface Ethernet0 how day off

router1(config)# **interface FastEthernet0/0**

router1(config-if)# **ip access group 2 out**

Create screenshot result execution teamsrouter1# **show**

access list

In pairs let's ping A, B, C, PC5, D. IN result should it will work out nextaccess matrix

From\To	A	B	C	E	D
A	+	+	+	-	-
B	+	+	+	+	+
C	+	+	+	+	+
E	-	+	+	+	+
D	-	+	+	+	+

Table 1

We see, What policy security from theoretical parts fully implemented.

3.2 Let's delete it ACL c e0 interface And applicable How input To interface s0

router1(config)# **interface fa0/0**

router1(config-if) **#no IP access group 2 out**
router1(config-if) **#int s2/0**
router1(config-if) **#ip access group 2 in**

In pairs let's ping A, B, C, PC5, D. IN result should it will work out nextaccess matrix

From\To	A	B	C	E	D
A	+	+	+	-	-
B	+	+	+	-	-
C	+	+	+	+	+
E	-	-	+	+	+
D	-	-	+	+	+

Table 2

We see, What Now traffic between networks 10.1.1.0/25 And 10.1.1.128/25 prohibited. Traffic is also not possible between the 10.1.1.0/25 network and the 15.1.1.0/24 network except computer WITH With address 15.1.1.5.

4. We use topology And configuration point 1 this laboratory workLet's cancel

configuration access, made in paragraph 1

Router2(config)# **no access list 1 deny 24.17.2.18 0.0.0.0**
Router2(config)# **no access-list 1 permit 0.0.0.0**

255.255.255.255 Let's apply list To Ethernet interface of router 2

Router2(config)# **interface fa0/0**

Router2(config-if)# **no IP access group 1 in**

Let's resolve come in on router1 telnet on his two interface With password router1

Router1(config)# **line vty 0 4**

Router1(config-line)# **login**

Router1(config-line)# **password**

router1

Our EACL will be do couple various things. First We we will only resolve telnet from subnets sequential connections 24.17.2.16/240 For entrance on router1

router1(conf)# **access-list 101 permit tcp 24.17.2.16 0.0.0.15 any eq telnet log**

Option log will force router show exit at triggering listaccess.

Let's resolve on router router1 all traffic from Ethernet 0 subnets 24.17.2.0/240

router1(conf)# **access-list 102 permit IP 24.17.2.0 0.0.0.15 any**

Let's check the installation lists

router1#show access list

```
Extended IP access list 101
    permit tcp 24.17.2.16 0.0.0.15 any eq telnet log (0 matches)
Extended IP access list 102
    permit ip 24.17.2.0 0.0.0.15 any log (1 matches)
```

Now applicable lists To interfaces For incoming packagesrouter1(conf)#

interface Serial2/0

router1(conf-if)# **IP access group 101**

inrouter1(conf-if)# **interface fa0/0**

router1(conf-if)# **IP access group 102**

in

For checks, What EACL are present on interfaces, use teamrouter1# **show running-config**

or

router1# **show IP interface**

Let's check functioning EACL. Let's join to router4 And let's try unsuccessfully ping interface Serial2/0 on router1

router4# **ping 24.17.2.17**

EACL number 101 blocked ping. But must allow telnetrouter4# **telnet**

24.17.2.17

Successfully. Let's introduce password router1. Prompt router4# changed on router1>. By clicking simultaneously ctrl-shift-6 and then 6, let's return to router4. About the triggering of EACL 101 on router1 us will indicate log

```
00:06:50:  %SEC-6-IPACCESSLOGDP: list 101 permitted TCP 24.17.2.18 -> 24.17.2.17 (8/0), 5 packets
```

Let's see number sessions And we'll kill telnet

compoundrouter4# **show sess**

router4# **disconnect 1**

Let's join to router2 And We'll see, Can whether We ping interfaceSerial0 on router4.

Router2# **ping 24.17.2.18**

Why unsuccessfully? Plastic bag starts V Router2, is coming through Router1 (O triggeringEACL 102 on router1 us will indicate log

```
00:03:29:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 24.17.2.18 (8/0), 5 packets
```

) and arrives at Router4. On Router4, it is reformatted and sent back to Router1. When Router4 reshapes the packet, the source address becomes the destination address and address receiver becomes address source. When plastic bag comes on interface Serial0 on router1 is rejected because its source address is equal to the interface IP address. Serial0 on router4 24.17.2.17, A Here allowed only tcp.

Let's join to router2 And We'll see, Can whether We ping interfaceEthernet0 on router1.

router2# **ping 24.17.2.1**

Successfully. Likewise And For telnet

router2# **telnet 24.17.2.1**

EACL are working successfully. ABOUT triggering EACL 102 on router1 us will indicate log.

```
00:05:22:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 24.17.2.1 (8/0), 5 packets
```

Note, what's the log? So same constantly shows RIP updates

```
00:06:42:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 255.255.255.255 (8/0), 5 packets
00:06:12:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 255.255.255.255 (8/0), 5 packets
00:07:42:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 255.255.255.255 (8/0), 5 packets
00:07:12:  %SEC-6-IPACCESSLOGDP: list 102 permitted IP 24.17.2.2 -> 255.255.255.255 (8/0), 5 packets
```

5. Named ACL

Let's cancel on router1 binding EACL To interfaces

router1(conf)# **interface Serial0**

router1(conf-if)# **no IP access group 101**

inrouter1(conf-if)# **interface Ethernet0**

router1(conf-if)# **no ip access-group 102**

inAnd let's cancel on router1 EACL

router1(conf)# **no access list 101**

router1(conf)# **no access list 102**

Let's set the task to prohibit only pings from router4 to router2 throughout the entire network. List Access can be placed on both router1 and router2. Although it is recommended to place ACLscloser to the source (to reduce traffic), in this example we will place the named list With name deny_ping on router2.

router2(config)# **ip access list extended deny_ping**

router2(config-ext-nacl)# **deny icmp 24.17.2.18 0.0.0.0 24.17.2.2 0.0.0.0 log**

router2(config- ext-nacl)# **permit ip any any log**

First team indicates, What We we create named extended list access command named deny_ping. The second command specifies that ICMP traffic is prohibited from address source strictly 24.17.2.18 And address receiver strictly 24.17.2.2. Third the team allows the rest IP traffic.

Let's check the list creation

router2# **show access list**

```
Extended IP access list deny_ping
    deny   icmp host 24.17.2.18 host 24.17.2.2 log (0 matches)
    permit ip any any log (0 matches)
```

That's right, we see in the first line just a different form of presentation.teams deny icmp 24.17.2.18 0.0.0.0 24.17.2.2 0.0.0.0 log.

Let's apply list For input traffic interface Ethernet0 on router2Router2(conf)# **interface Ethernet0**

Router2(conf-if)# **ip access-group deny_ping in** Let's join To

router4 And let's ping router 2router4# **ping 24.17.2.2**

Failure. Let's join To router1 And let's ping router2Router1#

ping 24.17.2.2

Success. Let's join To router2 and We'll see on two separate log messages:first O prohibition ping from router4 And second O resolution ping from router1

```
00:11:18:  %SEC-6-IPACCESSLOGDP: list 0 permitted IP 24.17.2.1 -> 24.17.2.2 (8/0), 5 packets
00:12:30:  %SEC-6-IPACCESSLOGDP: list 0 permitted IP 24.17.2.1 -> 255.255.255.255 (8/0), 5 packets
```

6. Let's consider more difficult questions extended lists access. Let's createtopology

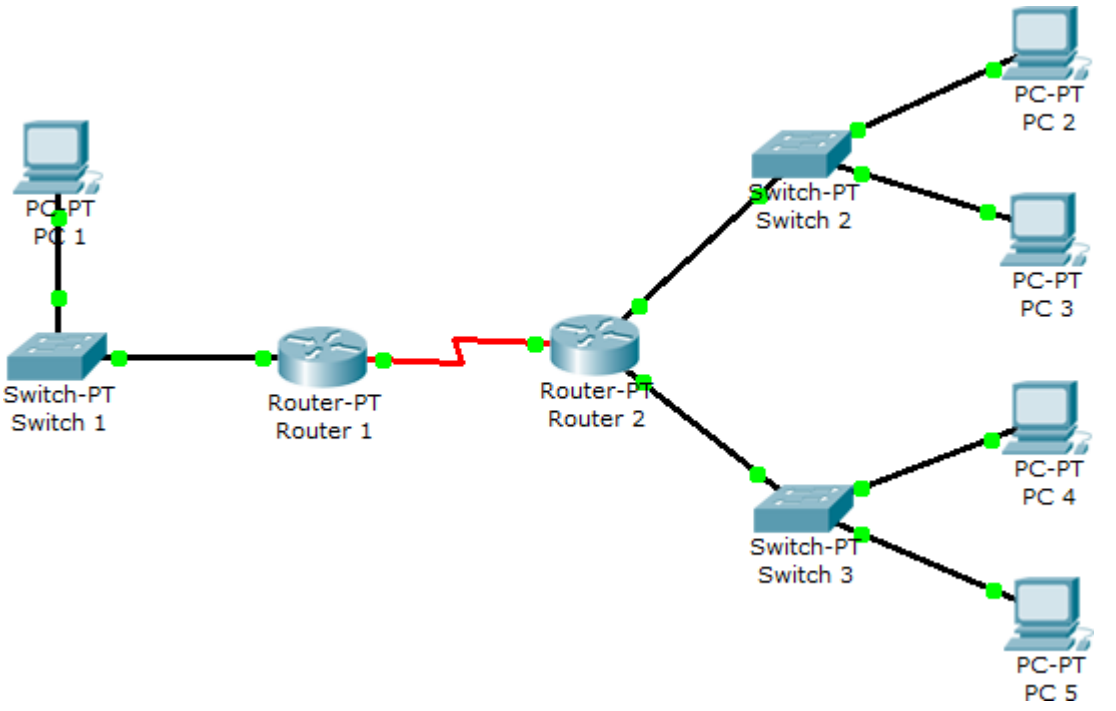


Figure 4.

Use switches models 1912. Router Router1 - models 805. Router Router2 - models 1605.

Let's appoint IP addresses routers

	Router1	Router2
Fa0/0	1.1.3.1/24	1.1.1.129/25
Fa1/0		1.1.1.1/25
Serial2/0	1.1.2.1/24	1.1.2.2/24

And computers

Hostname	IP on ethernet0	Gateway
PC1	1.1.3.2 255.255.255.0	1.1.3.1
PC2	1.1.1.130 255.255.255.128	1.1.1.129
PC3	1.1.1.131 255.255.255.128	1.1.1.129
PC4	1.1.1.2 255.255.255.128	1.1.1.1
PC5	1.1.1.3 255.255.255.128	1.1.1.1

On Router1 And Router2 we configure RIP

Router(config)# **router rip**

Router(config-router)# **network 1.0.0.0**

Interfaces everyone devices should ping with everyone devices.

6.1. List access network-network.

Let's create a list that allows traffic from the local network of computers PC4 and PC5 V local net computer PC1 And prohibits traffic from local networks computers PC2 and PC3 to the local network of computer PC1. Since the traffic comes from router2 to router1 , then you should place an access list on the serial2/0 interface of router1 for input traffic

Router1(conf)# **access-list 100 permit ip 1.1.1.0 0.0.0.127 1.1.3.0 0.0.0.255 log**

Router1(conf)# **access-list 100 permit IP 1.1.2.0 0.0.0.255 any log**

The first team directly solves the given problem, and the second one solves it broadcasting RIP protocols. Let's check Creation

Router1# **show access list**

```
Extended IP access list 100
    permit ip 1.1.1.0 0.0.0.127 1.1.3.0 0.0.0.255 log (0 matches)
    permit ip 1.1.2.0 0.0.0.255 any log (11 matches)
```

Let's apply list access To interface.

Router1(conf)# interface Serial2/0

Router1(conf-if)# ip access group 100 in

For testing list access, try ping PC1 from PC2, PC3, PC4And PC5.

PC# **Ping 1.1.3.2**

Pings won't work for PC2 and PC3. Pings will work for PC4 and PC5. Access list works. Take a look logs on router1

```
01:31:39:  %SEC-6-IPACCESSLOGDP: list 100 permitted IP 1.1.1.2 -> 1.1.3.2 (8/0), 5 packets
```

.

6.2. List access host-host.

Let's create on router2 list access, which blocks access To PC5 only With PC2. Control attempts access Can By logs on router2.

Router2(conf)# **access-list 101 deny IP 1.1.1.130 0.0.0.0 1.1.1.3 0.0.0.0 log**

Router2(conf)# **access-list 101 permit ip any any**

Let's check Creation

Router2# **show access**

```
Extended IP access list 101
    deny ip host 1.1.1.130 host 1.1.1.3
    permit ip any any
```

list

Let's apply list access To fast Ethernet interface router2Router2(conf)# **interface**

FastEthernet0/0

Router2(conf-if)# **ip access group 101 in**

Join us To PC2 And check, What You Not you can kick PC5PC2# **Ping**

1.1.1.3

On router2 will appear log

```
01:51:44:  %SEC-6-IPACCESSLOGDP: list 101 denied IP 1.1.1.130 -> 1.1.1.3 (8/0), 5 packets
```

Join us To PC3 And check, What You you can kick PC5.

PC3# **Ping 1.1.1.3**

On router2 will appear log

```
01:54:41:  %SEC-6-IPACCESSLOGDP: list 101 permitted IP 1.1.1.131 -> 1.1.1.3 (8/0), 5 packets
```

6.3. List access network-host.

In the beginning let's delete previous lists access With interfaces Router1 And Router2.

Router1(conf)# **interface Serial2/0**

Router1(conf-if)# **no IP access group 100 in**

And

Router2(conf)# **interface FastEthernet0/0**

Router2(conf-if)# **no IP access group 101 in**

Let's create an extended access list that blocks all traffic to PC1 from local network of computers PC2 and PC3. Since we are blocking all traffic, we will use IP protocol.

Router2(conf)#access-list 102 deny IP 1.1.1.128 0.0.0.127 1.1.3.2 0.0.0.0

logRouter2(conf)#access-list 102 permit IP any any

Let's check Creation

Router2# **show access**

```
Extended IP access list 102
    deny ip 1.1.1.128 0.0.0.127 host 1.1.3.2
    permit ip any any
```

list

Let's apply list To outgoing traffic on interface Serial2/0 Router2

Router2(conf)# **interface Serial2/0**

Router2(conf-if)# **ip access group 102 out**

To check the list, try pinging PC1 (1.1.3.2) from PC2 and PC3. Pings They won't work. For some reason, the simulator doesn't log anything on the Router2 console. But you can see the effect. see So

```
Router2#sh ac
Extended IP access list 102
    deny ip 1.1.1.128 0.0.0.127 host 1.1.3.2 (8 match(es))
    permit ip any any

Router2#sh ac
Extended IP access list 102
    deny ip 1.1.1.128 0.0.0.127 host 1.1.3.2 (16 match(es))
    permit ip any any
```

You you see after each unsuccessful ping quantity tracked (matches) packages is increasing.

Control questions

1. What's happened ACL?
2. Which address is criterion For permissions/prohibitions package?
3. Where are applied ACL?
4. How ask element ACL And What such inverse mask?

5. How router processes elements ACL?
6. Which element Always implicitly present in ACL?
7. How ACL apply To interface And then cancel it?
8. How is different input ACL from day off?
9. Where V networks recommended place ACL?
10. What kind three teams Can check content ACL And binding Tointerface.
11. What filter extended ACL?
12. Which one? additional functionality have extended ACL By comparison with standard?
13. Can whether, using advanced ACL, impose restrictions on traffic Tocertain TCP/IP service?
14. Describe procedure creation named ACL.
15. How edit specific line V numerical ACL?
16. How edit specific line V named ACL?
17. How is different formats teams For input elements numerical And namedACL?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute contract three point practical parts. Check access according toTable 1, A then table 2.
4. Show to the teacher, What net satisfies matrix access from tables 1.
5. Show to the teacher, What net satisfies matrix access from tables 2.
6. Do it V Packet Tracer exercise For independent work.
7. Build your own access matrix according to option and show to the teacher,What net satisfies this matrix.
8. Make out report. Content report Look below.
9. Protect report.

Exercise For independent work

1. Apply list access 2, created V point 3 practical parts, according tooption

Variant	Router	Interface	Input/output
1	router 1	E0	in
2	router 1	S0	out
3	router 1	E1	in
4	router 1	E1	out
5	router 2	E0	in
6	router 2	E0	out
7	router 2	S0	in

8	router 2	S0	out
9	router 2	E1	in
10	router 2	E1	out

2. Create screenshot result execution teamsrouter1#

show access list

And

router1# **show running-config**

3. Build matrix access.
4. Do it three subparagraph point 6 practical parts For topology ondrawing 4 And your own version **v** configurations, given V table

	Router1	Router2
Fa0/0	1.v.3.1/24	1.v.1.129/25
Fa0/1		1.v.1.1/25
Serial0	1.v.2.1/24	1.v.2.2/24

Hostname	IP on Ethernet	Gateway
PC1	1.v.3.2 255.255.255.0	1.v.3.1
PC2	1.v.1.130 255.255.255.128	1.v.1.129
PC3	1.v.1.131 255.255.255.128	1.v.1.129
PC4	1.v.1.2 255.255.255.128	1.v.1.1
PC5	1.v.1.3 255.255.255.128	1.v.1.1

Do it those same screenshots, which made V paragraph 6 practical parts.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshots topologies, created at execution practical parts.
2. All screenshots, created at execution practical parts.
3. Configurations everyone routers from .txt files configurations, created atexecution practical parts.
4. Configuration routers from .txt files, created at executionparagraph 1 tasks For independent work.
5. Matrix access, specified V paragraph 3 tasks For independent work.
6. Configuration routers from .txt files, created at executionparagraph 4 tasks For independent work.
7. All screenshots, specified V task For independent work.

Practical class №12. Network Layer Protocols (Part 3).

Theoretical Part

Network address translation (NAT) is designed to simplify and concealment IP addressing. NAT allows introduce external to the world internal structure IP addressing enterprises otherwise, how she on itself case looks like. This permits organizations unite With Internet, Not having inside myself global unique IP addressing. This provides Internet access for corporate internal IP networks With internal IP addresses (intranet), which globally are non-unique and therefore cannot be routed on the Internet. NAT is used Also For connections territorially distributed divisions organizations through Internet.

The following ranges have been allocated by the global community for Intranet addressing: addresses

Class A: 10.0.0.0-10.255.255.255
Class B: 172.16.0.0-172.16.255.255
Class C: 192.168.1-192.168.255.255

NAT translates the internal IP address from the internal address space to IP address in external address space. When NAT receives plastic bag from intranet, He changes the source address in it, recalculates the checksum and sends it to Internet.

NAT translates and maps addresses from one area to another. This ensures transparent routing from node To node. IN NAT exists some ways broadcasts addresses, used in various private cases.

Cisco uses For NAT specific terminology For nodes V intranet And Internet How before and after transformations addresses:

Inside address. The address used within an organization. Different organizations can have the same internal addresses.

External address (outside). An address defined somewhere outside the given organization. External address other organizations Maybe coincide With internal address this organizations.

Global address. This is a registered and legal IP address that can pass through Internet.

Local address. Address IP, used internally V Intranet. These addresses Not cross Internet addresses and That's why are being considered How local.

Inside local address. The address used within the organization, not crossing the Internet addresses.

Inside global address. The address used within an organization, being Internet address.

Outside local address. An address defined somewhere outside the given organizations, Not being Internet address.

External global address (outside global). Address, definite somewhere outside this organizations, being Internet address.

The simulator always shows that the Outside Local address is always equal external global address (outside global).

When sending packets from an internal host interface, NAT replaces the address in it source to some global address. When receiving the response packet, NAT replaces it in him global address receiver (address external interface local router) on address interface internal host. For such replacements router supports special tables transformations addresses, which are constantly updated. There are three methods of address translation: static, dynamic and overload. With static NAT, explicitly using IOS commands specify pairs of internal_address - global_address. When dynamically When converting global addresses, they are taken from a specific pool of external addresses. overload All internal addresses, subject transformation, are replaced on the only one global external address router interface.

To configure NAT, you must define internal and external IP addresses on the router. external networks using **the ip nat inside | outside commands** . This command is defined on interface level, that is, in the context of the **interface command** . Additional commands depend from used type NAT. This or exercise static NAT, or defining a pool of external addresses or setting a command for overloading. As a rule, should also be asked access control list ACL to define internal traffic that will be transformed. The ACL itself does not perform any NAT transformations.

Let us also dwell on overload, which is usually called PAT. (Port Address Translation - address translation using ports). PAT allows multiple internal hosts to use one global address. One option PAT implementation is based on the use of a sequence of free TCP and UDP ports And consists of V next.

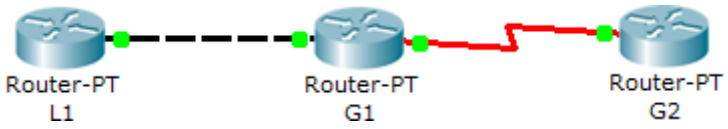
The NAT service is located on router M with inside global address X. Let there be a packet P from the internal local address Yi and port Pi to the external addressG And port p. Plastic bag passes through routerM. NAT replaces V him address Yi source And source port Pi internal hosta on unique a couple of X:Pinew, Where Pinnew
– the next free port number. The row (Yi: Pi, X: Pinew, G:p) is entered into the table. NAT of router M. The response packet will contain X in the receiver address field, and in The destination port field is Pinew. The source port address field will be G:p. Router M by the values X, Pinew, G, p finds in its NAT table the row (Yi:Pi , X: Pinew, G:p) and replaces the receiver address in the packet X on Yi, and the destination port Pinew on Pi. Response The packet will arrive at the desired address Yi with the desired destination port Pi. Port Pinew is coming back V list free ports.

The NAT process is transparent to internal addresses. So, a host with an internal address Yi,sent plastic bag in external world And received answer "Not guesses", What plastic bag

passed NAT transformation on the router both when sending and when receiving. The internal host appears to have direct access to the external host. world.

Practical Part.

1. Download V simulator topology depicted on drawing.



Drawing 1

Create configuration

	L1	G1	G2
Ethern	10.10.1.2 255.255.255.0	10.10.1.1 255.255.255.0	
Serial		175.10.1.1 255.255.255.0	175.10.1.2 255.255.255.0

Ask OSPF routing to G1G1(config)#

router ospf 1

G1(config- router)# **network 10.10.1.0 0.0.0.255 area 0**
G1(config-router)# **network 175.10.1.0 0.0.0.255 area 0**
On L1
L1 (config)# **router ospf 1**
L1 (config- router)# **network 10.10.1.0 0.0.0.255 area 0**
For G2
G2 (config)# **router ospf 1**
G2(config-router)# **network 175.10.1.0 0.0.0.255 area 0**
On G2 is solvable entrance via Telnet With

password G2G2 (config)# **line vty 0 4**

G2 (config-line)# **login**
G2 (config-line)# **password G2**

Check it out performance networks With help teams ping. Check it out Telnet-compound from L1 (10.10.1.2) To G2

L1# **telnet 175.10.1.2**

Password : **G2** G2>

show users

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:01:18
* 67 vty 0                 idle                 00:00:00 10.10.1.2
```

Exit telnet: ctrl+shift+6 then **x** . Close telnet sessions with the command disconnect on L1 And G2.

Necessary tune NAT/PAT on router G1. Need to tune three forms of address translation: statistical translation of network addresses, dynamic translation And overload (translation addresses ports). We assume, What net Ethernet 10.10.1.0/24 This

an internal intranet network that connects to the outside world via G1, namely via net 175.10.1.0/24 sequential interface.

1.1 On router G1 we will configure NAT for static translation of internal local Ethernet address of router L1 10.10.1.2 to the new internal global address 169.10.1.2, available at organizations:

G1(config)#ip nat inside source static 10.10.1.2 169.10.1.2 Let's

define net fastEthernet0/0 interface How internal

G1(config)#interface fa0/0

G1(config-if)# IP nat inside

Let's define net serial 2/0 interface How external

G1(config-if)#interface s2/0

G1(config-if#ip nat outside

For conclusion tables translations addresses enter team on routerG1# **show IP nat translations**

```
Pro  Inside global     Inside local       Outside local      Outside global
---  169.10.1.2        10.10.1.2          ---                ---
```

Test the translation by creating a Telnet connection from L1 to G2. Telnet into G2enter team show users. You should see translated IP address 169.10.1.2.

L1# telnet 175.10.1.2

Password: **G2**

G2> show users

```
    Line      User       Host(s)                Idle Location
*   0 con 0                 idle                00:00:00
*   1 vty 1                 idle                169.10.1.2
```

Instead of 169.10.1.2 Can use And involved address interfaceSerial2/0 G1 175.10.1.1

G1(config)# **no IP nat inside source static 10.10.1.2 169.10.1.2**G1(config)# **ip nat inside source static 10.10.1.2 175.10.1.1** L1# **telnet 175.10.1.2**

Password : **G2**

G2> **show users**

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:03:49
 * 67 vty 0                 idle                 00:00:00 175.10.1.1
```

1.2. On router G1 delete previous NAT command statisticaltranslation

G1(config)# **no IP nat inside source static 10.10.1.2 175.10.1.1**

And set up NAT For dynamic translation Ethernet addresses router L1.We use region addresses V range: 169.10.1.50 - 169.10.1.100. Let's define pool addresses **pool1**

G1(config)# **ip nat pool pool1 169.10.1.50 169.10.1.100 netmask 255.255.255.0**

Let's ask NAT transformation addresses from list 1 V pool addresses **pool1**

G1(config)# **ip nat inside source list 1 pool pool1**

Let's set it up And let's check list access 1 For internal addresses, which will be transform

G1(config)# **access-list 1 permit 10.10.1.0 0.0.0.255**

^Z

G1# **Show access list**

Necessarily With help teams show running-config check, What routerG1 picked up introduced teams. Among conclusion should be

```
!
ip nat pool pool1 169.10.1.50 169.10.1.100 netmask 255.255.255.0
ip nat inside source list 1 pool pool1
ip classless
!
!
access-list 1 permit 10.10.1.0 0.0.0.255
!
```

Test the translation by creating a Telnet connection from L1 to router G2. Log in using Telnet to G2 and enter the show users command. You should see the translated IP address. 169.10.1.50.

L 1# **telnet 175.10.1.2**

Password : **G 2**

G 2> **show**

```
    Line      User       Host(s)              Idle Location
*   0 con 0                idle                 00:00:00
*   1 vty 1                idle                 169.10.1.50
users
```

That There is NAT took from pool addresses first free address 169.10.1.50.

To display the address translation table, enter the show ip nat translations command on router G1.

```
Pro  Inside global     Inside local       Outside local      Outside global
tcp 169.10.1.50:1025   10.10.1.2:1025     175.10.1.2:23      175.10.1.2:23
tcp 169.10.1.50:1026   10.10.1.2:1026     175.10.1.2:23      175.10.1.2:23
tcp 169.10.1.50:1027   10.10.1.2:1027     175.10.1.2:23      175.10.1.2:23
tcp 169.10.1.50:1028   10.10.1.2:1028     175.10.1.2:23      175.10.1.2:23
tcp 169.10.1.50:1029   10.10.1.2:1029     175.10.1.2:23      175.10.1.2:23
```

1.3 On router G1 delete previous NAT commands dynamic translation And set up overload (translation addresses ports) Ethernet addresses router L1 (10.10.1.2) on address interface serial2/0 (175.10.1.1) on router G1.

G1(config)# **no ip nat pool pool1 169.10.1.50 169.10.1.100 netmask 255.255.255.0**

G1(config)# **no nat inside source list 1 pool pool1**

G1(config)# **ip nat inside source list 1 interface s2/0 overload**

Necessarily With help teams show running-config check, What routerG1 picked up introduced teams. Among conclusion should be

```
!
ip nat inside source list 1 interface Serial2/0 overload
ip classless
!
!
access-list 1 permit 10.10.1.0 0.0.0.255
!
```

Test the translation by creating a Telnet connection from L1 to router G2. While On router G2, enter the show users command. You should see the translated IP address 175.10.1.1.

L 1# **telnet 175.10.1.2**
Password : **G 2**
G 2> **show**

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:34
* 67 vty 0                 idle                 00:00:00 175.10.1.1
```

users

List the NAT translations on router G1. G1#show IP nat translations

```
Pro  Inside global     Inside local       Outside local      Outside global
tcp 175.10.1.1:1025    10.10.1.2:1025     175.10.1.2:23      175.10.1.2:23
tcp 175.10.1.1:1026    10.10.1.2:1026     175.10.1.2:23      175.10.1.2:23
tcp 175.10.1.1:1027    10.10.1.2:1027     175.10.1.2:23      175.10.1.2:23
tcp 175.10.1.1:1028    10.10.1.2:1028     175.10.1.2:23      175.10.1.2:23
tcp 175.10.1.1:1029    10.10.1.2:1029     175.10.1.2:23      175.10.1.2:23
```

2. Create topology. Models routers L1, L2, G1 And G2 -805, A LG And G - 1605.

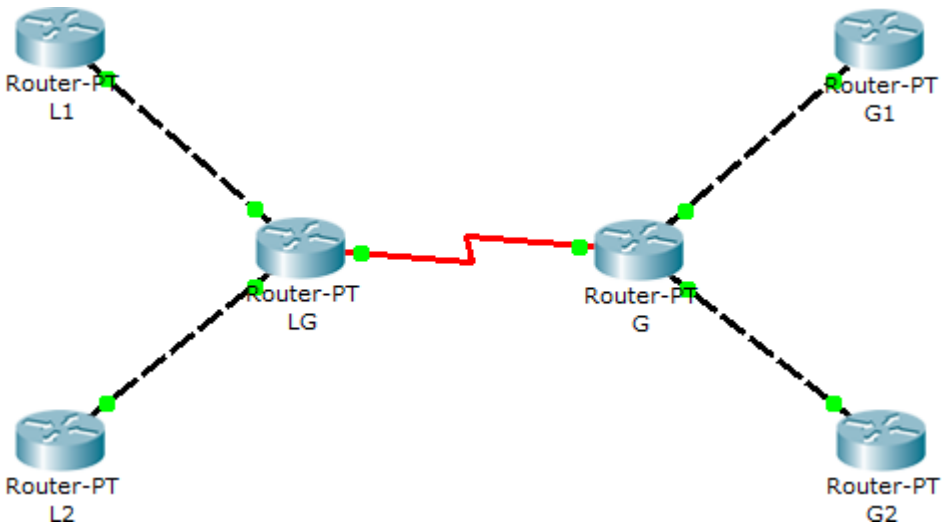


Figure 2

Let's configure addresses according to tables. All masks 255.255.255.0

	L1	L2	LG	G	G1	G2
Eth0	10.1.1.2		10.1.1.1	1.1.2.1	1.1.2.2	
Eth1		10.1.2.2	10.1.2.1	1.1.3.1		1.1.3.2
serial			1.1.1.1	1.1.1.2		

Let's set it up OSPF routing

LG(config)# **router ospf 1**
LG(config-router)# **network 1.1.1.0 0.0.0.255 area 10**
LG(config-router)# **network 10.1.1.0 0.0.0.255 area 10**
LG(config-router)# **network 10.1.2.0 0.0.0.255 area 10**

G(config)# **router ospf 1**
G(config-router)# **network 1.1.1.0 0.0.0.255 area 10**
G(config-router)# **network 1.1.2.0 0.0.0.255 area 10**
G(config-router)# **network 1.1.3.0 0.0.0.255 area 10**

L1(config)# **router ospf 1**
L1(config-router)# **network 10.1.1.0 0.0.0.255 area 10**

L2(config)# **router ospf 1**
L2(config-router)# **network 10.1.2.0 0.0.0.255 area 10**

G1(config)# **router ospf 1**
G1(config-router)# **network 1.1.2.0 0.0.0.255 area 10**

G2(config)# **router ospf 1**
G2(config-router)# **network 1.1.3.0 0.0.0.255 area 10**

And let's allow telnet on G1 And

G2:G1(config)# **line vty 0 4**
G1(config-line)# **login**
G1(config-line)# **password**
G1

G2(config)# **line vty 0 4**
G2(config-line)# **login**
G2(config-line)# **password**
G2

Check it out functioning: come in telnet from L1 on G1, from L1 on G2, from L2 onG1, from L2 on G2.

Be sure to kill all telnet sessions with the **disconnect 1 command** . In total, you will need8 teams. By two on each device: L1, L2, G1 And G2.

Check it out absence telnet connections team **show session.**

Announce on router LG networks 10.1.1.0/24 and 10.1.2.0/24 How internal, A net 1.1.1.0/24 How external

LG(config)# **interface s2/0**

LG(config-if)# **ip nat outside**

LG(config-if)# **interface**

fa0/0LG(config-if)# **ip nat**

inside LG(config-if)#

interface fa1/0LG(config-if)#

ip nat inside

Let's create list access For addresses two internal Ethernet networks

LG(config)# **access-list 2 permit 10.1.0.0 0.0.255.255**

AND let's launch PAT transformation these addresses on interior global address 1.1.1.1 interface Serial2/0

LG(config) **#ip nat inside source list 2 interface s2/0 overload**

Check functionality: Telnet from L1 to G1L1# **telnet 1.1.2.2**

Password: **G1**

G1> **show users**

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:08:20
 * 67 vty 0                 idle                 00:00:00 1.1.1.1
```

Go out from telnet sessions, by clicking Ctrl-Shift-6

then x.Log in via telnet from L1 on G2

L1# **telnet 1.1.3.2**

Password : **G2**

G2> **show users**

```
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:09:55
 * 67 vty 0                 idle                 00:00:00 1.1.1.1
```

Exit the telnet session by pressing Ctrl-shift-6 then x. Let's

move on on L2 device. Come in telnet from L2 on G1L2#

telnet 1.1.2.2

Password:

G1G1> **sh**

us

```
    Line       User       Host(s)              Idle       Location
  67 vty 0                idle                 00:03:56 1.1.1.1
* 68 vty 1                idle                 00:00:00 1.1.1.1
```

Go out from telnet sessions, by clicking Ctrl-Shift-6

then x.Log in via telnet from L2 on G2

L2# **telnet 1.1.2.2**

Password : **G2**

G2> **sh us**

```
    Line       User       Host(s)              Idle       Location
  67 vty 0                idle                 00:04:36 1.1.1.1
* 68 vty 1                idle                 00:00:00 1.1.1.1
```

We we see And on G1 And on G2 By two telnet sessions. All four sessions shown Howsessions from one addresses - internal global addresses 1.1.1.1 interface Serial2/0.

Let's move on on LG. Let's see four broadcasts addresses

LG# **show ip nat tr**

```
Pro  Inside global     Inside local       Outside local      Outside global
icmp1.1.1.1:9392       10.1.1.2:9392      1.1.2.2:9392       1.1.2.2:9392
icmp1.1.1.1:9393       10.1.1.2:9393      1.1.2.2:9393       1.1.2.2:9393
icmp1.1.1.1:9394       10.1.1.2:9394      1.1.2.2:9394       1.1.2.2:9394
icmp1.1.1.1:9395       10.1.1.2:9395      1.1.2.2:9395       1.1.2.2:9395
icmp1.1.1.1:9396       10.1.1.2:9396      1.1.2.2:9396       1.1.2.2:9396


icmp1.1.1.1:9392       10.1.1.2:9392      1.1.3.2:9392       1.1.3.2:9392
icmp1.1.1.1:9393       10.1.1.2:9393      1.1.3.2:9393       1.1.3.2:9393
icmp1.1.1.1:9394       10.1.1.2:9394      1.1.3.2:9394       1.1.3.2:9394
icmp1.1.1.1:9395       10.1.1.2:9395      1.1.3.2:9395       1.1.3.2:9395
icmp1.1.1.1:9396       10.1.1.2:9396      1.1.3.2:9396       1.1.3.2:9396


icmp1.1.1.1:9392       10.1.2.2:9392      1.1.2.2:9392       1.1.2.2:9392
icmp1.1.1.1:9393       10.1.2.2:9393      1.1.2.2:9393       1.1.2.2:9393
icmp1.1.1.1:9394       10.1.2.2:9394      1.1.2.2:9394       1.1.2.2:9394
icmp1.1.1.1:9395       10.1.2.2:9395      1.1.2.2:9395       1.1.2.2:9395
icmp1.1.1.1:9396       10.1.2.2:9396      1.1.2.2:9396       1.1.2.2:9396


icmp1.1.1.1:9392       10.1.2.2:9392      1.1.3.2:9392       1.1.3.2:9392
icmp1.1.1.1:9393       10.1.2.2:9393      1.1.3.2:9393       1.1.3.2:9393
icmp1.1.1.1:9394       10.1.2.2:9394      1.1.3.2:9394       1.1.3.2:9394
icmp1.1.1.1:9395       10.1.2.2:9395      1.1.3.2:9395       1.1.3.2:9395
icmp1.1.1.1:9396       10.1.2.2:9396      1.1.3.2:9396       1.1.3.2:9396
```

Order broadcasts corresponds order input teams **telnet**

First portion broadcasts corresponds teamL1# **telnet**

1.1.2.2

Second portion broadcasts corresponds teamL1#

telnet 1.1.3.2

Third portion broadcasts corresponds team

L2# **telnet 1.1.2.2**
The fourth portion broadcasts corresponds teamL2#

telnet 1.1.3.2

In everyone cases is used interior global address 1.1.1.1 interfaceSerial2/0.

Control questions

1. Which tasks decides NAT.
2. How connected problem shortages IP addresses And NAT?
3. Which You you know ranges for Intranet addressing?
4. What's happened interior address?
5. What such external address?
6. What such global address?
7. What such local address?
8. What such interior local address?
9. What such interior global address?
10. What such external global address?
11. What such external local address?
12. Name it three method transformations addresses.
13. Explain How works PAT.
14. What functionality is lost on a host with an internal local address in network that has a connection to the outside world through NAT, compared to a host with global address?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute contract All points practical part.
4. Create All screenshots, given V practical parts.
5. Show to the teacher result execution last one teams **show IP nattr** from points 1 And 2 practical parts.
6. Do it V Packet Tracer exercise For independent work.
7. Show to the teacher result execution last one teams **show IP nattr** from points 1 And 2 tasks For independent work.
8. Make out report. Content report Look below.
9. Protect report.

Exercise For independent work

1. Do it paragraph 1 practical parts For topology on drawing 1 And his ownoptions **v** configurations, given V table

	L1	G1	G2
Ethern	10.10. **v** .2 255.255.255.0	10.10. **v** .1 255.255.255.0	
Serial0		175. **v** .1.1 255.255.255.0	175. **v** .1.2 255.255.255.0

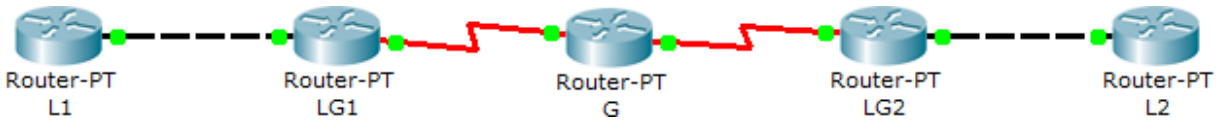
Do it those same screenshots, which made V paragraph 1 practical parts.

2. Do it point 2 practical parts for topology in the picture 2 and your ownoptions **v** configurations, given V table

	L1	L2	LG	G	G1	G2
Eth0	10. **v** .1.2		10. **v** .1.1	1. **v** .2.1	1. **v** .2.2	
Eth1		10. **v** .2.2	10.1.2.1	1. **v** .3.1		1. **v** .3.2
serial			1. **v** .1.1	1. **v** .1.2		

Do it those same screenshots, which made V paragraph 2 practical parts.

3.1. Create topology



3.2. Let's configure addresses according to tables. All masks 255.255.255.0. **v** - number options.

	L1	LG1	G	LG2	L2
Serial0		1. **v** .1.2	1. **v** .1.1		
Serial1			1. **v** .2.1	1. **v** .2.2	
Ethernet	10. **v** .1.2	10. **v** .1.1		10. **v** .1.1	10. **v** .1.2

We see exactly the same addresses for two Ethernet networks. Thus, we we simulate a real situation where network devices L1 and L2 of two different firms have the same local internal addresses 10. **v** .1.2 and are connected to the external peace (G) through routers LG1 And LG2, having NAT.

3.3. Allow me access By telnet to router G.

3.4. Please provide a demonstrable answer to the question: is it possible to set this up in the simulator? routing And NAT, to router L1 (L2) entered By telnet on router G under global internal address 1. **v** .1.2 (1. **v** .2.2). Answer (positive or negative) provide contents rtr files Andscreenshots.

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshots topologies, created at execution practical parts.
2. All screenshots, created at execution practical parts.
3. Configurations everyone from .txt files, created during execution practicalparts.
6. Configuration of routers from .txt configuration files created duringexecution For independent work.
7. All screenshots, specified V task For independent work.

Practical class №13. Network Layer Protocols (Part 4).

Remote access

There are three type sequential channels connections:

1. Networks With switching channels: dial-up telephone net, ISDN.

2. Selected or rented channels: DSL, cable modems And channels connectionstype 64k, T1, T3, OS-12,

3. Networks With switching packages: Frame Relay, X.25 And ATM.

Broadcast data Maybe be carried out How synchronously, So And asynchronously. Rented highlighted channels usually require synchronous sequential connections.

Each one line connections connected With consistent port router CSU/DSU (channel service unit/data service unit) device channel/ device service data).

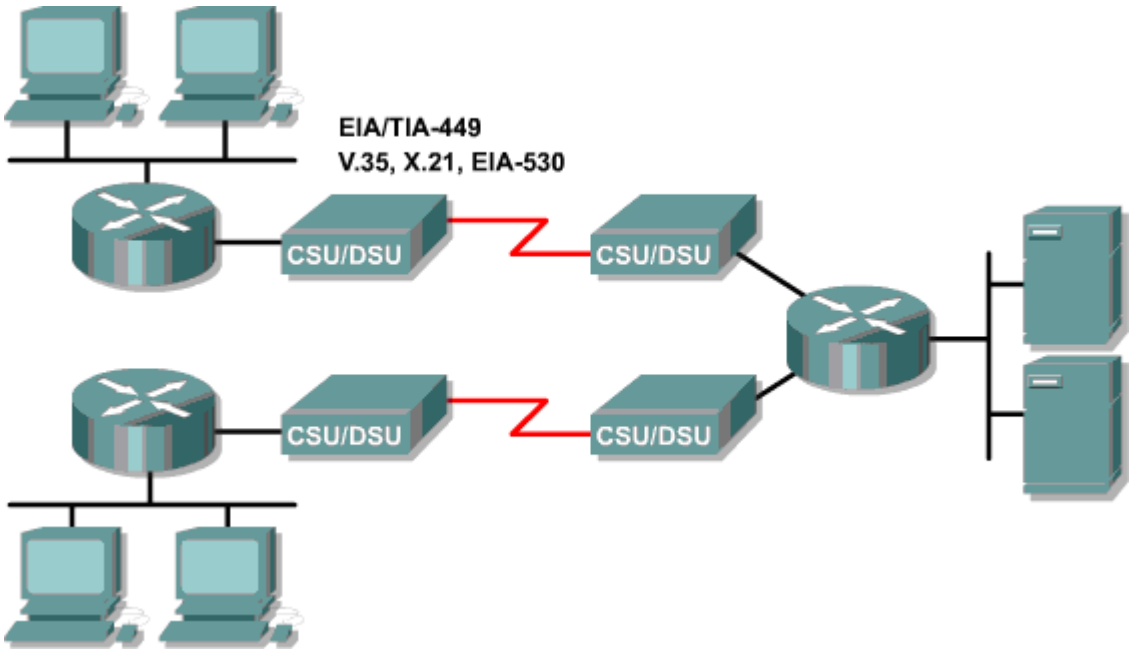


Figure 1.

Hence, besides actually wires from the communication provider, each compound requires separate synchronous consistent port on router And device CSU/DSU. How result, price contents of several dedicated lines increases sharply. Therefore, most companies find construction fully connected WAN on allocated lines too much expensive solution.

CSU/DSU is DCE (data communications equipment) - transmission equipment data) device. DCE adapts physical interface on DTE (data terminal

equipment - terminal equipment data) device To rules transmissions signals in the carrier networks. An example of DTE the device is router.

The CSU/DSU provides modulation, time synchronization and is used for interactions With digital transmitting equipment. It is essential, What CSU/DSU is used router For connections With digital channel in in many ways like this same the way a PC uses a modem for communication with an analog telephone channel. That is, V PC-modem connection PC is DTE device, A modem - DCE device.

Selected or rented channels

Typically, serial connections in networks operate with the followingspeeds

56 kbps
64 kbps
T1 (1.544 Mbps) standard USA
E1 (2.048 Mbps) European standard E3
(34.064 Mbps) European standardT3
(44.736 Mbps) standard USA

DTE (router) connected With DCE (CSU/DSU) through synchronous serial port using one of the following standards: EIA/TIA-232 (RS-232), EIA/TIA-449, V.35, X.21, EIA-530.

For connecting DTE (router, PC) to an analog modem (DCE (CSU/DSU)) EIA/TIA-232 is used. Released over 30 years ago, it has become a classic. However He Not acceptable on allocated lines For speeds more how 120 kbps.

Standard V.35 suitable For more high speeds (more 2 Mbps). Heare used For connections port router To T1/E1 through separate CSU/DSU.

Today For many sequential channels connections, such How T1, many Routers have a CSU/DSU integrated into the interface card. That There is, No needs V separate DCE (CSU/DSU).

Networks With switching packages SKP.

IN difference from rented lines And connections With switching channels, switching packages Not supposed to on highlighted, point-to-point compound through load-bearing net. Instead of this packages data are routed V load-bearing networks on based on the addressing contained in the packet or frame headers, which allows to the provider support many consumers on some physical lines And switches.

IN networks With switching packages provider configures my equipment switching For creation virtual chains (virtual circuits (VCs)) For provision through connections. Virtual chains can be constant or can be built

On demand. Frame Relay is a typical packet switching service in the WAN. Often are used Also technologies ATM And X.25.

The first SCPs were built using the X.25 protocol. Since X.25 was designed for work on unreliable telephone copper chains, That He provides detection mistakes

SKP is a network with multiple access using special equipment for delivering user traffic. The physical carrier of signals within the SCP are, How rule, high-speed highlighted channels connections, more often total optical. For provision required through connections inside Investigative Committee configuration is in progress switching equipment.

SKPs offer the network administrator less control than point-to-point connections. dot. However, price virtual chains V Investigative Committee less, how allocated lines. Access to the SCP itself is typically via a synchronous serial port router By the only one allocated lines T1 or T3 And allows connect to many remote sites. Without an SCP, a separate one will be required. dedicated line To to everyone remote website.

Virtual chains Frame Relay provides speed up to to speed T3, making high-speed packet switching technology cost-effective alternative highlighted lines. The only thing synchronous consistentThe connection to the SCP can support multiple virtual circuits in configurations point-to-multipoint (one-to-many) And point-to-point (Rice. 2). Process combinations several gears data V one physical lines it's called multiplexing.

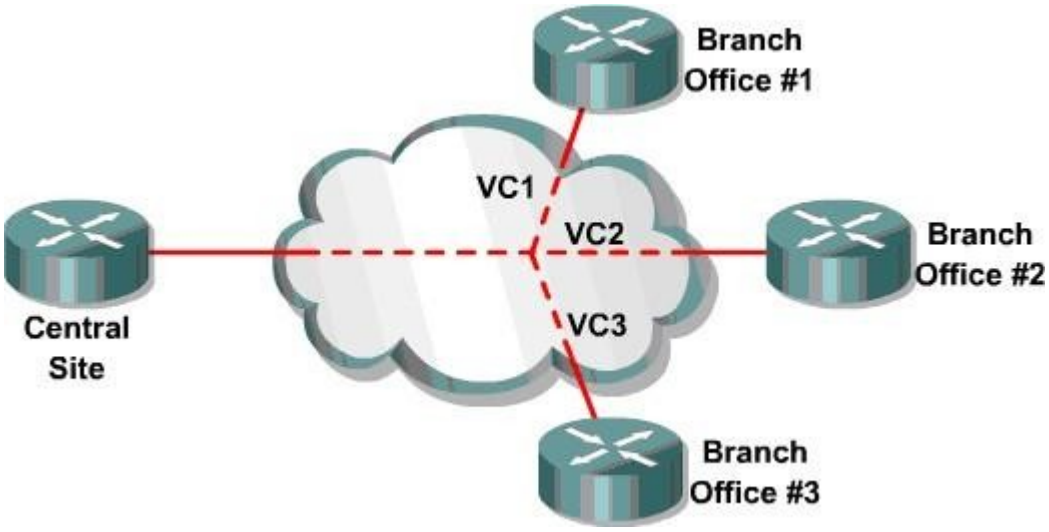


Figure 2.

Multiplexing is made possible by the fact that DTE (usually router) encapsulates data V packages SKP, containing addresses SKP. The ISP switches use these addresses to determine how and where to deliver separate plastic bag. IN case Frame Relay these addresses are called DLCI (Data Link Connection

Identifiers). Multiplexing capability means that one router port together with one CSU/DSU device it can support dozens of virtual circuits, each from which leads To separate website. Hence, switching packages does accessible By price even Creation fully connected topology.

Frame Relay Not corrects mistakes And Fine adapted For work on highly reliable digital channels transmissions.

Frame Relay Not provides that degree reliability, flexibility And security, which provide highlighted lines, which more preferred For critically important traffic and large volume exchange information.

Another popular packet switching technology is ATM (Asynchronous Transfer Mode). Transfer Mode). ATM is an international standard for element-by-element transmission, in whichinformation of various types such as data, voice and video are placed in cells fixed lengths V 53 byte. Fixed length cells allows lead their processing hardware in a way, What reduces temporary delays. ATM designed So to take advantage of advantages high-speed Wednesday transmissions E3, T3 and SONET.

Protocols global networks

Routers encapsulate IP packets before transmitting them over a communication channel.in frames second network level.

Typical protocols second level global networks:

Point-to-Point Protocol (PPP) - protocol connections router - router And router -host For synchronous And asynchronous channels.

Serial Line Internet Protocol (SLIP) - predecessor PPP, used For sequential connections point-to-point protocol TCP/IP.

High-Level Data Link Control (HDLC) - is property Cisco And is used For connections two devices Cisco.

X.25/LAPB is a standard that defines the method of connection between DTE and DCE devices at remote terminal access And computer communications V public networks data.

Frame Relay is a high-performance protocol used in many network environments. interfaces

The figure shows which data communication protocols are used in each of the three types connections in WAN

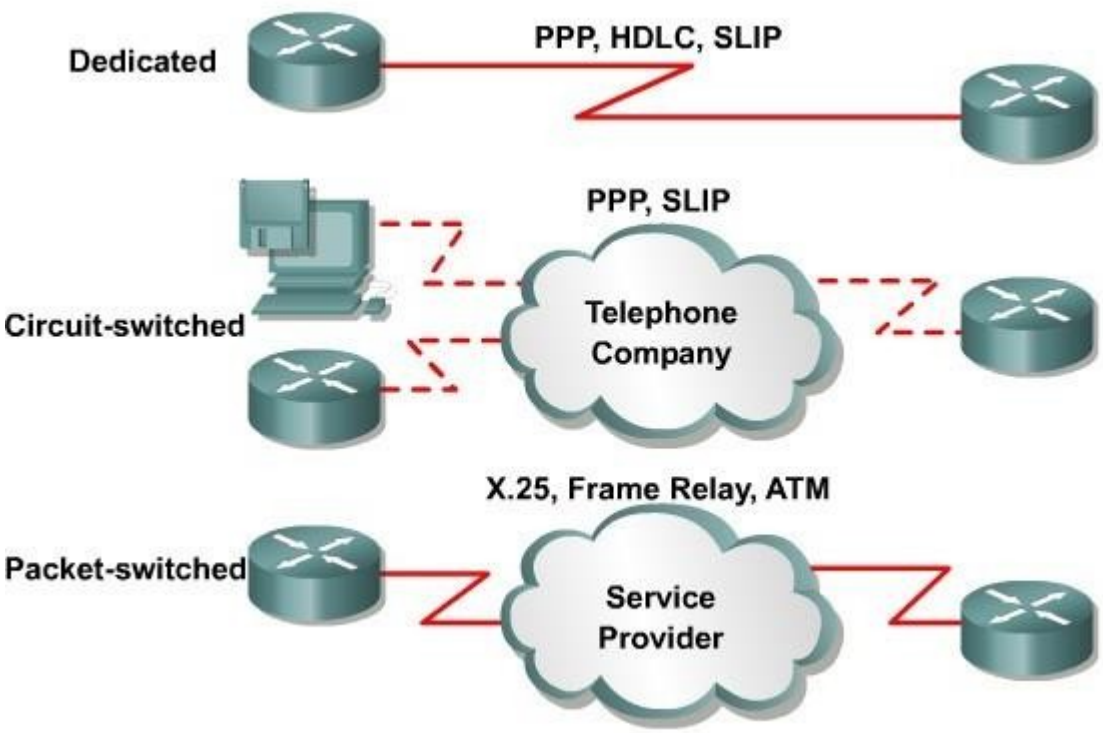


Figure 3.

Frame Relay

IN present time Frame Relay replaces X.25 How technology switching packets. Standardized in 1990, Frame Relay simplifies data link layer functions And provide only check on mistakes, But Not their correction. Such low redundancy approach To switching packages increases performance And efficiency. Modern fiber-optic communication channels and digital means service transmissions provide much less mistakes, how their copper predecessors. For this reason, the use of X.25-like reliability mechanisms on channel level Now at all is assessed How unnecessary. Correction mistakes is carried out in protocols more high level, For example TCP.

Frame Relay - ITU and ANSI standard . ITU-T - International Telecommunications Union (International Union Telecommunications) And ANSI - American National Standards Institute (American National Institute Standards). Standards define the process fortransmissions data By networks with switching packages. Frame Relay it is oriented on compound technology connections data, which optimized, to provide high performance And efficiency.

Modern telecommunication networks are characterized by being relatively free from digital transmission errors and highly reliable infrastructure. Frame Relay relies almost entirely on upper-layer protocols to detect and correct errors. Frame Relay does not have the retransmission mechanisms used in X.25. Without mechanisms corrections mistakes Frame Relay wins at X.25 By speed. IN result Frame Relay acceptable for use there, Where required high

performance, How V local networks. Physical net, on which deployed Frame Relay, Maybe be or public or private network And have different physical nature: optics, satellite channels connections highlighted lines.

Frame Relay defines process relationships between DTE client, type router, And DCE provider. How only traffic reaches switch provider, Frame Relay Not defines way, By to whom data are transmitted V within networks Frame Relay. That's why, provider Frame Relay Maybe use various technologies, such as ATM or PPP, to move data from one end to the other his networks To to another.

Devices Frame Relay

Devices connected to a Frame Relay global network can be either DTE or DCE devices. DTE devices are considered as terminal equipmentAnd usually are located on territories clients - consumers services Frame Relay. Examples of DTE devices are routers and FRAD (Frame Access Devices)Relay Access Devices). FRAD is a special device for communication between LAN and Frame Relay.

Intranet devices DCE belong to the provider. They provide synchronization and/or packet switching services in the network and provide effective transmission data in WAN.

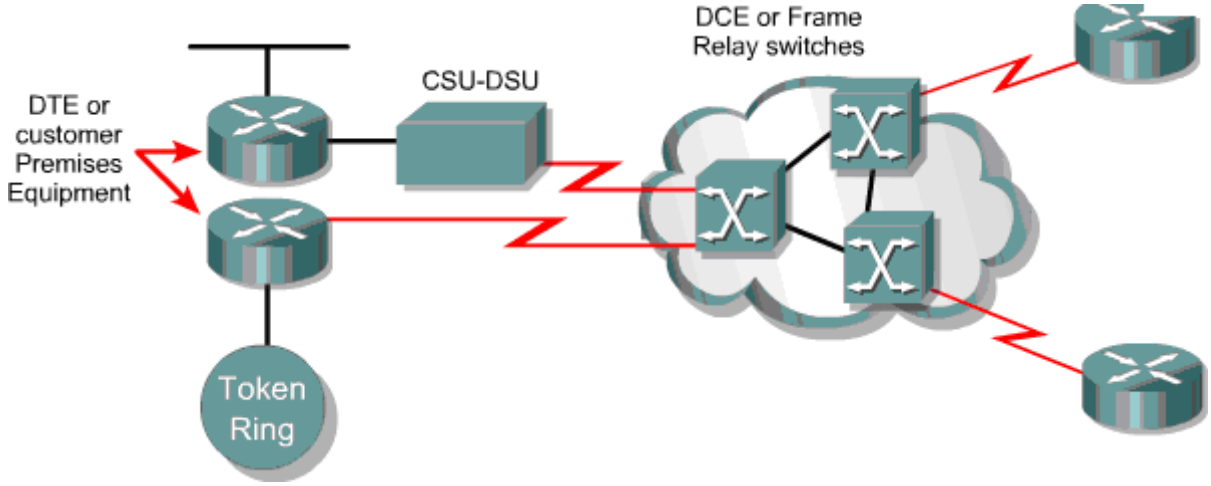


Figure 4.

Net Frame Relay is being built With help switches (switch) Frame Relay, acting as DCEs. Within a Frame Relay network, various technologies transmissions data, For example ATM. Physical channels connections Also Not are regulated - This Maybe be optics, satellite channels connections, highlighted lines.

Regardless of the technology inside the Frame Relay network, the connection between the consumer and provider Frame Relay is carried out according to protocol Frame Relay.

Functioning Frame Relay

Usually than greater distance the dedicated line covers, more expensive service. Support for fully connected remote sites using dedicated lines is too expensive for many organizations. On the other hand, switched networks packages provide way multiplexing several logical gears data By the only one physical connections. The only thing compound To networks With packet switching provider will be less expensive than separate dedicated lines between consumer And each remote website. Networks With switching packages use virtual circuits to deliver packets from end to end across a shared infrastructure.

A packet-switching service such as Frame Relay requires the consumer supported only one chain, usually T1, To central office (CO) provider. Frame Relay provides huge efficiency By cost, So as one website Maybe connect with by many geographically remote websites, using the only one line T1 And one DCE (CSU/DSU) device For connections To local CO.

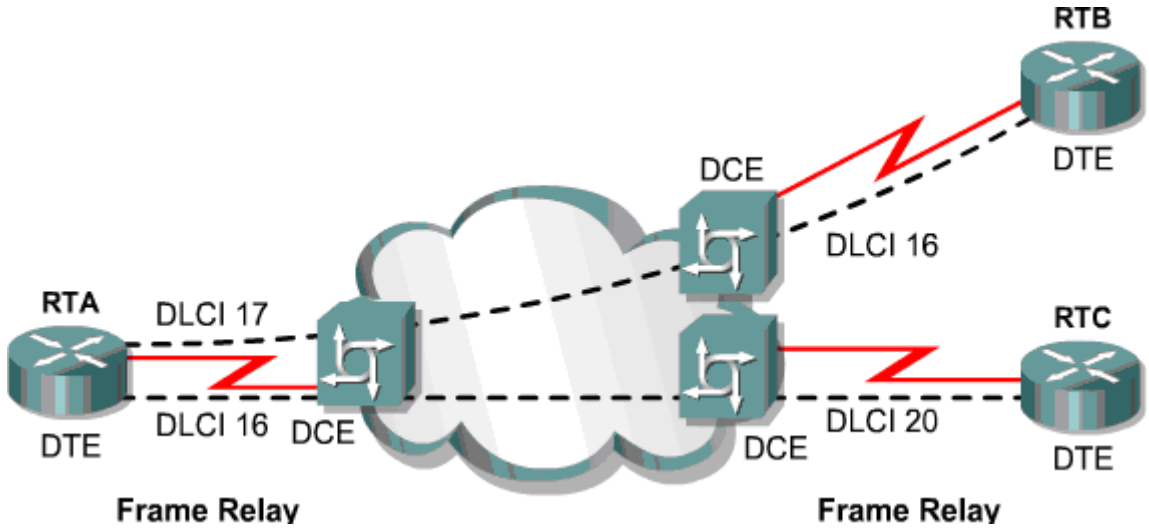
For communications between any two sites provider services must establish a virtual circuit between these sites within the Frame Relay network. Although payment There's a fee for each virtual circuit, so this fee is small. This makes Frame Relay ideal. technology For creation fully connected topology.

Frame Relay networks support both permanent virtual circuits (PVCs) virtual circuits) So And switched virtual chains SVC (switched virtual circuits). PVC

- most typical For Frame Relay. PVC are constantly established connections, which are used, When networks Frame Relay there is stable traffic between certain DTE devices .

SVCs are temporary connections used when a single traffic between DTE devices. So How They temporary, compound SVC requires installations And completion For each connections. Majority providers supports only PVC.

IN Frame Relay to everyone end virtual chains is appointed identifier connections. Switching equipment provider supports table, displaying these identifiers on weekend ports. At receipt frame switch analyzes identifier And delivers frame on corresponding day off port.



Drawing 5. Frame Relay DLCI

IN networks Frame Relay like this identifier it's called DLCI (data - link) connection identifier). They identifies virtual chain. For creation PVC switch uses two DLCIs For each couples DTE devices (routers).

Two DTE devices connected by a virtual circuit can use different DLCI values to refer to the same connection. In Figure 5, the PVC linking routers RTA And RTB, has DLCI equal 17, appointed between RTA And directly connected switch. DLCI number 16 on the RTB defines that same PVC connection between RTB and directly connected switch. Between those, RTA uses DLCI 16 for reference on PVC, which connects with RTC.

For Togo, to router RTA knew, Which PVC use on third network level, IP addresses must be displayed in DLCI numbers. As shown in the picture router RTA must display addresses third level V accessible DLCI.

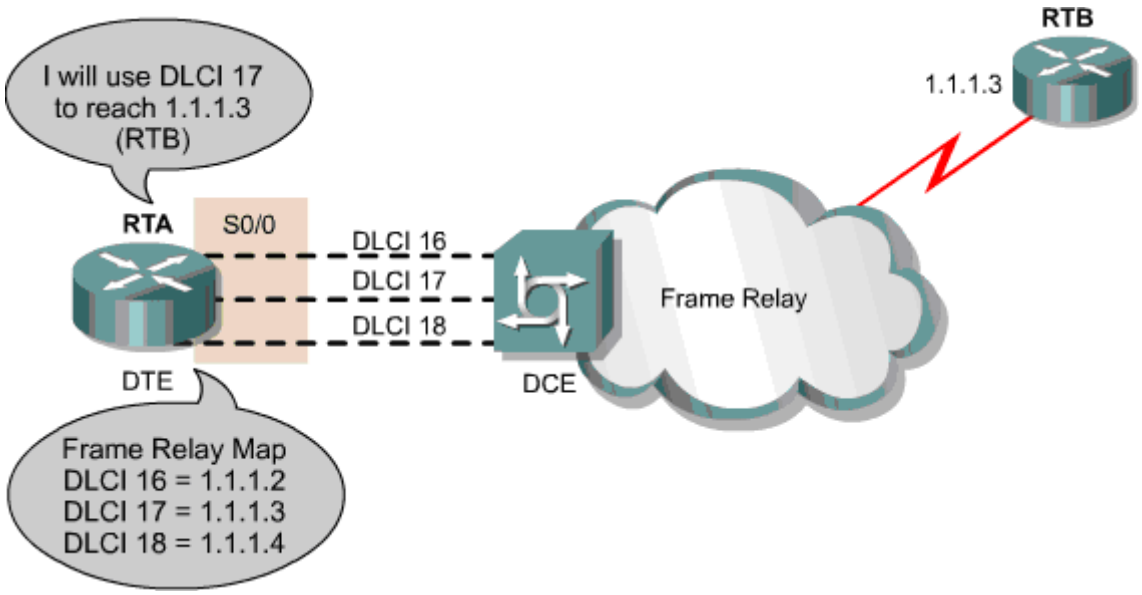


Figure 6.

For example, RTA displays IP address 1.1.1.3 router RTB on DLCI 17. Since the RTA knows which DLCI to use, it follows that to reach the recipient encapsulate the IP packet into a Frame Relay frame containing the appropriate number DLCI.

Routers Cisco support two type headings Frame Relay: Cisco And ietf.
First type - For Cisco equipment, second - For devices of different types manufacturers.

By including the DLCI number in the Frame Relay header, RTA can communicate with both RTB, and with RTC via one physical circuit. With such statistical multiplexing Bandwidth is automatically allocated to active channels. If RTA does not havepackages For parcels on RTB, That RTA Maybe use all accessible strip transmission For connections With RTC. At TDM (Time division multiplexing) multiplexing For each channel, outside dependencies from availability V channel dataon transmission, stands out certain stripe.

For organizations WAN provider services Frame Relay appoints your own clients numbers DLCI. Usually, DLCI from 0 to 15 And from 1008 to 1023 are reserved For special purposes. The service provider assigns DLCI numbers to clients in the range of 16 to 1007. For broadcasting Can use DLCI 1019 And 1020. Local The Local Management Interface (LMI) uses DLCI 1023 or 0. Some providers services Frame Relay can allow your own clients choose own numbers DLCI.

For constructions displays numbers DLCI V addresses third level, The router must first know which VCs are available. Typically, the process of determining available VC And their numbers DLCI is carried out according to standard LMI.

Once the router knows the DLCI numbers for the available VCs, it must define which addresses third level display on which numbers DLCI.Address mapping can be configured either manually or dynamically. Regardless of whether the DLCI is mapped to a remote IP address manually or dynamically, the DLCI used must not have the same values on both ends PVC.

Frame Relay LMI

LMI is a signaling standard between a DTE device (router) and a DCE device (switch Frame Relay). LMI answers for control connection between devices, verifies, What data are transmitted, periodically reports O appearance new PVC And about destruction already existing PVC.

Now exists three incompatible implementation LMI Cisco, ansi And q933a.

At use Cisco iOS release 11.2 And Later, router is trying automatically define type LMI , used switchboard provider

Inverse ARP

WITH help acceptable configuration teams number DLCI Maybe be manually mapped to a third-level address. In complex networks, constructing a static display may require a lot of effort and such display is not suitable to changing the Frame Relay topology. With LMI, a Frame Relay switch can notify routers O DLCI new virtual chains. This notification Not contains address 3 level. Station, received notification will know O new connection, But Not will have opportunity address another side. Without new configuration or mechanism for determining the address of the other party, new virtual chain Not Maybe be used.

Inverse Address Resolution Protocol (Inverse ARP was developed to provide a mechanism for dynamically mapping a DLCI to an address. third level. Inverse ARP works in much the same way as LAN ARP. However, in ARP device knows remote IP address And needs V definition MAC addresses remote devices. IN Inverse ARP, router knows address 2 level, which is a DLCI, but needs V definition remote IP addresses.

How only router received from switch information O available PVCand their DLCI, it can send an inverse ARP request to the other end of each PVC about his address third level. IN That same this time request supplies remote system the local system's third-level address. Information received from inverse ARP, is used For constructions displays Frame Relay on IP.

If V router Cisco interface configurable on usage encapsulation Frame Relay, That inverse ARP turns on automatically. If For a specific interface is configured static mapping, then Inverse ARP is automatically disabled for this protocol and this DLCI. If the router If the other end does not support inverse ARP, then static ARP should be used. display.

Configuration encapsulation V Frame Relay

At configuration sequential interface router ForFrame Relay encapsulation must be defined for connections to Frame Relay. two possible encapsulation - ietf And cisco. On devices Cisco By default Cisco encapsulation is used. The Cisco method is proprietary and not Maybe be used, If router Cisco connected By networks Frame Relay With equipment another manufacturer.

For basic configurations Frame Relay V Cisco iOS versions older 11.1, using inverse ARP and auto-detection of LMI type, you only need to set the address third level and install encapsulation V Frame Relay

Router(config-if)# **encapsulation frame relay {cisco | ietf}**

If Cisco IOS version 11.1 is used or earlier , then necessary ask LMI typeRouter(config-if)# **frame-relay lmi-type {ansi | Cisco | q933a }**

It is important to remember that the Frame Relay service provider creates a virtual circuit within Frame Relay network connecting two remote user network devices, as rule, router. How only router And switch Frame Relay, To to which it is connected, complete the exchange of LMI information, the Frame Relay network has everything you need to create a virtual circuit to another remote router. A Frame Relay network is not like the Internet, where any two devices connected to him, can communicate with each other. In a Frame Relay network, before two routers will be able to exchange information, provider services Frame Relay must in advance install between them virtual circuit.

Configuration displays Frame Relay

If dynamic address mapping is used, then for each active The router's PVC inverse ARP service requests an IP address from the router. next hop. How only requesting router receives response inverse ARP, it updates the mapping table of third-level addresses to numbers DLCI. For Cisco devices, dynamic address mapping is enabled by default. If the Frame Relay equipment supports inverse ARP and auto-negotiation of the type LMI, then dynamic address mapping takes place automatically. Therefore, Not required static displays addresses.

If the equipment does not support inverse ARP and auto-detection of LMI type, then the static display must be configured manually using the frame- command relay map. Once a static mapping is defined for a given DLCI, the serviceinverse ARP turns off.

To configure a static display, use the following syntax: Router(config-if)# **frame-relay map protocol protocol-address dlci [broadcast] [ietf | cisco],**

Where protocol – appletalk, clns, decent, IP, xns, vines, dlci – number DLCI, ietf | Cisco - defines type encapsulation, By default - cisco.

Option broadcast - means broadcast transmission. Used at configuring routing protocols and allows you to consider networks with multiple access and without broadcasting (which is Frame Relay) in much the same way as broadcast networks With multiple access (LAN). For example

Router(config)# **interface Serial2/0**
Router(config-if) **#ip address 1.1.1.1 255.255.255.0**
Router(config-if)# **encapsulation frame relay**
Router(config-if)# **frame relay map IP 1.1.1.2 110 broadcast cisco**
Here 1.1.1.1 local, A 1.1.1.2 remote IP address.

If Cisco encapsulation is configured on the serial interface, this encapsulation applies ko to everyone VC on this interface. If on interface interacts equipment Cisco And Not Cisco, That follows selectively ask encapsulation IETF.

Examination configurations interface Frame Relay

After configuring Frame Relay, you should check that the connections are active. This is carried out with with the help of several teams show:

The show interfaces serial command displays encapsulation and status information. protocols first And second level, A Also O broadcast DLCI, O everyone DLCI numbers used in the serial interface and about the DLCI used forLMI.

Team **show frame relay PVC** shows status each configured connections And statistics traffic. Team shows status everyone PVC, configured on router.

The show frame-relay map command displays the elements of the current address mapping.And information O connections.

Team **show frame relay lmi** shows statistics traffic LMI: number messages O status, which exchanged local router And switchFrame Relay.

Topologies Frame Relay

Frame Relay permits interaction remote websites several waysStar, Sometimes they call hub and spoke

Full mesh Partially related (Partial mesh)

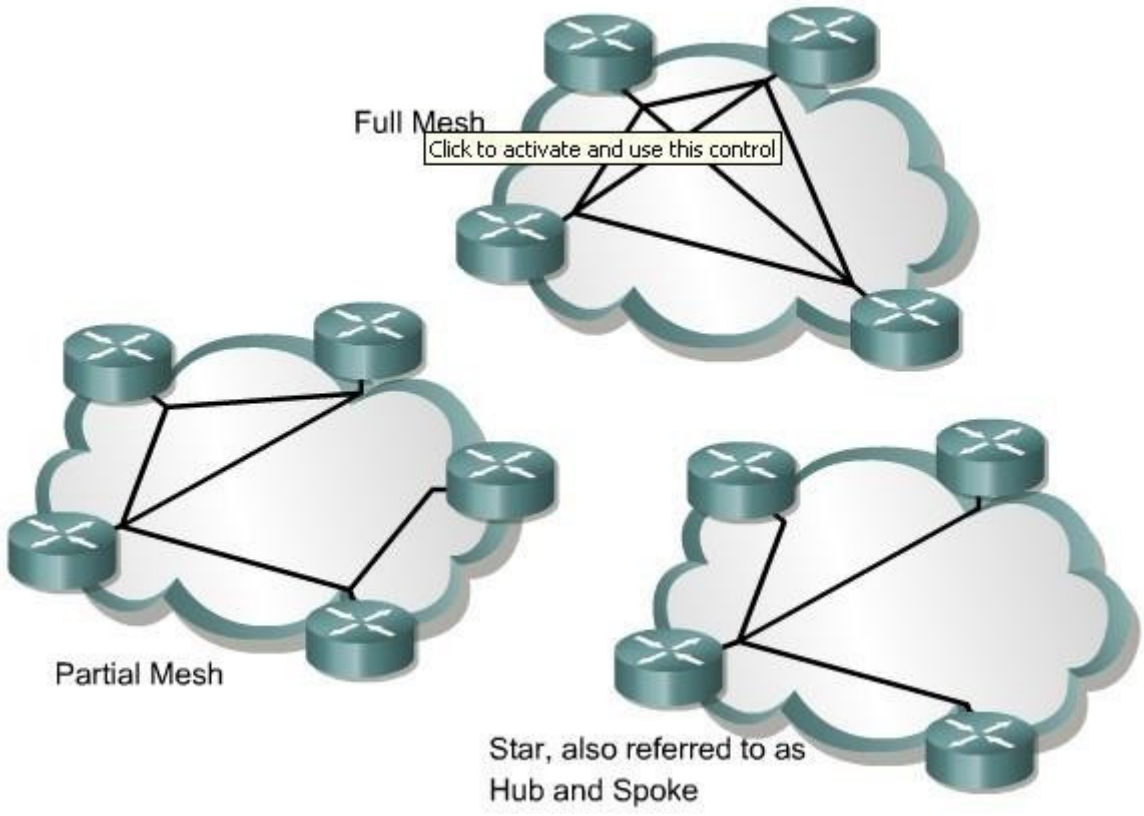


Figure 7.

The star topology is the most popular due to its cost effectiveness. IN this topology deleted websites are connecting To central site, which provides services And services. This least Expensive topology demanding minimum numbers PVC. Usually central router uses one interface for connections with by many PVC.

IN fully connected topology All routers have PVC ko to everyone routers. Topology excessive, But reliable: If some compound disconnected, routers can change routes. As the number of nodes increases, the costsharp is increasing.

In a partially connected topology, not all sites are directly related. Presence of PVC between routers is determined by volume traffic, architecture networks or others considerations.

Configuration subinterfaces For Frame Relay.

Subinterfaces There is logical subdivision physical interface. WITH help configurations subinterfaces every PVC Maybe be configured How compound point-to-point. This allows to everyone subinterface act How leased line. This is because each point-to-point subinterface is considered How separate physical interface.

In the point-to-point case, a single subinterface is used to establish PVC connections to another physical interface or subinterface on the remote computer. IN this case each pair subinterfaces Maybe be V his ownown subnets And every subinterface has the only one DLCI.

For configuration subinterfaces on physical interface is appointed Frame Relay encapsulation (Cisco or IETF). If the physical interface already has an IP address address, it must be removed, since each subinterface has its own IP address. If physical interface has address, That frames Not will be received local subinterfaces:

RTA(config) **#interface s2/0**
RTA(config-if)# **encapsulation frame relay ietf**
Next, determine subinterfaces, using next teams.
Router(config-if)# **interface serial number subinterface-number {multipoint | point-to-point}**

Next team creates subinterface type 2 point - point on Serial 2/0:RTA(config)# **interface serial s0/0.2 point-to-point**

Next team creates subinterface 5 type multipoint on Serial 2/0:RTA(config)# **interface serial s2/0.5 multipoint**

Note, What After entering these commands, the operating system IOS is changing line invitations on **config-subif** , meaning mode configurations subinterface.

Subinterface numbers can be assigned in configuration mode subinterface or V globally configuration mode V range from 1 to

4294967295. At configurations subinterface point to point, ordinary practice is to be numbered subinterface according to DLCI value of this PVC.

After creating the subinterface, you should set the IP address RTA(config-subif)# **ip address 2.1.1.1 255.255.255.0**

Next or configurable static display Frame Relay or the command is used **frame-relay interface-dlci** to associate a subinterface with a DLCI. This command is required for all point-to-point subinterfaces. It is also required for multipoint subinterfaces with inverse ARP enabled. It is not required. For subinterfaces multipoint, which are configured With help static displays routes.

A Frame Relay switch in Figure 8 uses LMI to inform RTA, What available three active PVC with DLCI numbers 18, 19, and 20.

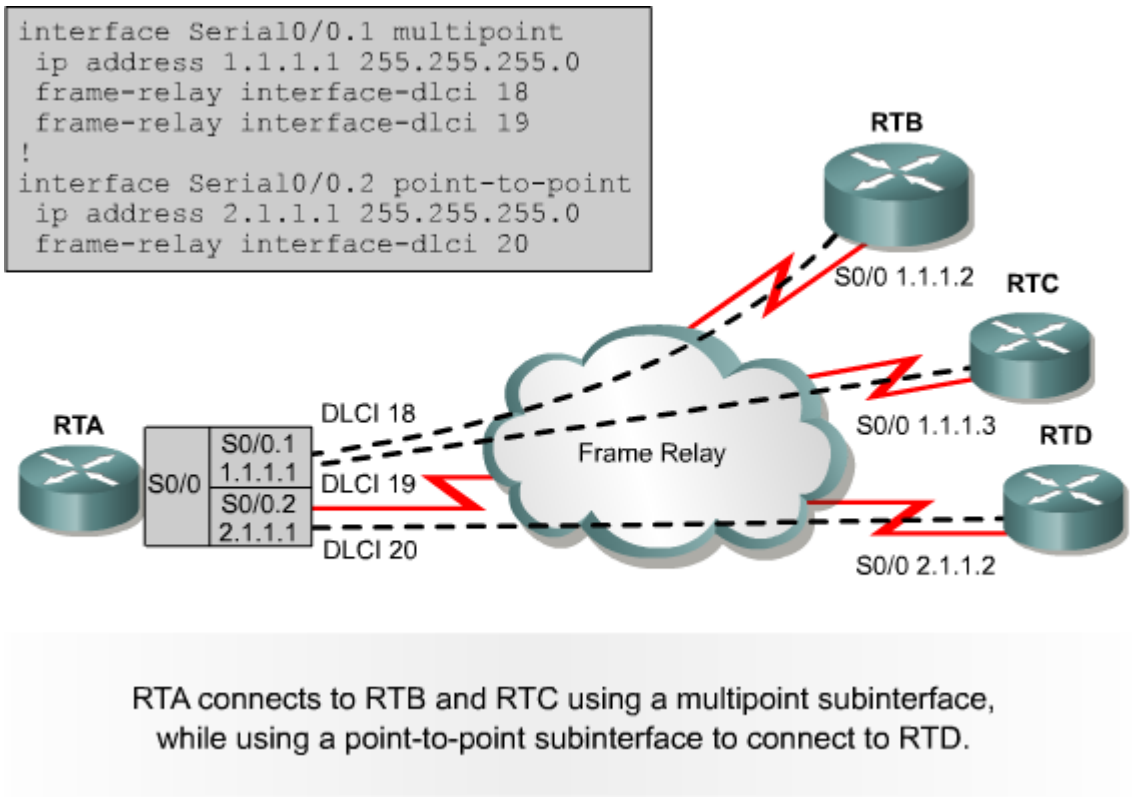


Figure 8.

When RTA learns about DLCIs 18, 19, and 20 on interface S0/0, RTA does not know which DLCI to use with which subinterface. This is because LMI does not provide a way notifying RTA that DLCI 20 should be used by interface S0/0.2 and not S0/0.1. Hence every subinterface must be manually associated With acceptable number DLCI.

multipoint mode is not fully supported by the simulator and is not considered will.

Practical Part

Boson designer always creates a fully meshed Frame Relay topology. To create network topology With using Frame Relay, at the beginning necessary decide, which routers and through which of their serial interfaces will they be connected toFrame Relay. Next, right-click on one of these routers, which will be connected to Frame Relay, and select the Add context menu items connection then necessary interface serial. IN appeared modal window highlight Select the Point-to-Multy-Point Serial Connection (Frame Relay) radio button . Click Next. It will appear new modal window. Select V first list first router, which You do you want connect To Frame Relay, in second list choose his interface that will be connected to Frame Relay and click the Add button. Select In the first list, the second router that you want to connect to Frame Relay, in second list select its interface, which he will connected to Frame Relay and Click the Add button. Repeat for all routers. Click the Connect button. The designer will create a fully meshed topology by defining PVCs and DLCIs. A window will appear with appointed DLCI. Can their edit. Recommended With them Can agree by clicking OK. You can later change the DLCI values by right-clicking button mice on cloud Frame Relay.

Simulator Not V complete measure supports Frame Relay.

1. We create topology on 805 routers

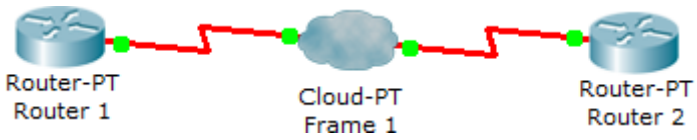


Figure 9.

Configuring Frame Relay

		TO ROUTER				
FROM ROUTER		Router 1	Router 2			
	Router 1		102			
	Router 2	201				

Figure 10.

1.1 Dynamic appointments addresses

router1(config)# **interface serial0**

router1(config-if)# **encapsulation frame relay**

router1(config-if)# **IP address 215.10.1.1 255.255.255.0**

router1(config-if **)# no frame relay inverse-arp**

router1(config-if **)# no shut**
router2(config)# **interface serial0**
router2(config-if)# **encapsulation frame relay**
router2(config-if)# **IP address 215.10.1.2**
255.255.255.0router2(config-if)# **no shut**

Let's introduce team **show interfaces serial0** on both routers . It will show are you connected to Frame Relay. You should see phrases 'up and line protocol is up' And 'DTE LMI up'.

the show frame-relay map command on both routers. On router1 it It won't show anything because **inverse-arp is disabled** . On router2, it will show the display. local DLCI to the remote IP address 201-215.10.1.1.

The show frame-relay pvc command should show the PVC status 'ACTIVE' on router2 and PVC status 'INACTIVE' on router1.

Let's turn it on **inverse-arp**
router1(config-if **)#frame-relay inverse-arp**
Now on router1 it will show the mapping of the local DLCI to the remote IP address 102-215.10.1.2 **The show frame-relay pvc command** should show the PVC status 'ACTIVE' on Router1. Ping both router.

1.2 Static appointments addresses simulator versions 5.3 Not supports. Simulator versions 6.0 Final beta supports.

Download former topology from drawings 9 And 10.

And create new configuration

router1(config)# **interface serial0**
router1(config-if)# **encapsulation frame relay**
router1(config-if)# **IP address 215.10.1.1 255.255.255.0**
router1(config-if)# **frame relay map IP 215.10.1.2 102 broadcast**
router1(config-if)# **no shut**

router2(config)# **interface serial0**
router2(config-if)# **encapsulation frame relay**
router2(config-if)# **IP address 215.10.1.2 255.255.255.0**
router2(config-if)# **frame relay map IP 215.10.1.1 201 broadcast**
router2(config-if)# **no shut**

Enter on both routers commands “show interfaces serial0”, “show frame- relay map”, “show frame relay PVC And “show frame relay lmi”. Ping both router.

1.3 Usage subinterfaces
Download former topology from 9 drawings And 10 And create new configuration
router1(config)# **interface series0**
router1(config-if)# **encapsulation frame relay**
router1(config-if)# **no shut**

router1(config-if)# **interface serial0.102 point-to-point**
router1(config-subif)# **IP address 215.10.1.1**
255.255.255.0router1(config-subif)# **frame-relay**
interface-dlci 102 router2(config)# **interface serial0**
router2(config-if)# **no shut**
router2(config-if)# **encapsulation frame relay**
router2(config-if)# **interface serial0.201 point-to-point**
router2(config-subif)# **IP address 215.10.1.2**
255.255.255.0router2(config-subif)# **frame-relay**
interface-dlci 201

Enter On both routers, run the show ip command. interface brief . You should see appointed addresses And active states interfaces (status = up And up). Note that the “show frame-relay map” command does not show addresses for subinterfaces, but displays the subinterface-DLCI relationship. The same information is also displayed by the command “show frame relay pvc”. Ping both router.

2. Let's create topology global networks firms from three branches. Not losing communities V quality models local networks branches we use By alone computer.

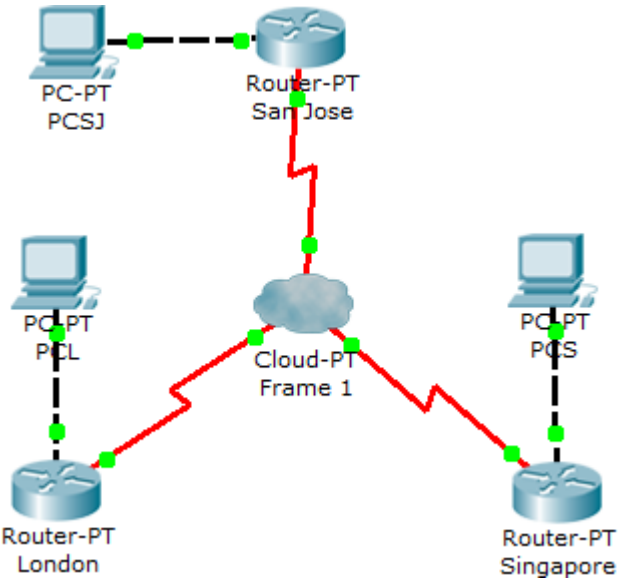
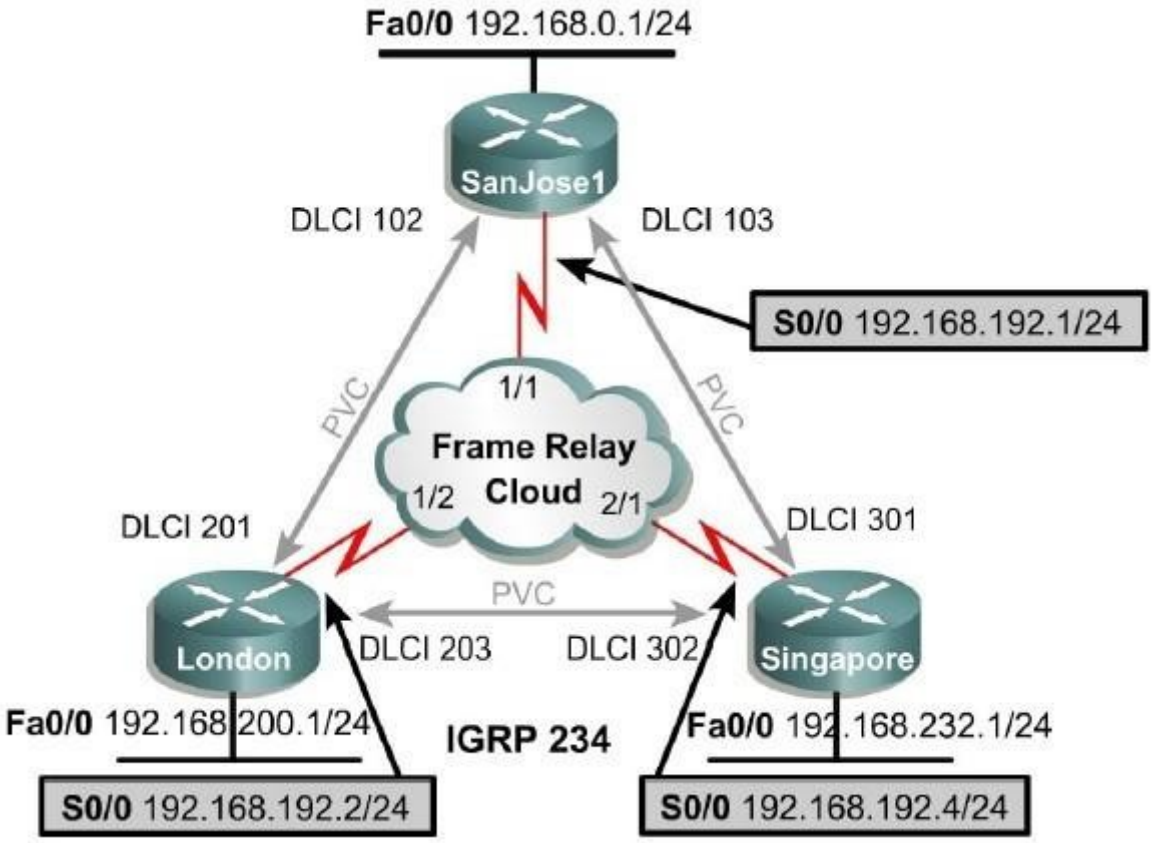


Figure 11.

Let's appoint DLCI according to drawing



Rice 12.

Let's configure three router For Frame Relay For connections three branches firmsBy fully connected topology. IN as a protocol routing we use OSPF.

2.1. Dynamic setting On the

SanJose1 router Router(config)#

hostname SanJose

SanJose(config)# **interface Serial0**

SanJose(config-if) **#ip address 192.168.192.1 255.255.255.0**
SanJose(config-if)# **encapsulation frame relay**
San Jose (config-if)# **no shut**
SanJose(config-if)# **interface Ethernet0**
SanJose(config-if) **#ip address 192.168.0.1 255.255.255.0**
San Jose (config-if)# **no shut**

SanJose(config-if)# **exit**

SanJose(config)# **router ospf**

100

SanJose(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

On router London Router(config)#

hostname London

London(config)# **interface Serial0**

London(config-if) **#ip address 192.168.192.2 255.255.255.0**
London(config-if)# **encapsulation frame relay**
London (config-if)# **no shut**
London(config-if) **#interface Ethernet0**
London(config-if) **#ip address 192.168.200.1 255.255.255.0**
London (config-if)# **no shut**

London(config-if)# **exit**

London(config)# **router OSPF**

100

London(config-router)# **network 192.168.0.0 0.0.255.255 area** 1

On router Singapore Router(config)#

hostname Singapore

Singapore(config)# **interface Serial0**

Singapore(config-if) **#ip address 192.168.192.4 255.255.255.0**
Singapore(config-if)# **encapsulation frame relay**
Singapore (config-if)# **no shut**
Singapore(config-if)# **interface Ethernet0**
Singapore(config-if) **#ip address 192.168.232.1 255.255.255.0**
Singapore (config-if)# **no shut**

Singapore (config-if)# **exit**

Singapore(config)# **router ospf**

100

Singapore(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Enter on everyone routers teams “show IP interface brief” And “show interfaces serial0” . You you can see states interfaces. Enter on both routers command “show frame-relay pvc” You can see the channel status frame relay (pvc status). For example

Singapore# **show frame relay PVC**

```
PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 301, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

input pkts 83                  output pkts 102              in bytes 9360
out bytes 3551                 dropped pkts 21              in FECN pkts 22
in BECN pkts 18                out FECN pkts 29             out BECN pkts 113
in DE pkts 98                  out DE pkts 114
out bcast pkts 65              out bcast bytes 537
pvc create time 00:32:04, last time pvc status changed 00:32:05

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 302, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

input pkts 93                  output pkts 11               in bytes 2025
out bytes 2818                 dropped pkts 7              in FECN pkts 64
in BECN pkts 11                out FECN pkts 81             out BECN pkts 45
in DE pkts 35                  out DE pkts 9
out bcast pkts 56              out bcast bytes 3868
pvc create time 00:32:04, last time pvc status changed 00:32:05
```

We we see active channels on San Jose (DLCI=301) And London (DLCI=302).

In real Frame Relay networks, channel states can be ACTIVE, INACTIVE, and DELETED. ACTIVE is a working end-to-end (DTE to DTE) circuit. State INACTIVE shows successful connection To Frame switch Relay (DTE To DCE) at absence router (DTE) on friend at the end PVC. This state it happens, when the router at the other end of the PVC either does not participate V Frame Relay for our network, or not configured . The DELETED status occurs when the router (DTE) And Frame switch Relay Not Deal about the parameters Frame Relay on this PVC.

Simulator versions 5.3 Not V complete measure supports states.

Team show frame relay map will show dynamically appointed display "external IP address" - "local dlci for canada pvc to a remote router with this external IP address." For example

Singapore# **show frame relay map**

```
Serial0 (up): ip 192.168.192.1 dlci 301(0x66,0x1860), dynamic,
              broadcast,CISCO, status defined, active
Serial0 (up): ip 192.168.192.2 dlci 302(0x66,0x1860), dynamic,
              broadcast,CISCO, status defined, active
```

We see the addresses of other routers. How did the Singapore router know them? When a Singapore router receives a DLCI list via the LMI protocol, it sends inverse ARP requests to each of its discovered PVC channels. Router on friend at the end PVC returns mine IP address.

From tables We we see, What broadcasting broadcast allowed, What allows routing protocols exchange routing information. Using the command show IP route, make sure What from There is London route to Singapore

London# **show IP route**

```
C       192.168.192.0/24 is directly connected, Serial0
C       192.168.200.0/24 is directly connected, Ethernet0
D       192.168.0.0/24 [110/65] via 192.168.192.1, 00:00:28, Serial0
D       192.168.232.0/24 [110/65] via 192.168.192.4, 00:00:44, Serial0
```

London has route on net 192.168.232.0/24 Singapore on address 192.168.192.4 throughSerial0.

We we see, What only **With one physical communication** To Frame Relay every router has **By two logical connections** .

Let's configure local networks branches

RS	IP	Gateway
PCSJ	192.168.0.2	192.168.0.1
PCL	192.168.200.2	192.168.200.1
PCS	192.168.232.2	192.168.232.1

Table 1.

Let's check the full configuration using the extended ping command. For example: We Can from router V San Jose check There is whether connection from branch computer PCL V London To branch computer PCS V Singapore.

```
SanJose#ping
Protocol [ip]:
Target IP address: 192.168.232.2
Repeat count [5]: 50
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:192.168.200.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 192.168.232.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/2/4 ms
```

un

e

Pings successful.

2.2. Static setting

Use simulator versions 6.0 Final beta.

Network engineers can be Not satisfied implicit dynamicconfiguration. Facilities dynamic displays DLCI - IP minimal because of static nature of most global connections. Once a connection is established, it Not changes years.

We will statically connect the branches into a global network. To do this, we need to create a new one. configuration again. Download V simulator former created topology And set up routers

San Jose

Router (config)# **hostname San Jose**

SanJose(config)# **interface Serial0**
SanJose(config-if) **#ip address 192.168.192.1**
255.255.255.0 SanJose(config-if)# **encapsulation frame**
relay SanJose(config-if)# **no frame-relay inverse-arp**
SanJose(config-if)# **frame-relay map IP 192.168.192.2 102 broadcast**
SanJose(config-if)# **frame-relay map IP 192.168.192.4 103 broadcast**
San Jose (config-if)# **no shut**
SanJose(config-if)# **interface Ethernet0**
SanJose(config-if) **#ip address 192.168.0.1 255.255.255.0**
San Jose (config-if)# **no shut**
SanJose(config-if)# **exit**
SanJose(config)# **router ospf**
100
SanJose(config-router)# **network 192.168.0.0 0.0.255.255 area 1**
London
Router(config)# **hostname London**
London(config-if **)#interface Serial0**
London(config-if)# **IP address 192.168.192.2**
255.255.255.0 London(config-if)# **no frame-relay inverse-**
arp London(config-if)# **encapsulation frame relay**
London(config-if)# **frame-relay map ip 192.168.192.1 201**
broadcastLondon(config-if)# **frame-relay map ip 192.168.192.4 203**
broadcast London (config-if)# **no shut**
London(config-if) **#interface Ethernet0**
London(config-if) **#ip address 192.168.200.1 255.255.255.0**
London (config-if)# **no shut**
London(config-if)# **exit**
London(config **)#router OSPF**
100
London(config-router)# **network 192.168.0.0 0.0.255.255 area 1**
Singapore
Router(config)# **hostname Singapore**
Singapore (config)# **interface Serial0**
Singapore (config-if)# **IP address 192.168.192.4 255.255.255.0**
Singapore (config-if **)# encapsulation frame relay**
Singapore (config-if)# **no frame relay inverse-arp**
Singapore (config-if)# **frame-relay map ip 192.168.192.1 301**
broadcastSingapore (config-if)# **frame-relay map ip 192.168.192.2 302**
broadcastSingapore (config-if)# **no shut**
Singapore (config-if)# **interface Ethernet0**
Singapore (config-if)# **IP address 192.168.232.1 255.255.255.0**
Singapore (config-if)# **no shut**
Singapore (config-if)# **exit**

Singapore (config)# **router ospf 100**
Singapore (config-router)# **network 192.168.0.0 0.0.255.255 area 1**

We used the **no frame-relay inverse-arp command** because without it the simulator displays addresses How statically so and dynamically.

The frame-relay map command associates the next hop IP address with the local DLCI. Key word broadcast permits passage broadcast traffic, for example For information O routes For routing protocols.

Enter on everyone routers teams “show IP interface brief” And “show interfaces serial0” . You you can see states interfaces. Enter on both router commands “show frame-relay pvc” and “show frame-relay lmi”. You can see states frame relay. Team show frame relay map will show statically appointed display "external IP address"-"local dlci For Canada PVC on remote router with this external IP address." You should see the word static. For example

SanJose)# **show frame relay map**

```
Serial0 (up): ip 192.168.192.2 dlci 102(0x66,0x1860), static,
              broadcast,CISCO, status defined, active
Serial0 (up): ip 192.168.192.4 dlci 103(0x66,0x1860), static,
              broadcast,CISCO, status defined, active
```

Using team show IP route, make sure What from London There is route on Singapore. TO unfortunately at simulator version 6.0 Final beta problems With routing.

Let's configure local networks branches How V table 1.

Let's check the full configuration using the extended ping command. For example: We Can from router V San Jose check There is whether connection from branch computer PCL V London To branch computer PCS V Singapore.

All pings should be successful. IN particulars between by everyone PC.

2.3 Usage subinterfaces

On simulator versions 6 final beta Not works dynamic routing.
We are working With simulator versions 5.31.

For improvements opportunities settings connections network engineers at the beginning use individual physical connections between by everyone two branches. However general price project turned out to be excessive. It's decided was use subinterfaces and Frame Relay. This allows for the creation of a separate logical channel between by everyone two branches. Every router has as before one physical line for connection to Frame Relay, but for each serial interface is configured with two subinterfaces. It becomes possible to use multiple PVC channels for each physical interface of the router. General price project turns out acceptable.

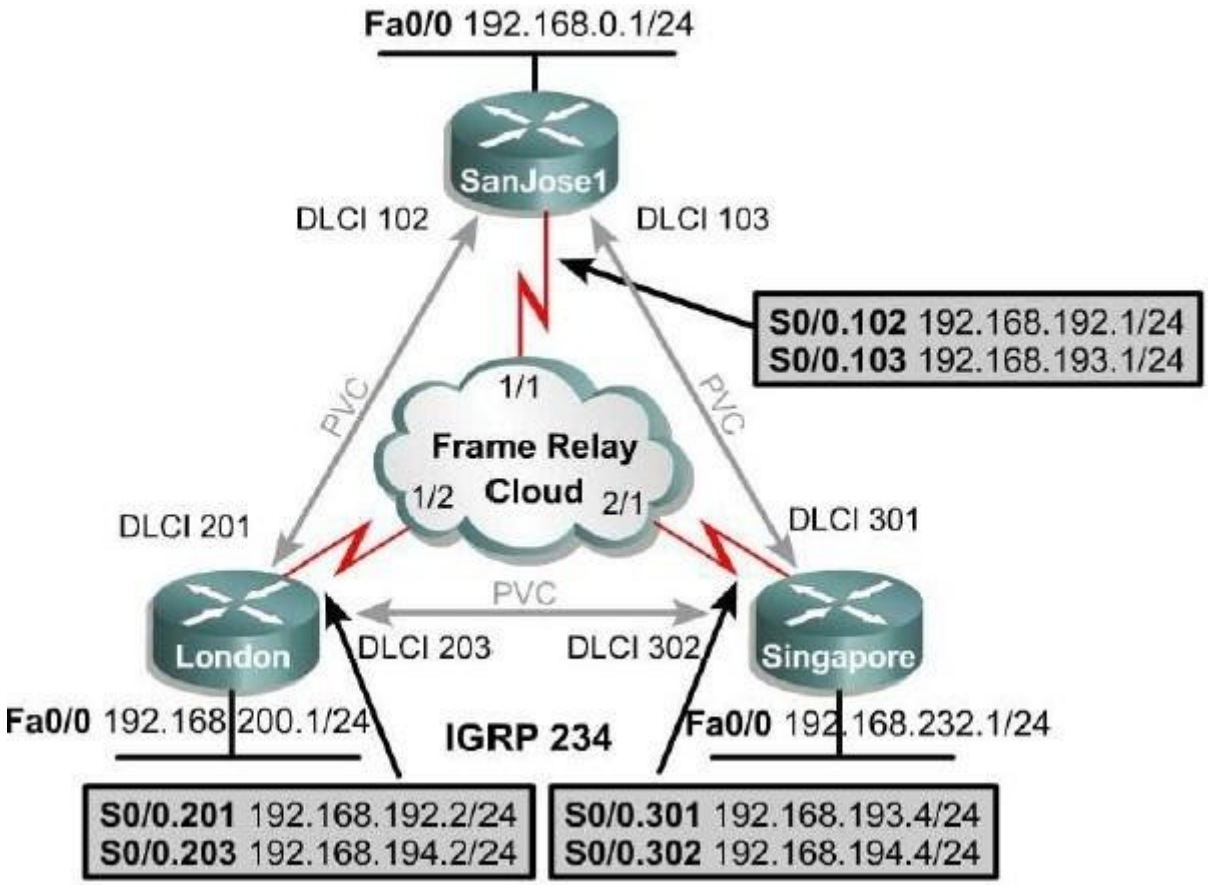


Figure 13.

To do this, you need to create a new configuration again. Restart the simulator and Load the previously created topology (Figure 11). Configure it on the routers subinterfaces according to Figure 13. For each PVC channel we use a separate subnet

PVC	DLCI	Subnet
San Jose-London	102 - 201	192.168.192.0/24
San Jose-Singapore	103 -301	192.168.193.0/24
London-Singapore	203 - 302	192.168.194.0/24

Table 2.

For this use teams. On router SanJose1Router(config)# **hostname San Jose**

SanJose(config)# **interface serial 0**

SanJose(config-if)# **encapsulation frame-relay**SanJose1(config-if)# **no shutdown**

The IP address is not assigned to the entire interface. Addresses are assigned to each subinterface.

Interfaces Frame Relay Can be translated or V mode point-to-point (point-to-point) or V mode multipoint (multipoint). Configuring subinterface point to point,

using DLCI. It is common practice to use the DLCI number as the number subinterface. Then easier determine Which channel PVC uses everysubinterface. For example, a subinterface 0.103 uses DLCI 103:

SanJose(config-if)# **interface s0.103 point-to-point**
SanJose(config-subif)# **ip address 192.168.193.1 255.255.255.0**
SanJose(config-subif)# **frame-relay interface-dlci 103**

Thoroughly enter V simulator team interface s0.103 point-to-point. Use ? For issuance hints after input another one words teams.

Team frame relay interface-dlci is used For definitions, Which DLCI uses every subinterface. Subinterface point-to-point Maybe use only one DLCI. If no subinterface is defined for a DLCI, the DLCI is associated with main interface s0.

Configuring subinterface For DLCI 102: SanJose(config)#

interface s0.102 point-to-point SanJose(config-subif)# **ip**

address 192.168.192.1 255.255.255.0

SanJose(config-subif)# **frame-relay interface-dlci**

102 Configuring Ethernet0 And routing

SanJose(config-if)# **interface Ethernet0**

SanJose(config-if) **#ip address 192.168.0.1 255.255.255.0**
SanJose(config-if **)#exit**

SanJose(config)# **router ospf**

100

SanJose(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Similarly, using drawing 13, configure rest routers. London

Router(config)# **hostname London**

London(config)# **interface Serial0**

London(config-if# **encapsulation frame**

relayLondon(config-if)# **no shutdown**

London(config-if) **#interface Serial0.201 point-to-point**
London(config-subif) **#ip address 192.168.192.2 255.255.255.0**
London(config-subif)# **frame-relay interface-dlci 201**

London(config-subif)# **interface Serial0.203 point-to-point**

London(config-subif)# **ip address 192.168.194.2**

255.255.255.0

London(config-subif)# **frame-relay interface-dlci 203**
London(config-subif)# **interface Ethernet0**
London(config-if) **#ip address 192.168.200.1 255.255.255.0**
London(config-if)# **no**

shutdownLondon(config-if)#

exit London(config)# **router**

OSPF 100

London(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Singapore

Router(config)# **hostname Singapore**
Singapore(config)# **interface Serial0**
Singapore(config-if)# **encapsulation frame-**
relaySingapore(config-if)# **no shutdown**
Singapore(config-if)# **interface Serial0.301 point-to-point**
Singapore(config-subif) **#ip address 192.168.193.4 255.255.255.0**
Singapore(config-subif)# **frame-relay interface-dlci 301**
Singapore(config-subif)# **interface Serial0.302 point-to-point**
Singapore(config-subif)# **ip address 192.168.194.4**
255.255.255.0
Singapore(config-subif)# **frame-relay interface-dlci 302**
Singapore(config-subif)# **interface Ethernet0**
Singapore(config-if)# **ip address 192.168.232.1**
255.255.255.0 Singapore(config-if)# **no shutdown**
Singapore(config-if)# **exit**
Singapore(config)# **router ospf**
100
Singapore(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Check the PVC status on each router with the show frame-relay pvc command. The show frame-relay map command does not map DLCIs to IP addresses in the case of subinterfaces. address. Each subinterface is treated as a separate physical interface for each PVC channel. In this case, each PVC channel contains only two hosts and there is no needs identify next hop.

To check that the addresses are assigned correctly and to ensure that everything subinterfaces are in active state, use the **show ip interface command brief.** Using the **show ip route command** , make sure What There is a route from London to Singapore

London#show ip route

```
Gateway of last resort is not set
C       192.168.192.0/24 is directly connected, 192.168.192.2
C       192.168.200.0/24 is directly connected, Ethernet0
C       192.168.194.0/24 is directly connected, 192.168.194.2
O       192.168.0.0/24 [110/1] via 192.168.192.1, 00:00:38, Serial0.201
O       192.168.193.0/24 [110/1] via 192.168.194.4, 00:00:15, Serial0.203
O       192.168.232.0/24 [110/1] via 192.168.192.1, 00:00:48, Serial0.201
```

We we see, What OSPF worked So, What London has route on net 192.168.232.0/24 Singapore through Serial0.201 on address192.168.192.1. Route, through

through Serial0.203 on address 192.168.194.4 Briefly speaking. A How at you? Questions optimization routes Here Not are being considered.

Let's configure local networks branches according to table 1.

Let's check the full configuration using the extended ping command. For example: We Can from router V San Jose check There is whether connection from branch computer PCL V London To branch computer PCS V Singapore.

All pings should be successful. IN particulars between by everyone PC.

3. Topology star

Traffic between London and Singapore was found to be low and it was decided abandon the PVC channel between them and use a star topology. All traffic between London And Singapore will pass through SanJose.

Let's load the old topology into the designer. Right-click on the cloud in it. Frame Relay, we will change the DLCI according to the figure, i.e. we will destroy the PVC between London and Singapore.

	SanJose	London	Singapore
SanJose		102	103
London	201		0
Singapore	301	0	

Figure 14.

We use subinterfaces V mode point-to-pointSanJose:

Router(config)# **hostname SanJose**

SanJose(config)# **interface Serial0**

SanJose(config-if)# **encapsulation frame-**

relaySanJose(config-if)# **no shutdown**

SanJose(config-if)# **interface Serial0.103 point-to-point**

SanJose(config-subif)# **ip address 192.168.193.1 255.255.255.0**

SanJose(config-subif)# **frame-relay interface-dlci 103**

SanJose(config-subif)# **interface Serial0.102 point-to-point**

SanJose(config-subif)# **ip address 192.168.192.1**

255.255.255.0

SanJose(config-subif)# **frame-relay interface-dlci 102**

SanJose(config-subif)# **interface Ethernet0**

SanJose(config-if)# **ip address 192.168.0.1**

255.255.255.0 SanJose(config-if)# **no shutdown**

SanJose(config-if)# **exit**

SanJose(config)# **router ospf**

100

SanJose(config-router)# **network 192.168.0.0 0.0.255.255 area 1**

London: Router(config)#

hostname London

London(config)# **interface Serial0**
London (config-if)# **encapsulation frame relay**
London (config-if)# **no shutdown**
London(config-if)# **interface Serial0.201 point-to-point**
London(config-subif)# **IP address 192.168.192.2**
255.255.255.0 London(config-subif)# **frame-relay interface-**
dlci 201 London(config-subif)# **interface Ethernet0**
London(config-if)# **IP address 192.168.200.1 255.255.255.0**
London (config-if)# **no shutdown**
London (config-if)# **exit**
London (config)# **router ospf 100**
London (config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Singapore:
Router(config)# **hostname Singapore**
Singapore (config)# **interface Serial0**
Singapore (config-if)# **encapsulation frame relay**
Singapore (config-if **)# no shutdown**
Singapore (config-if)# **interface Serial0.301 point-to-point**
Singapore (config-subif)# **ip address 192.168.193.4 255.255.255.0**
Singapore (config-subif)# **frame relay interface-dlci 301**
Singapore (config-subif)# **interface Ethernet0**
Singapore (config-if)# **IP address 192.168.232.1 255.255.255.0**
Singapore (config-if)# **no**
shutdown Singapore (config-if)#
exit Singapore (config)# **router**
ospf 100
Singapore (config-router)# **network 192.168.0.0 0.0.255.255 area 1**

Enter on everyone routers teams **show ip interface** brief and **show interfaces serial0** . You can see the interface states. Interfaces must be active. (UP)

Enter **the show frame-relay pvc** and **show frame- commands on both routers. relay lmi** . You you can see states frame relay. Let's note absence PVC between London And Singapore. For subinterfaces team **show frame relay map** Not will show display DLCI address . Use **show ip interface brief.**

Using team show IP route, make sure What from London There is route on Singapore

London#show ip route

```
C       192.168.200.0/24 is directly connected, Ethernet0
C       192.168.192.0/24 is directly connected, 192.168.192.2
O       192.168.193.0/24 [110/1] via 192.168.192.1, 00:00:39, Serial0.201
O       192.168.0.0/24 [110/1] via 192.168.192.1, 00:00:43, Serial0.201
O       192.168.232.0/24 [110/1] via 192.168.192.1, 00:00:47, Serial0.201
```

We see that London has a route to address 192.168.192.1 via Serial0.201 on net 192.168.232.0/24 Singapore.

Let's configure local branch networks according to Table 1. Let's check the complete configuration With help extended teams ping. For example We Can from router in SanJose check if there is a connection from the branch computer PCL in London To branch computer PCS V Singapore.

All pings should be successful. IN particulars between by everyone PC.

Let's see path packages from branch computer PCL V London To branch computer PCS V Singapore.

PCL# **trace 192.168.232.2**

```
1 192.168.200.1 0 msec 16 msec 0 msec
2 192.168.192.1 20 msec 16 msec 16 msec
3 192.168.193.4 20 msec 16 msec 16 msec
4 192.168.232.2 20 msec 16 msec *
```

He lies through router San Jose (192.168.192.1).

Control questions

1. Name it types sequential channels connections.
2. Where the device is located CSU/DSU And which functions it performs?
3. What's happened DTE And DCE?
4. How DTE connected With DCE?
5. Formulate an idea networks With switching packages SKP.
6. What's happened virtual circuits V Investigative Committee?
7. Name it types Investigative Committee?
8. Which physical communication channels use Investigative Committee?
9. How is being carried out access consumer To Investigative Committee?
10. Which technologies transmissions data are used in Investigative Committee?
11. IN how difference Frame Relay And X.25?
12. Protocol Frame Relay Not corrects errors. Where They Then are they being corrected?
13. What's happened ATM?
14. Name it protocols global networks And For what kind types of sequential channels connections They are used.
15. Name it DTE devices Frame Relay.
16. Name it DCE device Frame Relay.
17. How get in touch in Frame Relay devices DTE And DCE?
18. How differ PVC from SVC?
19. What's happened DLCI and how it correlates With PVC?
20. What necessary do, to hand over IP plastic bag through net Frame Relay?
21. How display DLCI on remote IP?
22. What such LMI?
23. Describe work protocol Inverse ARP.

24. How to configure a router's serial interface forconnections To Frame Relay.
25. When is used static display addresses?
26. How on router see to what PVC He connected?
27. How on router For interfaces see displays DLCI onremote IP?
28. How on router For subinterfaces see displays DLCI onremote IP?
29. Name it Topologies Frame Relay.
30. How is being carried out configuration subinterfaces For Frame Relay.
31. Which one? role plays team frame relay interface-dlci when configuring subinterfaces For Frame Relay.
32. Which restrictions has simulator at work With Frame Relay?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute contract All points practical part.
4. Create All screenshots, given V practical parts.
5. Show to the teacher result execution points 1, 2 and 3 practicalparts.
6. Do it V Packet Tracer exercise For independent work.
7. Show to the teacher result execution points 1, 2 And 3 tasks Forindependent work.
8. Make out report. Content report Look below.
9. Protect report.

Exercise For independent work

1. For fully connected topology four websites With local networks (Drawing 15)design Frame Relay net With:

A) dynamic appointment addresses;IN)

subinterfaces.

Use protocol OSPF routing.

IN yours at disposal subnet 10.v.0.0/16 , Where v - number options. Addresses networks Andassign interfaces on one's own.

Do it screenshots:

1. 4-x tables routings For each router.
2. Teams extended ping from any router For two arbitrarysteam computers.
3. The result of executing **the show frame-relaymap command** for each router

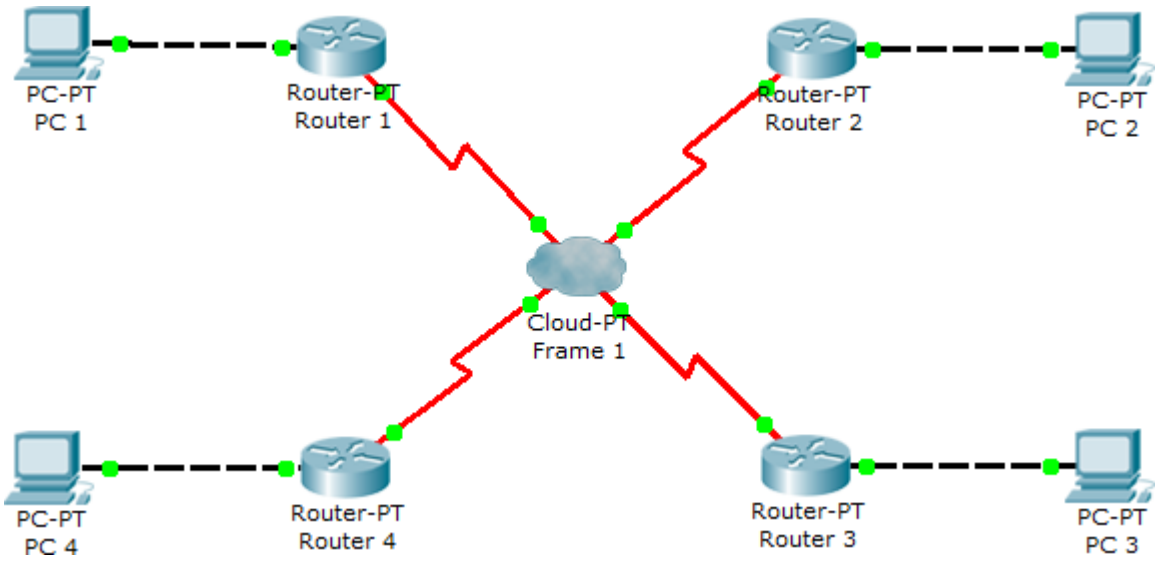


Figure 15.

2. Incompletely connected topology

IN designer, by clicking right button on cloud Frame Relay And having chosen paragraph Set FrameRelay Parameters, Can edit table DLCI

FROM ROUTER \ TO ROUTER	Router 1	Router 2	Router 3	Router 4
Router 1		102	103	104
Router 2	201		203	204
Router 3	301	302		304
Router 4	401	402	403	

And get various incompletely connected topology. Let's consider fourA)

Star (fork)

FROM ROUTER \ TO ROUTER	Router 1	Router 2	Router 3	Router 4
Router 1		102	103	104
Router 2	201		0	0
Router 3	301	0		0
Router 4	401	0	0	

B) Letter P

FROM ROUTER \ TO ROUTER	Router 1	Router 2	Router 3	Router 4
Router 1		102	0	0
Router 2	201		203	0
Router 3	0	302		304
Router 4	0	0	403	

IN) Letter ABOUT (square)

FROM ROUTER \ TO ROUTER	Router 1	Router 2	Router 3	Router 4
Router 1		102	0	104
Router 2	201		203	0
Router 3	0	302		304
Router 4	401	0	403	

Options

Option	Topology	Net
1	A	1.1.0.0/16
2	b	2.1.0.0/16
3	V	3.1.0.0/16
4	A	4.1.0.0/16
5	b	5.1.0.0/16
6	V	6.1.0.0/16
7	A	7.1.0.0/16
8	b	8.1.0.0/16
9	V	9.1.0.0/16
10	A	10.1.0.0/16
11	b	11.1.0.0/16
12	V	12.1.0.0/16

addresses yourself. Usesubinterfaces. Do it screenshots:

1. 4 tables routing for each router.
2. Teams extended ping from any router For two arbitrarysteam computers.
3. The result of executing **the show frame-relaymap command** for each router

Content report.

Report is being prepared V electronic view And is printed. Report contains

1. Screenshots topologies, created at execution practical parts.
2. All screenshots, created at execution practical parts.
3. Configurations of all configuration .txt files created during executionpractical parts.
6. Configuration routers from configuration .txt files, createdat completing tasks For independent work.
7. All screenshots, specified V task For independent work.

Practical class №14. Network Layer Protocols (Part 5).

Theoretical Part.

Local networks V present time accepted build on basis technologists dial-up Ethernet. They strive minimize number used concentrators (hubs-hab) And use predominantly switches (switches - switch). IN switchboard between receiver And transmitter on time connections is formed virtual channel (virtual circuit) point-to-point. Such net Maybe be considered as a set of independent transmitter-receiver pairs, each of which uses the entire bandwidth. The switch allows for parallel transmission information. Switching reduces probability overflow V networks Ethernet.

If a switch needs to transmit a packet to some output port, and this If the port is busy, the packet is placed in the buffer memory. This allows for speed negotiation. transmitters And receivers packages.

For dispatches frame through switch two are used method:

Sending With intermediate storage (store-and-forward). Plastic bag must be accepted fully to Togo how will it be started his dispatch.

Through method (cut-through). The switch accepts the start package, reads in him address point appointments And begins send plastic bag more to his complete receipt.

Ethernet switch recognizes MAS addresses devices V networks by way readings addresses sources V accepted packages. Switch remembers V their own internal tables contain information on which ports and from which MAC addresses packets are received. connecting multiple devices to one port via a hub in the table alone port will correspond some MAC- addresses. Tables are stored V memory, addressable By meaning (content-addressable memory, CAM): If address If the sender is not in the table, it is entered there. Along with address-port pairs, in The table also stores a timestamp. The timestamp in a table row is changed either when when a packet with the same address arrives at the switch, or when the switch contacts this address. If a table row has not been used for a certain period of time, then she is deleted. This allows switch to support correct list addresses devices For transmissions packages.

Using CAM table addresses And contained V who came package address receiver, the switch organizes a virtual connection from the sender port to the port recipient And transmits plastic bag through This compound.

Virtual compound between ports switch is preserved V flow transmission of one packet, i.e. for each packet a virtual connection is organized again on basis contained V this package recipient's address.

Because plastic bag transmitted only V That port, To to whom connected destination, rest devices connected to switch, will not receive this plastic bag.

IN switches Ethernet broadcast data between any in pairs ports is happening regardless And, hence, For each virtual connections stands out all stripe channel.

At transfer broadcast package, V switchboard is formed "fan" channels By principle one ko to many. Examples sources broadcast traffic are ARP And routing protocols.

Switches can be connected to each other. In this case, a group of switches can be connected in pairs directly or indirectly connected switches form one logical switch with theoretically an arbitrary number of ports. That is, switches allow you to theoretically create an arbitrarily large local network. The correct connection of switches, that is, The choice of network topology is one of the most important tasks in the design of local networks.

Recommended realize compound switches By layers (drawing 1): server layer, layer distribution (distribution) And layer access (access). Privates computers connect To layer access, A servers To server layer.

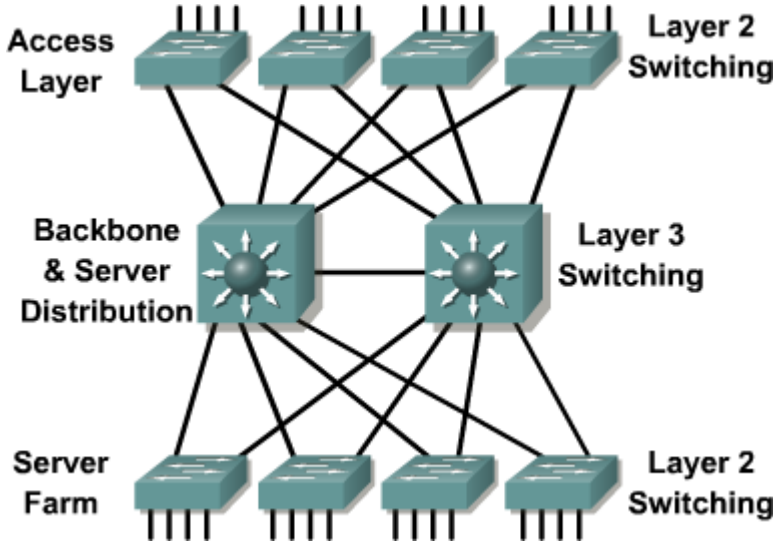


Figure 1.

The main obstacle to creating large local area networks using only only switches is a nonlinear growth of the volume of broadcast traffic with growth in the number of devices on the network. When the number of devices on the network exceeds 2000 (according to other Some estimates say 500, while others say 4000 – it all depends on the network topology and the class of problems being solved) The volume of broadcast traffic is increasing sharply. The addition of new devices is sharply reduces performance networks.

For example. If V networks from several thousands devices one from computers A makes an IP connection to another computer B on this network for the first time, then it must pre-send a broadcast ARP request to all devices on the network definitions MAC addresses computer B.

Local net, created With with the help of only switches represents one domain broadcasting. Decrease domain broadcasting Can, physically dividing local net on independent subnets (independent groups in pairs related switches) And connect their V united whole With using routers. This problem can only be solved at the network construction stage, but not in the moment of its operation. This is where virtual local area networks (VLANs) come to the rescue. (virtual local area network).

A virtual local area network (VLAN) is a collection of ports on a single network. or more switches (Drawing 2).

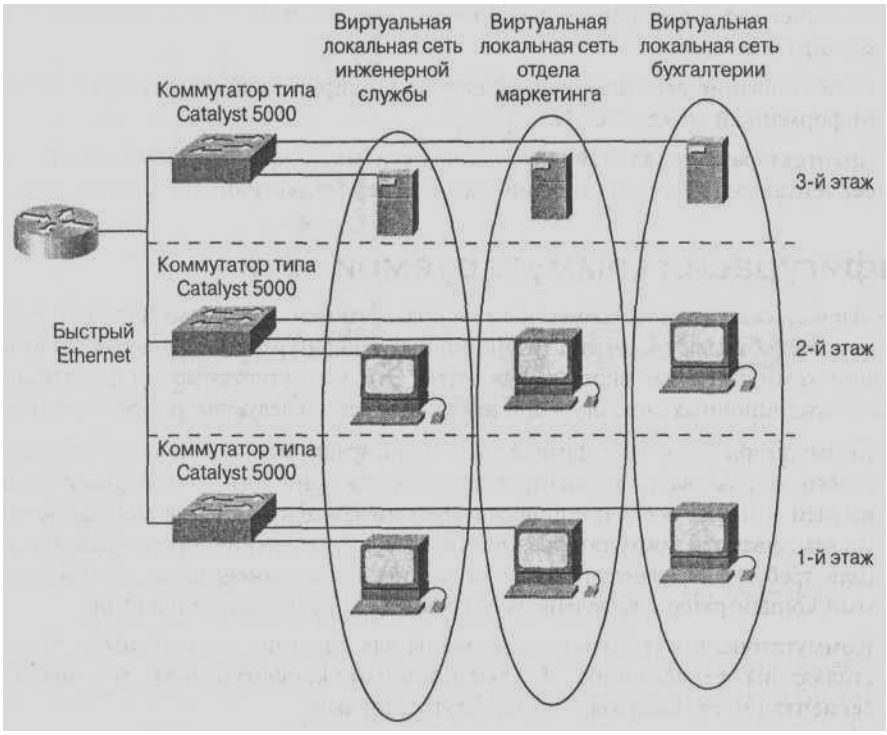


Figure 2.

VLAN allow logically break original local net on some independent local networks without physical interruption of network connections. For this The network administrator must assign which ports belong to each switch To what VLAN. By default All ports switch relate To one VLAN With number 1. The maximum number of VLANs in a switch is equal to the total number of its ports. Correct breakdown local networks on VLAN makes up one of most important tasks design.

VLANs behave the same as physically separated LANs. That is, There is after breakdowns networks on VLAN We we will receive some local networks, which further

must be combined into a single whole using routing on a third network level.

The VLAN concept, in addition to solving the problem of broadcast traffic, providesalso a number of additional advantages: the formation of local networks is not place the location of the nearest switch, and according to the computers belonging to the solution that one or other production tasks; Creation networks By type consumed computing resource And required server services (file server, server bases data). VLAN allow lead different politics security For different virtual networks; move a computer from one network to another without performing physical movements or reconnection.

For exchange information O VLAN switches use main (trunk) protocol. For implementation exchange information O VLAN between You must create trunk ports with switches. A trunk port is a port that used For transmissions information O VLAN V other network devices, attached to this port. Normal ports do not advertise information. about VLAN, But any port Maybe be configured for receiving/transmitting information O VLAN. You must activate the trunk protocol on the required ports, since it is disabledBy default.

The switch port operates in either access mode or trunk mode. Respectively connection, connected To port is or communication access or trunk connection. In access mode, a port belongs to only one VLAN. Port access is connected to the end device: PC, workstation, server, hub. Frames, passing through port access, are ordinary Ethernet frames.

Main roads connections capable support some VLAN. VLAN on various switches get in touch through main protocol. Main roadsports do not belong to a specific VLAN and are used to connect to others switches, routers or servers, having network adapters With opportunity For connections ko many VLAN.

Highways can expand VLAN By all networks. For main goals appoint high-speed ports switches: Gigabit Ethernet And 10 Gigabit .

For multiplexing traffic VLAN exist special protocols, allowing foster ports define, which one VLAN belongs plastic bag. For connections between devices Cisco is used protocol Inter-Switch Link (ISL). At If there is equipment from several manufacturers in the network, the IEEE protocol is used 802.1Q

Without main connections For support VLAN should be organized By one access link for each VLAN. This approach is expensive and inefficient, so trunk lines absolutely necessary during design local networks.

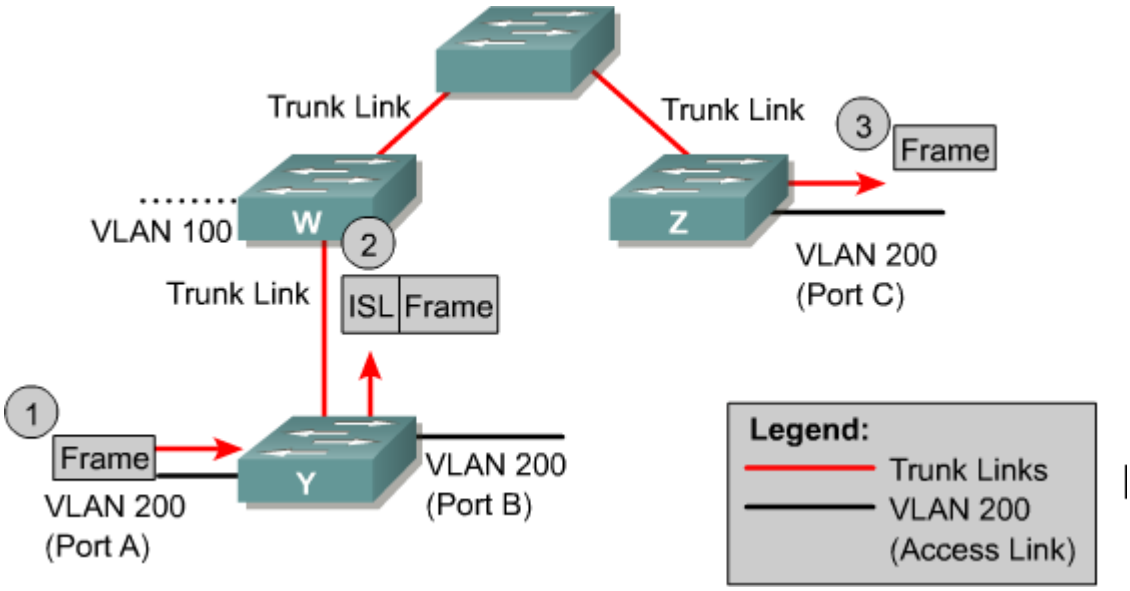


Figure 3.

In Figure 3, ports A and B on switch Y are defined as access links on the same and the same VLAN 200. By definition, they can only belong to one VLAN and not can receive Ethernet frames containing a VLAN identifier. For example, when Y receives traffic from port A to port B, then it does not add the ISL header to the ethernet frames.

Port C on switch Z is also an access port and also belongs to VLAN 200. If port A forwards frame V port WITH, That is happening following:

1. Switch Y receives frame And, comparing number port appointments With number VLAN, defines him like traffic, directed To VLAN 200 on friend switch,

2. Switch Y adds To frame ISL title With number VLAN And forwardsframe through intermediate switch to the main road connection.

3. This process repeats on each switchboard By paths frame To finalport WITH.

4. Switch Z receives frame, deletes ISL title And directs frame on port WITH.

If port located V main mode, That He Maybe be configured or For transport everyone VLAN or limited sets VLAN. Main roads connections are used to connect switches to other switches, routers or with servers, having support VLAN.

According to basic terminology, a backbone is a point-to-point connection that supports multiple VLANs. The purpose of the trunk is to preserve port numbers when creating connections between two devices, forming VLAN.

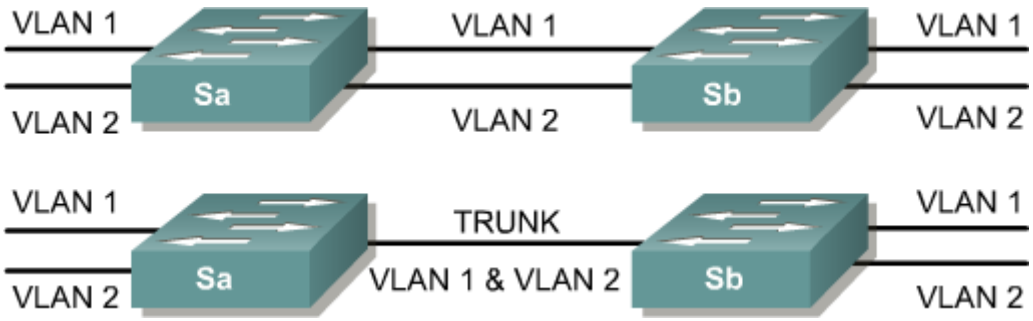


Figure 4.

Upper figure on drawing 4 shows way creation VLAN by way use two physical connections between switches (By one on every VLAN). This solution Badly scales: at addition third VLAN necessary sacrifice two more ports. This solution is inefficient in terms of division loads: low traffic on some links may not be worth the link being in a bunch virtual connections through one physical connection. On lower figure one physical connection capable carry traffic For any VLAN. For achievements this Switch Sa formats frames so that Sb knows which VLAN they are being sent to. For such packet design, either the IEEE 802.1Q or Cisco standard is used. protocol ISL (Inter-Switch Link).

For large networks manual configuration VLAN becomes very labor-intensive task. Cisco VLAN Trunk Protocol (VTP) serves For automatic exchange VLAN information via trunk ports. The advantage of using VTP is that you can control adding, removing or changing networks VLAN from switches on which created VTP servers. After settings yours switches How VTP servers, rest switches yours networks can be configured How clients, which only receive VLAN information. Disadvantage is unnecessary traffic, being created on main ports For devices, which Maybe Not needed this information.

If yours net will contain many switches, containing many virtual networks, located V different switches, Maybe, has meaning use VTP. If your network remains fairly static and VLANs are not be added or change By attitude To initial configurations, That better use static definition virtual networks.

IN topology local networks possible cycles (loops). For example, already three switches connected to each other in a circle form a cycle in the topology. Loops lead to ambiguity in determining the path from the source of packets to the receiver. For solutions this serious problems was developed protocol binder tree STP

(spanning tree protocol). For the topology graph of each VLAN defined in the network, a minimum spanning tree (a graph without cycles) with a vertex at some switch. For physical implementation such trees STP translates redundant ports V state blocking. Calculation trees is produced parallel on everyone switches. Next packages in VLAN they are coming only By paths, certain V built covering trees. At change topology, activation/stop ports is happening recount covering trees.

For creation topology binder tree exist special frames, called bridge protocol data units (BPDUs). Theseframes are being sent And accepted by everyone switches V networks through equal intervals time.

Configuration static VLAN

1. Static VLAN This totality ports on switch, which manuallyassigned by the team iOS at configuration interface.

To create an empty VLAN with number №VLAN on switches Cisco series 2950commands are used

Switch# **vlan database**

Switch(vlan)# **vlan VLAN**

No. Switch(vlan)# **exit** For

example, teams Switch#

vlan database

Switch(vlan)# **vlan 33**

Switch(vlan)# **exit**

will create an empty one VLAN With number 33 And system will give VLAN Name VLAN0033.

Note, What teams are being carried out Not V mode configurations.

The switchport mode command is used to set the interface to dynamic. mode, modes access or mode highways (trunk).

Switch(config-if **)#switchport mode [access | dynamic | trunk]**

Although the access mode is the default mode, in some cases the device,attached To port switch, Maybe translate his V main mode. That's why recommended All non-trunk ports transfer V mode access team **switchport mode access.**

To statically place the current interface into a VLAN, use the commandsSwitch(config-if)#

switchport mode access

Switch(config-if)# **switchport access vlan №number**

Where **№number -** number - number VLAN.

Team **interface range** defines range interfaces For subsequent configurations. For example, ports one through six could be placed in VLAN 10 teams

Switch(config)# **interface range fa0/1 - 6**

Switch(config-if-range)# **switchport access vlan 10**

After settings VLAN check setting teams **show running-config** , **showvlan** And **show vlan brief** .

At setting VLAN remember, What By default All ports are located in VLAN 1.

For creation or configuration highways VLAN You should tune portHow main

Switch(config-if)# **switchport mode trunk**

By default, the last command defines the port as a trunk for allVLAN in networks. However exist situations, when the highway should not supportall VLANs. A typical situation is with broadcast suppression. Broadcasting is sent on every port in VLAN. Main line connection performs How member VLAN Andshould miss All broadcasting. If on friend at the end highways No portsthe required VLAN, then the bandwidth and processor time of the devices are wasted.If VLAN Not is used on friend at the end highways, No needs allow this one VLAN on this highways. By default main ports accept And transmittraffic with everyone VLAN V networks. For abbreviations main traffic use team

Switch(config-if)# **switchport trunk allowed vlan vlan-list**

For example , team

Switch(config-if)# **switchport trunk allowed vlan 3**

Switch(config-if)# **switchport trunk allowed vlan 6-10**

permits on the highway VLAN 3 And then VLAN With 6 By 10. ABOUT volume, which VLANallowed on highways you can see team **show running-config.**

For deletions big number of VLANs from highways it's easier at first delete All VLAN, A then selectively allow.

The simplest way translate connection V mode access This ask on interfaces With hertwo sides By team

SwitchA(config-if)# **switchport mode access**

The simplest way translate connection V mode access This ask on interfaces With hertwo sides By team

SwitchA(config-if)# **switchport mode trunk**

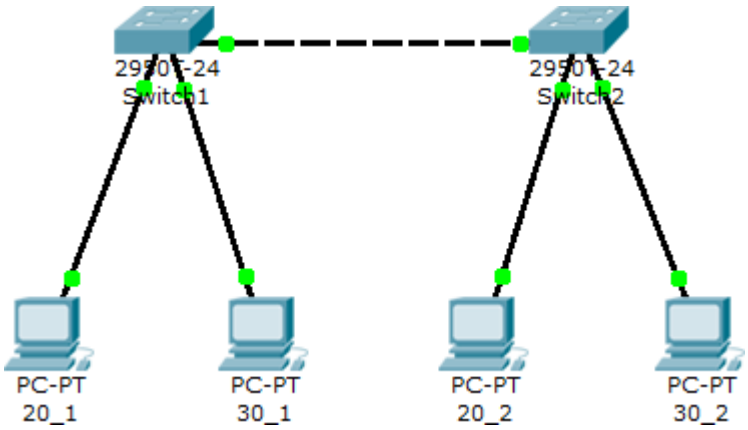
Practical Part

1. Assemble the topology shown in Figure 5. Connect the switches in two Gigabit Ethernet (gi1/1 and gi1/2) connections. Connect computers to the interfaces. according to table 1. Assign addresses to computers according to table 1. All computers are included V one subnet 172.16.0.0 255.255.0.0. Routes By default on computersNot install. Ping net.

Let's create two VLANs in our network. We'll place computers 20_1 and 20_2 in VLANs with number 20, A computers 30_1 And 30_2 let's place in VLAN with number 30.

Switch1(conf)# **interface fa0/2**

Switch1(conf-if)# **switchport access vlan**
20Switch1 (conf-if **)** # **interface fa0/3**
Switch1(conf-if)# **switchport access vlan**
30Switch2 (conf)# **interface fa0/2**
Switch2(conf-if)# **switchport access vlan**
20Switch2 (conf-if)# **interface fa0/3**
Switch2(conf-if)# **switchport access vlan**
30



Drawing 5.

Computer	Switch1	Switch2	Address
20_1	Fa0/2		172.16.20.1/16
30_1	Fa0/3		172.16.20.2/16
20_2		Fa0/2	172.16.30.1/16
30_2		Fa0/3	172.16.30.2/16
	Gi1/1	Gi1/1	

Table 1.

On both switches check results of creation VLAN, For exampleSwitch1# sh vl name 20

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   20                               active    Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0
```

And

```
Switch1#sh  vl br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
20   20                               active    Fa0/2
30   30                               active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Since there is no exchange of VLAN information between switches, computers will be ping only ourselves myself.

We organize highways on switches. For this we use Gigabit Ethernet portSwitch1(conf)# **interface gi1/1**

Switch1 (conf-if)# **switchport trunk allowed vlan add**

20Switch1 (conf-if)# **switchport trunk allowed vlan add**

30Switch1 (conf-if)# **no shutdown**

Switch2 (conf)# **interface gi1/1**

Switch2 (conf-if)# **switchport trunk allowed vlan add**

20Switch2 (conf-if)# **switchport trunk allowed vlan add**

30Switch2 (conf-if)# **no shut**

Now computers within the same VLAN should be able to ping, and computers located V various VLAN shouldn't ping (cm. table 2).

Ping from/to	20_1	30_1	20_2	30_2
20_1	Yes	No	Yes	No
30_1	No	Yes	No	Yes
20_2	Yes	No	Yes	No
30_2	No	Yes	No	Yes

Table 2.

Save configurations switches.

2. Let's save it topology previous task in new file. In this topology The router is connected by two links to the fa0/1 interfaces of the switches (Figure 6). Check again that computers within the same VLAN can ping, and computers located V various VLAN Not are pinged.

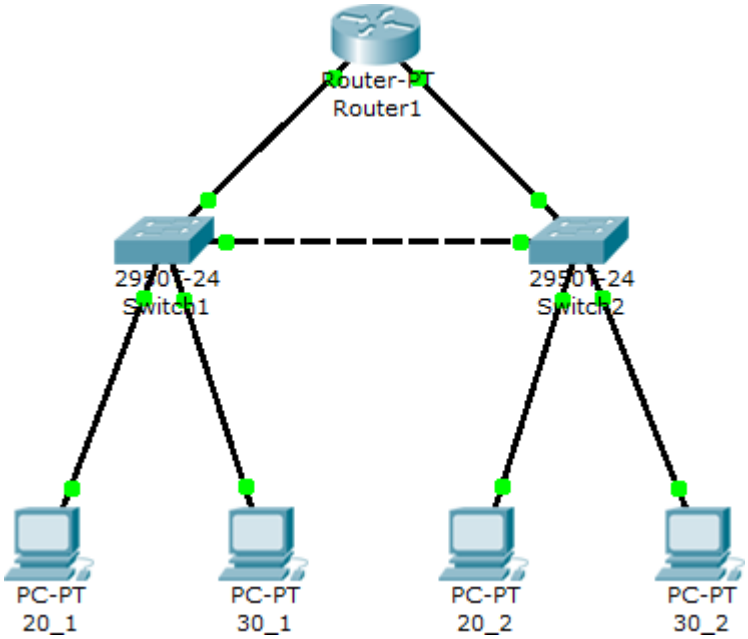


Figure 6.

Let's set the task of combining virtual networks using a router. For this follows break ours net 172.16.0.0/16 on two subnets 172.16.20.0/24 And 172.16.30.1/24. For this Just let's change masks at computers on 255.255.255.0.

Now computers can be pinged within the same VLAN and within the same IP subnets, A This Means only ourselves on yourself.

Let's introduce on switches interfaces, connected To router V virtual networks

Switch1(conf)# **interface fa0/1**

Switch1(conf-if)# **switchport access vlan**

20Switch2(conf)# **interface fa0/1**

Switch2(conf-if)# **switchport access vlan**

30Let's configure IP addresses on router

Router(conf)# **interface fa0/0**

Router(conf-if)# **ip address 172.16.20.254 255.255.255.0**
Router(conf-if)# **no shutdown**
Router(conf-if)# **interface fa1/0**
Router(conf-if)# **ip address 172.16.30.254 255.255.255.0**
Router(conf-if **)#no shutdown**

Now router routes our two networks 172.16.20.0/24 And 172.16.30.1/24. Let's add on ours computers routing By default on interfaces router.

Host	Gataway
20_1	172.16.20.254
20_2	172.16.20.254
30_1	172.16.30.254
30_2	172.16.30.254

Now from everyone devices ours networks We Can ping All our IP addresses.

3. Let's show you, How With using transit lines, We Can save money ports.

Let's change the topology by moving the gi1/2 trunk from the switches to the interface fa0/0 router (drawing 7). Let's load it topology V simulator. Let's load it By one after another V each device, except router, saved configurations. Note that in the Switch2 configuration, the trunk line is not installed on gi1/2. needed, Although she And Not interferes.

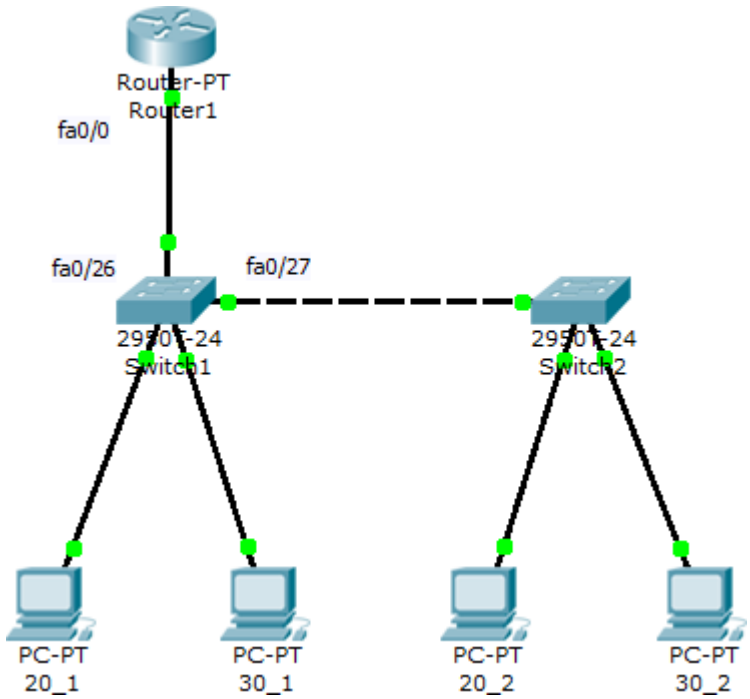


Figure 7.

On router breakdown interface fa0/0 on two subinterface fa0/0.20 And fa0/0.30. We will define dot1q insapulation on them and place them in virtual networks 20 and 30, respectively.

Router(conf)# **interface FastEthernet0/0.20**
Router(conf-subif)# **encapsulation dot1q 20**
Router(conf-subif)# **ip address 172.16.20.254**
255.255.255.0 Router(conf-subif)# **interface**
FastEthernet0/0.30 Router(conf-subif)# **encapsulation**
dot1q 30

Router(conf-subif)# **ip address 172.16.30.254 255.255.255.0**
Let's see table routesRouter#

show IP route

```
C       172.16.20.0 is directly connected, FastEthernet0/0.20
C       172.16.30.0 is directly connected, FastEthernet0/0.30
```

Check that you can ping all addresses on the network from each device. Do it on Router team extended ping from addresses 172.16.20.1 computer

20_1 from VLAN 20, connected To switchboard Switch1 To address 172.16.30.2computer

30_2 from VLAN 30, connected To switchboard Switch2

```
Router#ping
Protocol [ip]:
Target IP address: 172.16.30.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:172.16.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Control questions

1. Why prefer build local networks With help switches, Anot concentrators?
2. Which exist methods For sending a frame through switch?
3. How switch recognizes the MAC addresses connected devices?
4. Where And How V switchboard are stored addresses connected devices?
5. What such virtual compound And How for a long time it exists?
6. How much big local the network can be created With help switches?
7. How it is customary to build big local networks?
8. What is main obstacle For creation large local networksby using alone switches?
9. What such domain broadcasting?
10. How reduce domain broadcasting?
11. What such VLAN?
12. Which problems local networks solves VLAN?
13. How V local networks organize exchange VLAN information?
14. IN what kind modes are working ports switch?
15. Which VLAN belongs main port?
16. How spread one VLAN on some switches?
17. Can whether organize some VLAN on several switches withoutuse highways?
18. Why are they needed? protocols ISL And IEEE 802.1Q?

19. For what needed highways V V local networks?
20. Which solves problems VTP?
21. Which solves problems STP?
22. What kind teams Can organize VLAN?
23. Which team translate port V mode access And V mode highways?
24. Which team Can get information O VLAN?
25. IN local networks there are eleven VLAN. How many routersnecessary For associations all 11 VLAN in united whole?

Order execution And surrender work

1. To study theoretical And practical Part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute V Packet Tracer practical Part.
4. Do it V Packet Tracer exercise For independent work.
5. For your option, present to the teacher the opportunity to completeextended ping between any addresses For topologies on drawings 6 And 7.
6. Make out report. Content report Look below.
7. Protect report.

Exercise For independent work

Repeat All points practical parts For IP networks enterprises, according tooptions. Practical Part done For networks 172.16.0.0/16.

Var.	Net	Var.	Net	Var.	Net
1	2.1.0.0/16	5	6.1.0.0 /16	9	10.1.0. 0/16
2	3.1.0.0/16	6	7.1.0.0 /16	10	11.1.0. 0/16
3	4.1.0.0/16	7	8.1.0.0 /16	11	12.1.0. 0/16
4	5.1.0.0/16	8	9.1.0.0 /16	12	13.1.0. 0/16

Create those same screenshots, What And at execution practical parts.

Content report.

Report is being prepared V electronic view And is printed. Report contains
1. Screenshots topologies, created at execution practical parts.
2. Configurations of all routers from configuration.txt files,created when performing practical parts.

3. Configurations everyone routers from .txt files, created at executiontasks For independent work.

5. All screenshots, specified V task For independent work

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION
FEDERAL STATE AUTONOMOUS EDUCATIONAL
INSTITUTION OF HIGHER EDUCATION
NORTH CAUCASIAN FEDERAL UNIVERSITY

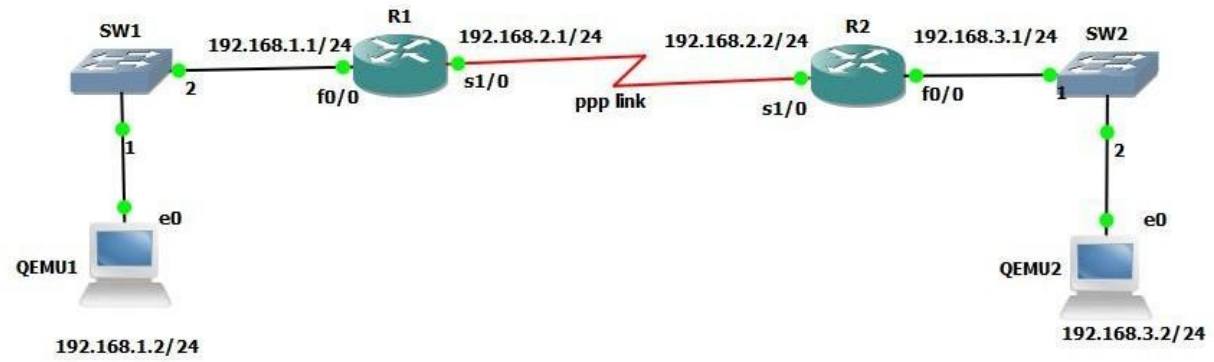
GUIDELINES

for completing independent work
By discipline "Principles of Communications / Принципы коммуникации"
for students in the field of study
02.04.01 Mathematics and Computer Science

Stavropol, 2026

Practical class №15. Network Layer Protocols (Part 6).

1. IN program GNS3 create next topology:



Drawing 1 - Topology networks

Basic configuration of routers for working with the PPP protocol consists of the encapsulation ppp command on serial router interfaces, in this case on the s1/0 interfaces of each of routers. An example of the basic configuration of each router shown below:

Router R1
Press RETURN to get
started!R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#int
f0/0R1(config-if)#int
s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ip address 192.168.2.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

Router R2 Press RETURN
to get started!R2>

```
R2>ena
R2#config t
R2(config)#int f0/0
R2( config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2( config-if)#int
f0/0R1(config-if)#int
s1/0
R2( config-if)#encapsulation ppp
R2( config-if)#ip address 192.168.2.2
255.255.255.0R2(config-if)#no shutd
R2( config-if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

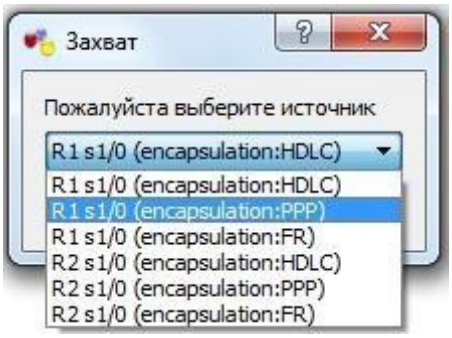
2. Launch WireShark

Before those How tune router R2 launch analyzer Wireshark network protocols for viewing the exchange of service packets between R1 and R2. To do this, you need to right-click on channel between routers and in the pop-up menu select a team "start capturing", How it is shown on drawing 2



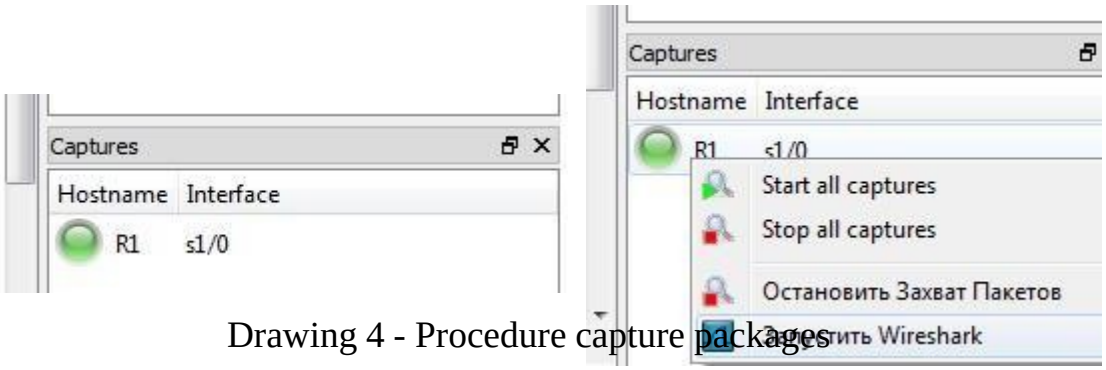
Drawing 2 - Capture packages

In the window that appears, select the encapsulation type and interface number. router, as shown in Figure 3. Then press the button "OK"



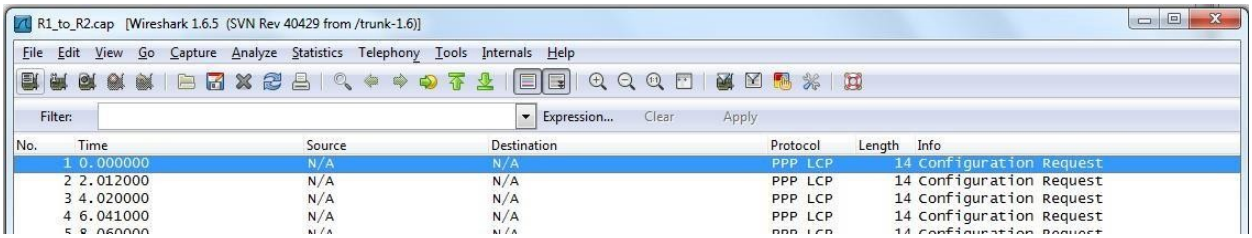
Drawing 3 - Choice type protocol

In the lower left "Capture" window, you will see the router name and number interface, With whom will happen capture packages, then click right button mice By name router And select "Start Wireshark".



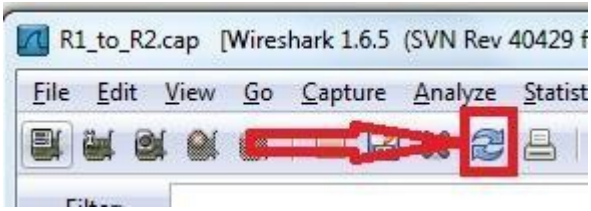
Drawing 4 - Procedure capture packages

After what will load program Wireshark drawing 5.



Drawing 5 - Window programs Wireshark

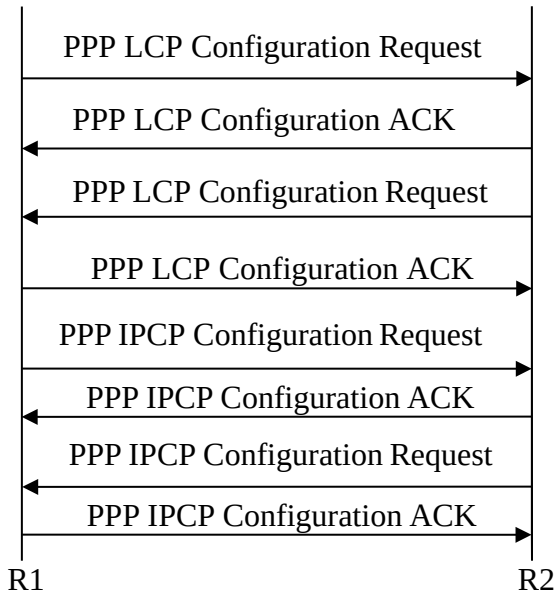
After configuring the second router in the toolbarprograms WireShark click on button "Refresh" drawing 6.



Drawing 6 - Update captured packages

3. Analysis captured packages

Next, look for PPP negotiation packets among the captured packets. connections, scenario establishments PPP connections next:



Drawing 7 - Scenario establishments PPP connections

Analyze the captured messages, think about how to determine which PPP LCP Configuration Request message does it correspond to? message PPP LCP Configuration ACK. Take a look options protocols LCP And IPCP.

4. Setting up hosts

IN this work V quality operating room systems hosts are used Linux, For settings IP parameters each Linux cars necessary enter next commands:

QEMU1:

Team	Meaning
sudo su	Entrance V mode superuser (mode administrator)
ifconfig eth0 192.168.1.2 netmask 255.255.255.0	Ask IP address and mask to the host
route add -no 0/0 gw 192.168.1.1	ask IP address gateway By default (default gateway)

After input teams With help utilities ping check availabilitygateway By default:

ping 192.168.1.1

combination key Ctrl+Z stop sending packages ICMP

QEMU2:

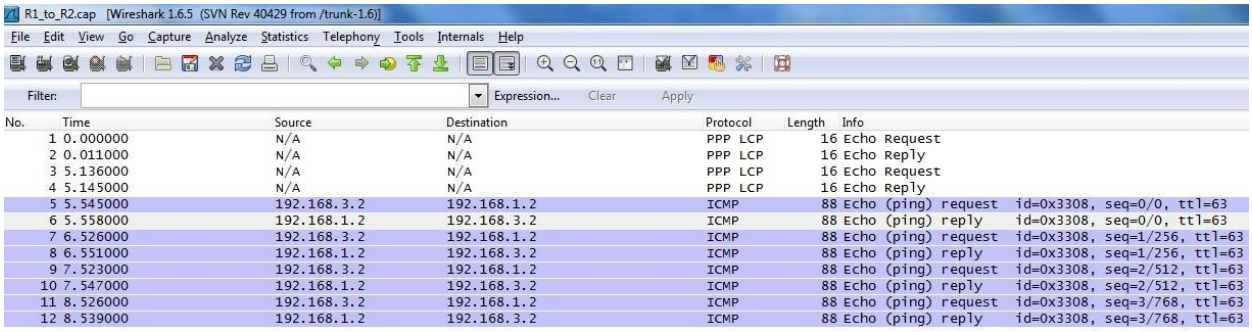
Team	Meaning
sudo su	Entrance V mode superuser (mode administrator)
ifconfig eth0 192.168.3.2 netmask 255.255.255.0	Ask IP address and mask to the host
route add -no 0/0 gw 192.168.3.1	ask IP address gateway By default (default gateway)

ping 192.168.3.1

Also check availability all the rest interfaces: 192.168.2.1,192.168.2.2, 192.168.1.1, 192.168.1.2.

5. Interception IP packages

After Togo How will recruited team ping 192.168.1.2 With hosta 192.168.3.2, using Wireshark, capture the transmitted ICMP echo packets request And ICMP echo reply.



You will analyze headings everyone protocols each from messages ICMP.

5. Authentication using the CHAP protocol (Challenge handshake)authentication protocol)

Please specify Name router With help teams **hostname[device_name]** V mode global configurations router

Ask password For entrance V user mode With help teams **enable password [password]** or **enable secret [password].** First The command saves the password in the configuration file in clear text, the second one in encrypted. WITH help teams **username [Name] password [password]** ask parameters remote router. IN quality **[Name] -** necessary use Name remote router, given With using **username** , you must use the password for **[password]** enter privileged mode of the remote router. Enabling CHAP authentication occurs after entering the **ppp authentication command chap** on each interface. At this necessary to password was same With both sides. Example settings each router shown below:

Router R1

Press RETURN to get started!
R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#int
f0/0R1(config-if)#int
s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ip address 192.168.2.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

R1(config)#enable password asdfg
R1(config)#hostname router_1
router_1(config)#int s1/0
router_1 (config-if)#ppp authentication
chaprouter_1(config-if)#exit
router_1(config)#username router_2 password asdfg

Router R2

Press RETURN to get started!
R2>
R2>ena
R2#config t

R2(config)#int f0/0
R2(config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2(config-if)#int
f0/0R1(config-if)#int
s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ip address 192.168.2.2
255.255.255.0R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#ip ro fываn ute 192.168.1.0 255.255.255.0 192.168.2.1

R2(config)#hostname router_2
router_2(config)#enable secret asdfg
router_2(config)#username router_1 password asdfg
router_2(config)#int s1/0
router_2 (config-if)#ppp authentication chap

After input configurations turn it off And turn on any from sequential interfaces For Togo to look procedure establishments connections With taking into account authentication. For viewingconnection establishment procedures update the list of intercepted packets V Wireshark. Below shown scroll messages, which necessary intercept

routeizer	Message	routeizer	Direction transmissions package
Router_1	1) PPP LCP Configuration Request 2) PPP LCP Configuration Ack 3) PPP LCP Configuration Request 4) PPP LCP Configuration Ack 5) PPP CHAP Challenge (NAME='router_2', VALUE=0x31c2e2f7e8795787c8b55eee5e619bed) 6) PPP CHAP Response (NAME='router_2', VALUE=0x608ffbf914c5994f126116d099840) 7) PPP CHAP Challenge (NAME='router_1', VALUE=0x006dd0d171b4dcd44af7ce2b7441) 8) PPP CHAP Response (NAME='router_1', VALUE=0xa50de75394abed934d4f6ffaa9c4c) 9) PPP CHAP Success (MESSAGE='') 10) PPP CHAP Success (MESSAGE='') 11) PPP IPCP Configuration Request 12) PPP IPCP Configuration Ack 13) PPP IPCP Configuration Request 14) PPP IPCP Configuration Ack	Router_2	1. ----------> 2. <---------- 3. <---------- 4. ----------> 5. ----------> 6. <---------- 7. ----------> 8. <---------- 9. ----------> 10. <---------- 11. ----------> 12. <---------- 13. ----------> 14. <----------

6. Authentication By protocol PAP (password authentication protocol)

WITH help teams **username [Name] password [password]** ask parameters remote router. **[Name] -** This Name must sendremote router, V quality **[password]** necessary use password, which will send remote router. Turning on PAP authentication occurs after entering the command **ppp authentication pap** on each interface. In interface configuration mode, you must enter team **ppp pap sent-username [Name] password [password].** Example settings each router shown below:

Router R1

Press RETURN to get
started!R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#int
f0/0R1(config-if)#int
s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ip address 192.168.2.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

R1(config)# username **switch** password **asdfg**
R1 (config)#int s1/0
R1 (config-if)# ppp authentication pap
R1 (config-if)# ppp pap sent-username *router_1* password *qwerty*

Router R2

Press RETURN to get
started!R2>
R2>ena
R2#config t
R2(config)#int f0/0
R2(config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2(config-if)#int
f0/0R1(config-if)#int
s1/0

R2(config-if)#encapsulation ppp
R2(config-if)#ip address 192.168.2.2
255.255.255.0R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

R2(config)# username *router_1* password *qwerty*
R2 (config)#int s1/0
R2 (config-if)# ppp authentication pap
R2 (config-if)# ppp pap sent-username **switch** password **asdfg**

After input configurations turn it off And turn on any from sequential interfaces For Togo to look procedure establishments connections With taking into account authentication. For viewingconnection establishment procedures update the list of intercepted packetsV Wireshark.

7. Encryption By protocol MPPE

For settings encryption necessary configure protocol MS-CHAP authentication, since MPPE uses keys generated by this protocol, the configuration of which is similar to the configuration of the CHAP protocol. Please specify Name router With help teams **hostname [device_name]** V mode global configurations router. Ask password For entrance V user mode With help teams**enable password [password]** or **enable secret [password].** First team saves password V file configurations V open view, second V encrypted. WITH help teams **username [Name] password [password]** ask parameters remote router. IN quality **[Name]** - necessary use Name remote router given With using **username** , you must use the password for **[password]** enter privileged mode of the remote router. Enabling authentication MS-CHAP is happening after input teams **ppp authentication ms-chap** on one from interfaces. On friend interface

necessary enter team **ppp chap password [password]** . Launch funds encryption is happening by way input teams **ppp encrypt mppe [key width] required** on both sides. In this example is used key bit depth V 56 bit. Example settings each routers are shown below:

Router R1

Press RETURN to get
started!R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#int s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ip address 192.168.2.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

R1(config)#enable password asdfg
R1(config)#hostname router_1
router_1(config)#username router_2 password asdfg
router_1(config)#int s1/0
router_ 1(config-if)#ppp authentication ms-chap

---

router_1(config-if)# ppp encrypt mppe 40 required

Router R2

Press RETURN to get
started!R2>
R2>ena
R2#config t
R2(config)#int f0/0
R2(config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2(config-if)#int
f0/0R1(config-if)#int
s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ip address 192.168.2.2
255.255.255.0R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

R2(config)#hostname router_2

```
router_2(config)#username router_1 password asdfg
router_2(config)#enable secret asdfg
router_2(config)#int s1/0
router_2 ( config-if)# ppp authentication ms-
---------------------------------------------------------------------------
chaprouter_2(config-if)#ppp encrypt mppe 40
```

After input configurations turn it off And turn on any from sequential interfaces For Togo to look procedure establishments connections With taking into account authentication. For viewingconnection establishment procedures update the list of intercepted packetsin Wireshark. Also send ICMP messages from one host to another with using the utility ping.

7. Compression data

7.1 Compression useful data With help MPPC

If ppp is used on low-speed communication channels, then in this In this case, it is necessary to use compression of ppp packets, one of the protocols compression using the Lumpel-Ziv algorithm is the MPPC protocol (Microsoft Point- to-Point Compression) . For activation this protocol on each of interfaces, you need to enter the **compress mppc command.** To check that What is happening compression send ICMP message size 512 byte, and with help WireShark take a look in How many once it will compressed **.** For To send an ICMP packet of any size, you must enter the command **ping [ip address] size [packet size in bytes]** . Example of configuration of each router shown below:

Router R1

```
Press RETURN to get
started!R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1( config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1( config-if)#int
f0/0R1(config-if)#int
s1/0
R1( config-if)#encapsulation ppp
```

R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)# compress
mppcR1(config-if)#no shutd
R1(config-if)#exit
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

Router R2
Press RETURN to get
started!R2>
R2>ena
R2#config t
R2(config)#int f0/0
R2(config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2(config-if)#int
f0/0R1(config-if)#int
s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)# compress
mppcR2(config-if)#no shutd
R2(config-if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
R2(config)# ctrl +z
R2(config)#ping 192.168.2.1 size 512

7.1 Compression fields addresses And management V title PPP

When agreeing on the option of compression of address and control fields, it is necessaryenter two commands:

ppp acfclocalrequest - allows sending compression option tomessage Conf req

ppp acfc remote apply - allows accept from remote sidesmessage Conf req With compression option address fields and management

7.2 Compression fields protocol V title PPP

When negotiating the protocol field compression option, the PPP protocol will use single-byte field protocol V place two-byte. For inclusions this option necessary Also use two commands:

ppp pfc local request - allows you to send a compression option in a message Conf req

ppp pfc remote apply - позволяет принимать от удаленной стороны message Conf req With option compression fields addresses And management

7.3 Compression fields headings IP And TSR

This option agrees V sessions IPCP And described V RFC3544, For To enable this option when establishing a ppp connection, you must each in the interface, enter the command:

IP RTP header compression - compression IP, udp, tcp, rtp

headingsIP tcp header compression -- compression IP, udp, tcp

headings

8. Protocol monitoring quality channel connections LQM

The LQM protocol is described in RFC 1989 recommendation. It allows you to determine quantity distorted packages, For his launch necessary enter team V mode configurations interface:

ppp quality [quantity distorted packages]

9. Turning on numbered regime

IN numbered mode every frame PPP has mine ordinal number, which cyclically repeats from 0-7, V such mode every transmitted frame PPP confirmed, those the most guaranteed delivery data. IN this mode For guaranteed delivery data A sliding window mechanism of 7 packets is used. To activate such regime necessary on each interface enter next team in mode configurations interface:

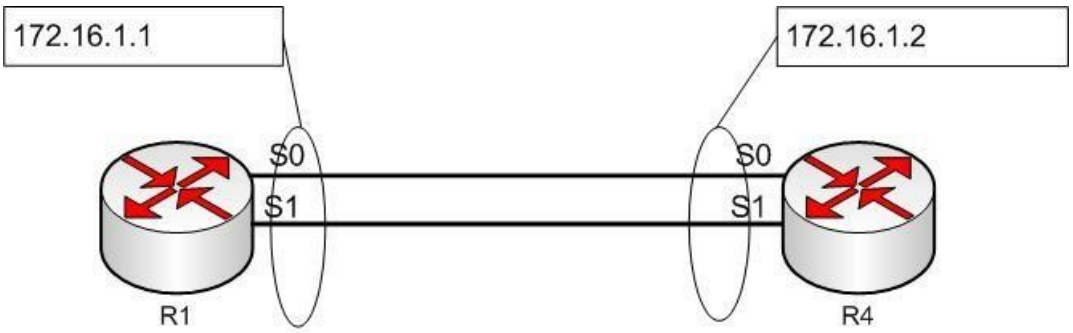
ppp reliable-link

10. Installation size frame PPP

By default, the PPP protocol uses a frame size of 1500 bytes. To change this parameter you need to enter the following commands in the mode configurations interface:

mtu [размер кадра]
ppp mtu adaptive

11. Multichannel PPP



Drawing 8 - MPPP

This protocol applies V volume case, When some physical channels necessary unite V one logical. Example basic configurations each router shown below:

Router R1

Press RETURN to get
started!R1>
R1>ena
R1#config t
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#int multilink 1
R1(config-if)#encapsulation
ppp
R1(config-if)#ip address 192.168.2.1
255.255.255.0R1(config-if)#no shutd
R1(config-if)#exit
R1(config)#int
s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp multilink
group 1R1(config-if)#no shutd
R1(config-if)#exit
R1(config-if)#int
s1/1
R1(config-if)#encapsulation ppp
R1(config-if)#ppp multilink
group 1R1(config-if)#no shutd
R1(config-if)#exit

R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2

Router R2

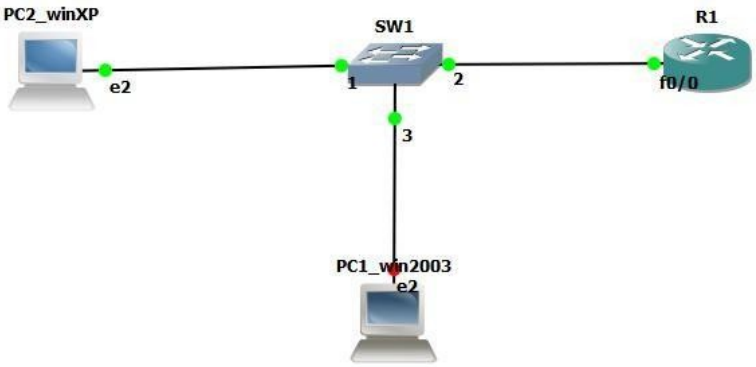
Press RETURN to get started!
R2>
R2>ena
R2#config t
R2(config)#int f0/0
R2(config-if)#ip address 192.168.3.1
255.255.255.0R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#int multilink 1
R2(config-if)#encapsulation
ppp
R2(config-if)#ip address 192.168.2.2
255.255.255.0R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#int
s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp multilink
group 1R2(config-if)#no shutd
R2(config-if)#exit
R2(config-if)#int
s1/1
R2(config-if)#encapsulation ppp
R2(config-if)#ppp multilink
group 1R2(config-if)#no shutd
R2(config-if)#exit
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
R2# show ppp multilink

Multilink1, bundle name is R1
  Endpoint discriminator is R1
  Bundle up for 00:11:03, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
  0/0 fragments/bytes in reassemblies list
    0 lost fragments, 2 reordered
    1/20 discarded fragments/bytes, 2 lost received
    0x11 received sequence, 0x2E sent sequence
  Member links: **2 active** , 0 inactive (max not set, min not set)
**   Se1/1, since 00:07:44**
**   Se1/0, since 00:07:39**
No inactive multilink interfaces

12. PPPoE

12.1 Configuration RRPoE on router

IN program GNS3 collect next diagram drawing 12.1.1



Drawing 9 - RRPoE topology

To configure a router as a PPPoE servernecessary enter next commands:

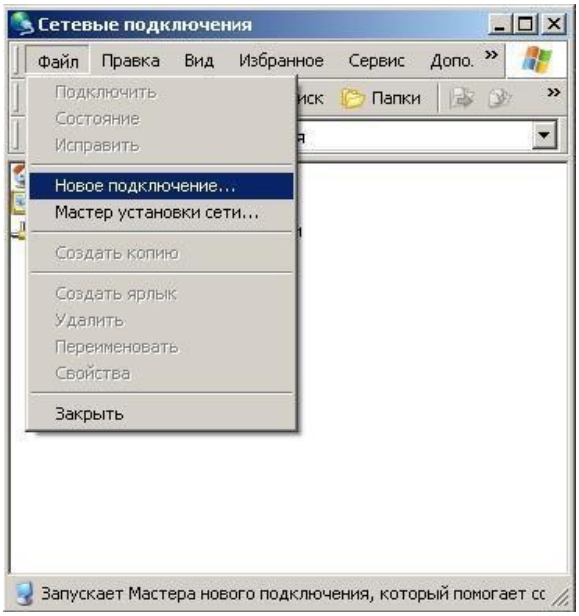
```
R1#config t
R1(config)#vpdn enable
R1(config)#vpdn-group
1
R1( config-vpdn)#accept-dialin
R1(config-vpdn-acc-in)#protocol pppoe
R1( config-vpdn-acc-in)#virtual-template
1R1(config-vpdn-acc-in)#exit
R1( config-vpdn)#exit
R1(config)#int virtual template 1
R1( config-if)#ip unnumbered fastEthernet 0/0
R1(config-if)#mtu 1400
R1( config-if)#ppp authentication chap
R1( config-if)#peer default ip address dhcp-pool
10R1(config-if)#exit
R1( config)#int f0/0
R1(config-if)#no
shutdR1(config-if)#
R1( config-if)#pppoe
enableR1(config-if)#exit
R1(config)#username WinXP password
qwertyR1(config)#ip dhcp pool 10
R1(dhcp-config)#network 1.0.0.0 255.0.0.0
```

12.2 Setting up client parts

Setting up PPPoE connections V Windows 2003/XP.

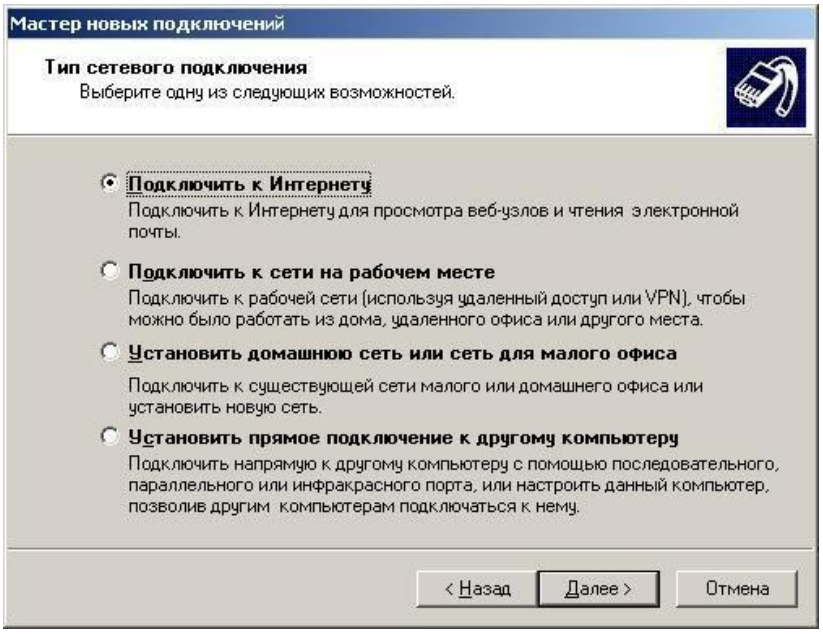
1. Click menu **Start** , select submenu **Setting up** , then **Network connections** ,

2. IN menu windows **Network connections** choose paragraph **File** , further, **New connection** .



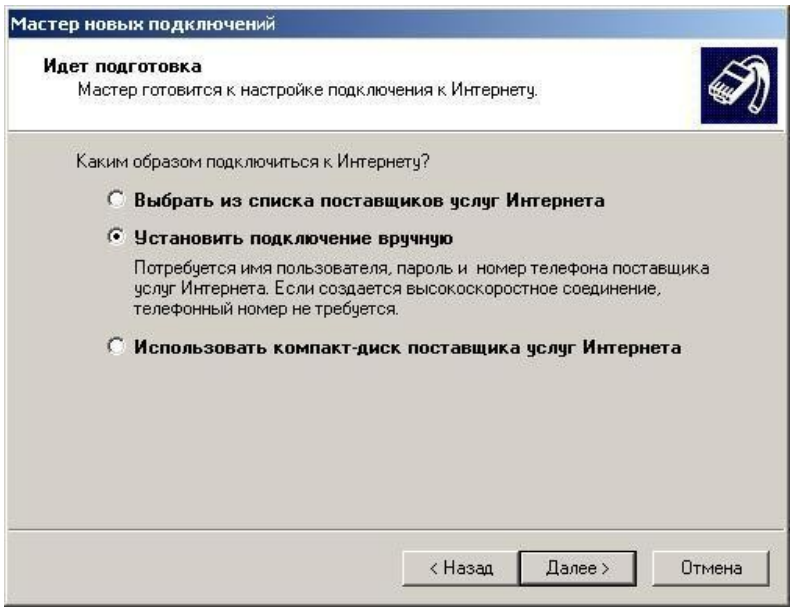
Drawing 12.2.1 - Network connections

3. IN master new connections press **More** And we choose paragraph **Connect To Internet** , press **Next**



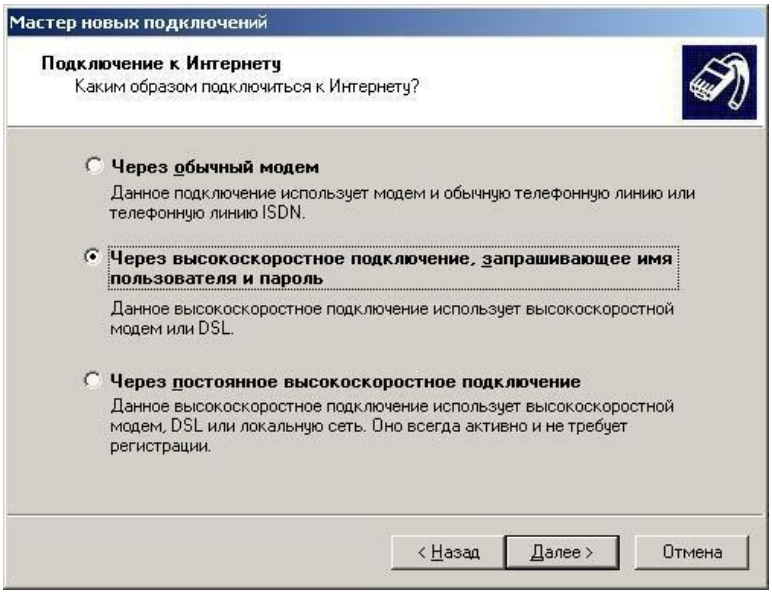
Drawing 12.2.2 - Choice type network connections

4. Select option **Install connection manually** , press **Next**



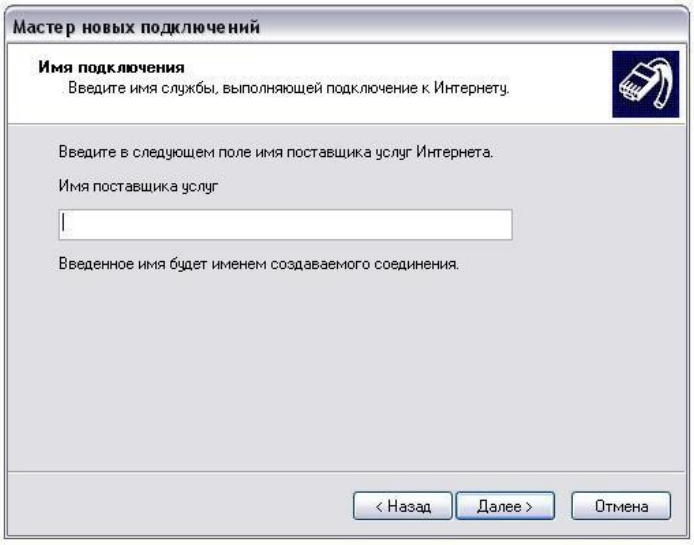
Drawing 12.2.3 - Choice method settings network connections

5. Select an option **Via a high-speed connection, requesting Name user And password** , press **Next**



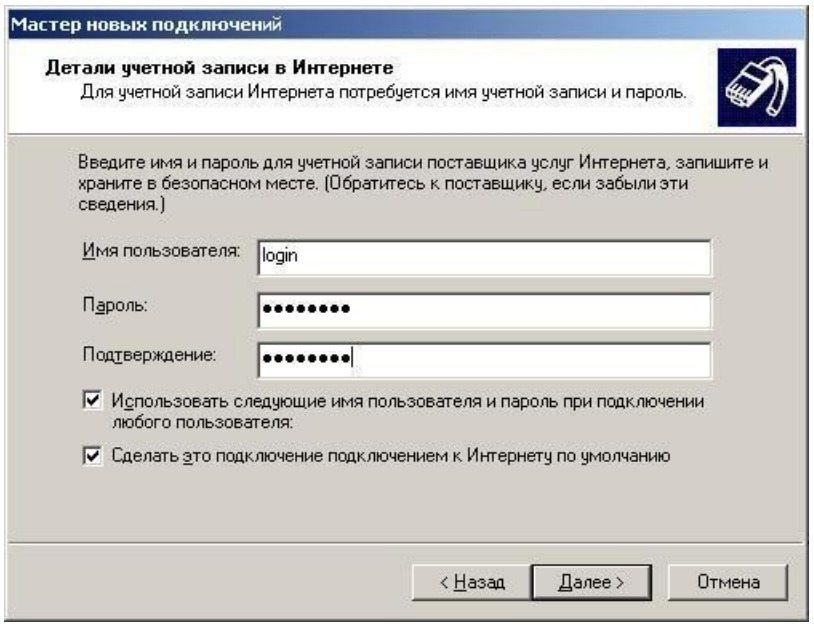
Drawing 12.2.4 - Choice method connections

6. Next V field **Name supplier services** we enter arbitrary Name,for example, **Inet-Comfort** , press **Next**



Drawing 12.2.5 - Setting up name supplier services

7. IN next window we enter **Login** And **Password** V corresponding fields, press **Next** .



Drawing 12.2.6 - Setting up an account records

IN ours case login =winxp, password=qwerty

8. We select paragraph **Add label connections on worker table** ,press **Ready** .
9. Install PPPoE compound, And implement capture packages By establishment PPPoE connections.

Content report:

1. Three topology drawing 1, 8, 9;
2. Listing settings routers For each topology;
3. Captures approvals PPP connections For everyone studied options;
4. Capture By establishment PPPoE connection.

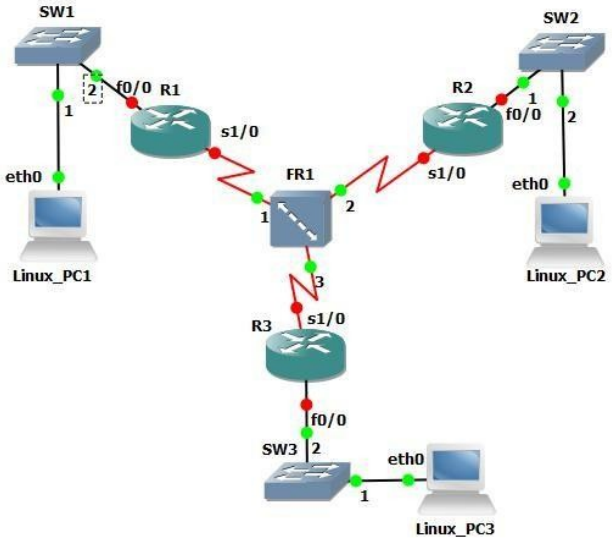
Control questions:

1. Structure package PPP;
2. Procedure establishments RRR connections;
3. Options protocol RRR;
4. Messages protocol LCP;
5. Messages protocol IPCP;
6. Procedure authentication By protocol CHAP;
7. Procedure authentication By protocol PAP;
8. Coordination method encryption By protocol MPPE;
9. Coordination algorithm compression By protocol MPPC;
10. Purpose protocol MPPP And procedure his approvals;
11. Establishment connections By protocol PPPoE;
12. Coordination IP parameters By protocol IPCP For clients RRPoE.

Practical class No. 16 - Network Layer Protocols (Part 7).

IN this laboratory work necessary configure interfaces Frame Relay.

1. Make up next topology

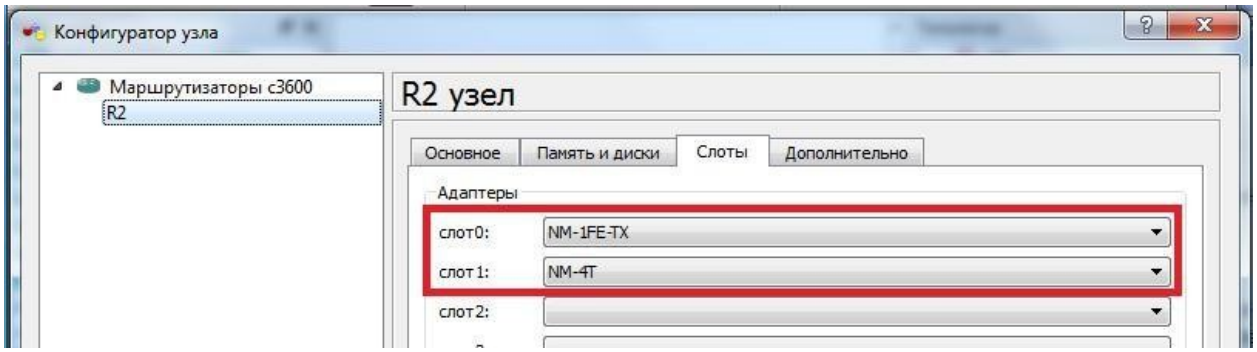


Drawing 13 - Under study topology

Table 1 - IP interface addresses

R1	R2	R3	Linux_PC1	Linux_PC2	Linux_PC3
F0/0 - 2.0.0.1/8 S1/0 - 1.0.0.1/8	F0/0 - 3.0.0.1/8 S1/0 - 1.0.0.2/8	F0/0 - 4.0.0.1/8 S1/0 - 1.0.0.3/8	2.0.0.2/8	3.0.0.2/8	4.0.0.2/8

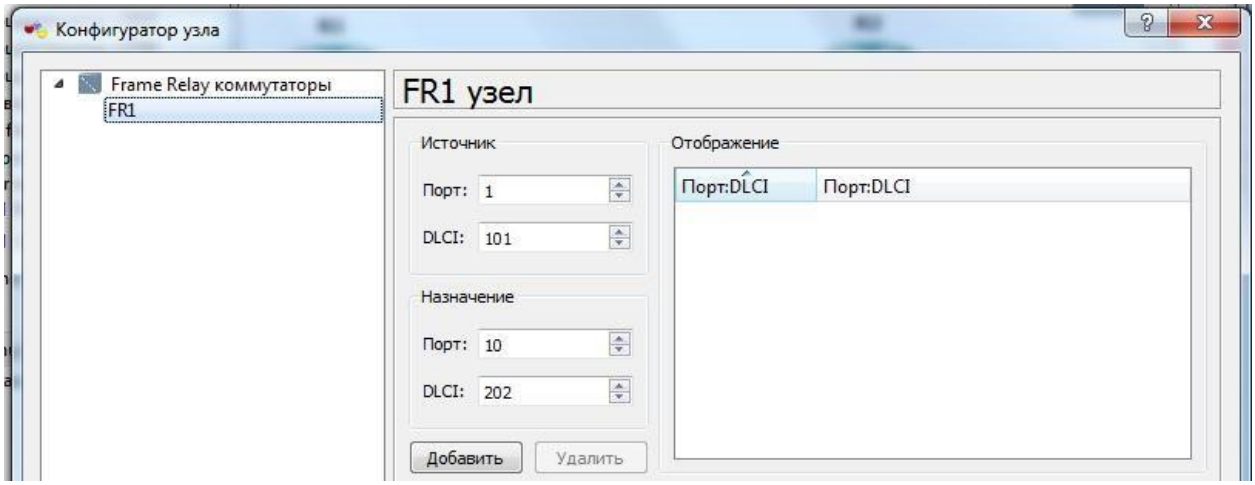
IN this example V quality routers are used Cisco 3640 c network modules NM-1FE-TX And NM-4T, configuration everyone routers are identical. To configure network modules, click on Right-click on the router and select "Configure", then what will open window Configurator node" Figure 14.



Drawing 14 - Configurator node

For settings switch Frame Relay click By him rightbutton mice, after what choose paragraph "tune", will open window

Configurator node" drawing 15.



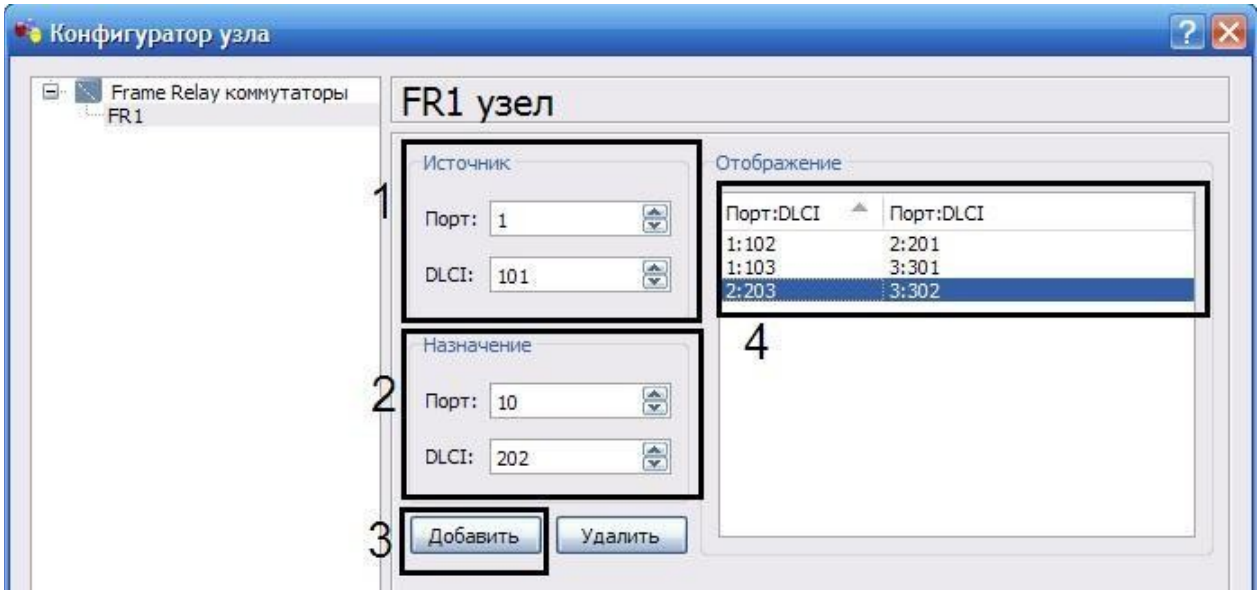
Drawing 15 - configurator node Frame Relay

In this window, you need to create a commutation table for the switch.Frame Relay. IN laboratory work necessary connect three router, first router will connected With first portswitch, second router with second port And third router With third port. Ports on switchboard Frame Relay will appear, When will compiled table switching. IN this laboratory work table switching will look nextway:

Таблица 2 - Таблица коммутации

	Port	DLCI	Port	DLCI
1	1	102	2	201
2	1	103	3	301
3	2	203	3	302

According to line 1 of the switching table, packets arriving at port 1 FR switch with DLCI=102 will be redirected to port 2 with replacement DLCI identifier at 201, the same thing happens when on port 2 A packet with DLCI=201 arrives, it will be redirected to port 1 with replacement DLCI at 102. Since there are only three ports in the switching table, then these ports will be created on the switch. To create the first line such a switching table it is necessary to perform the actions shown in drawing 16.



Drawing 16 - Creation tables switching

1. IN section "Source" V field "Port" we enter 1, V field DLCIwe enter 102;

2. In the “Destination” section, in the “Port” field, enter 2, in the “DLCI” fieldwe enter 201;

3. Click here button "Add".

Likewise we add next lines tables switching.

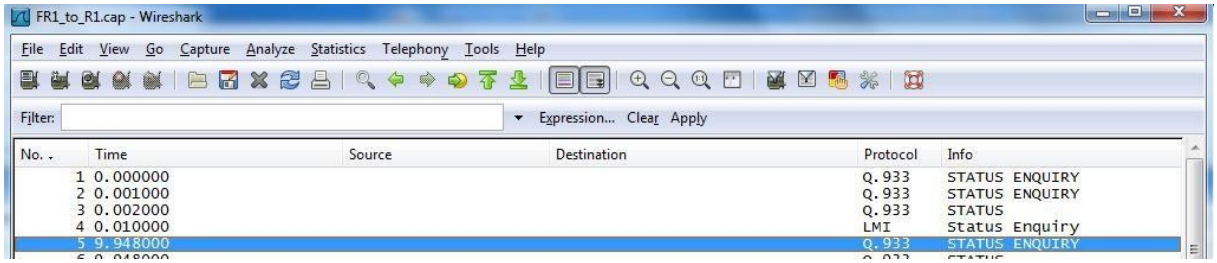
Для соединения коммутаторов с маршрутизаторами необходимо нажать button "Add Link"  on panels tools, For facilitiestake advantage point Manual.

Then left-click on the FR switch, selecting port 1, then left-click on the router and select one from sequential ports, V this laboratory work on everyonerouters will chosen port s1/0.

After connections everyone router With switches, connect Ethernet switches with routers, similarly, only in As a port for connection, use port f0/ 0 and then connect Linux_PC With switches Ethernet.

For Togo to see How ports devices connected between by yourself necessary press next button on panels tools  .

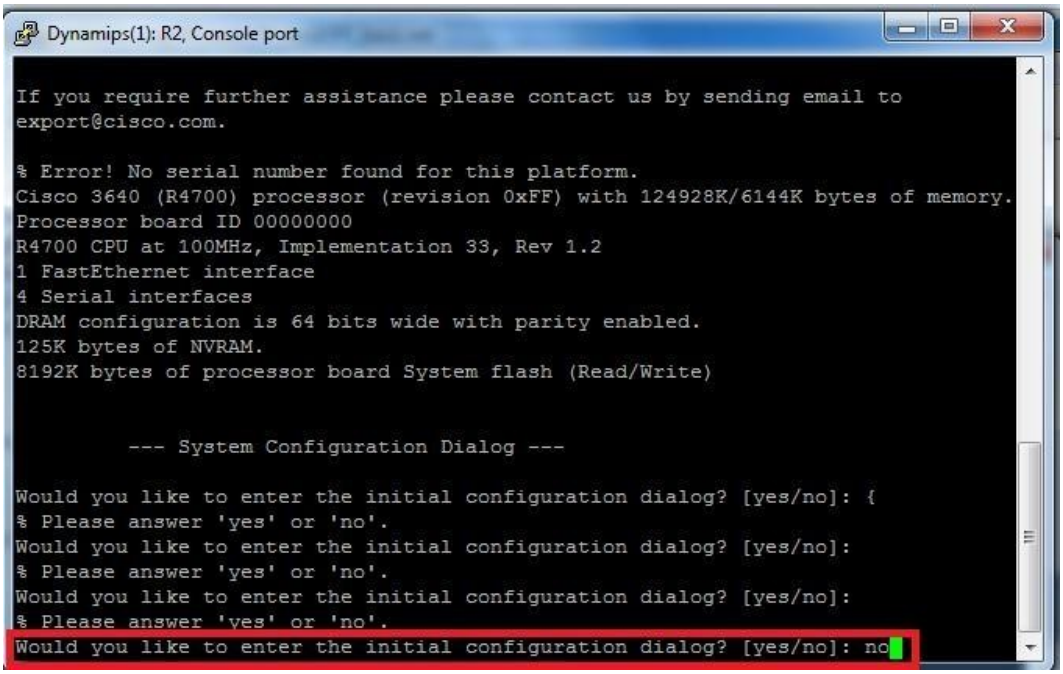
For execution laboratory work launch analyzer protocols,
In this work, WireShark will be used, right-click on connection between R1 and FR1, select the “Capture” option, after which it will start program WireShark, Figure 17.



Drawing 17 - window WireShark

Setting up interfaces Frame Relay

Start the router by selecting it with the left mouse button and pressing button start  , launch console window For input teams, by clicking button  . after downloads router V window dial team ***no*** And clickEnter, to refuse from primary settings router, drawing 17.



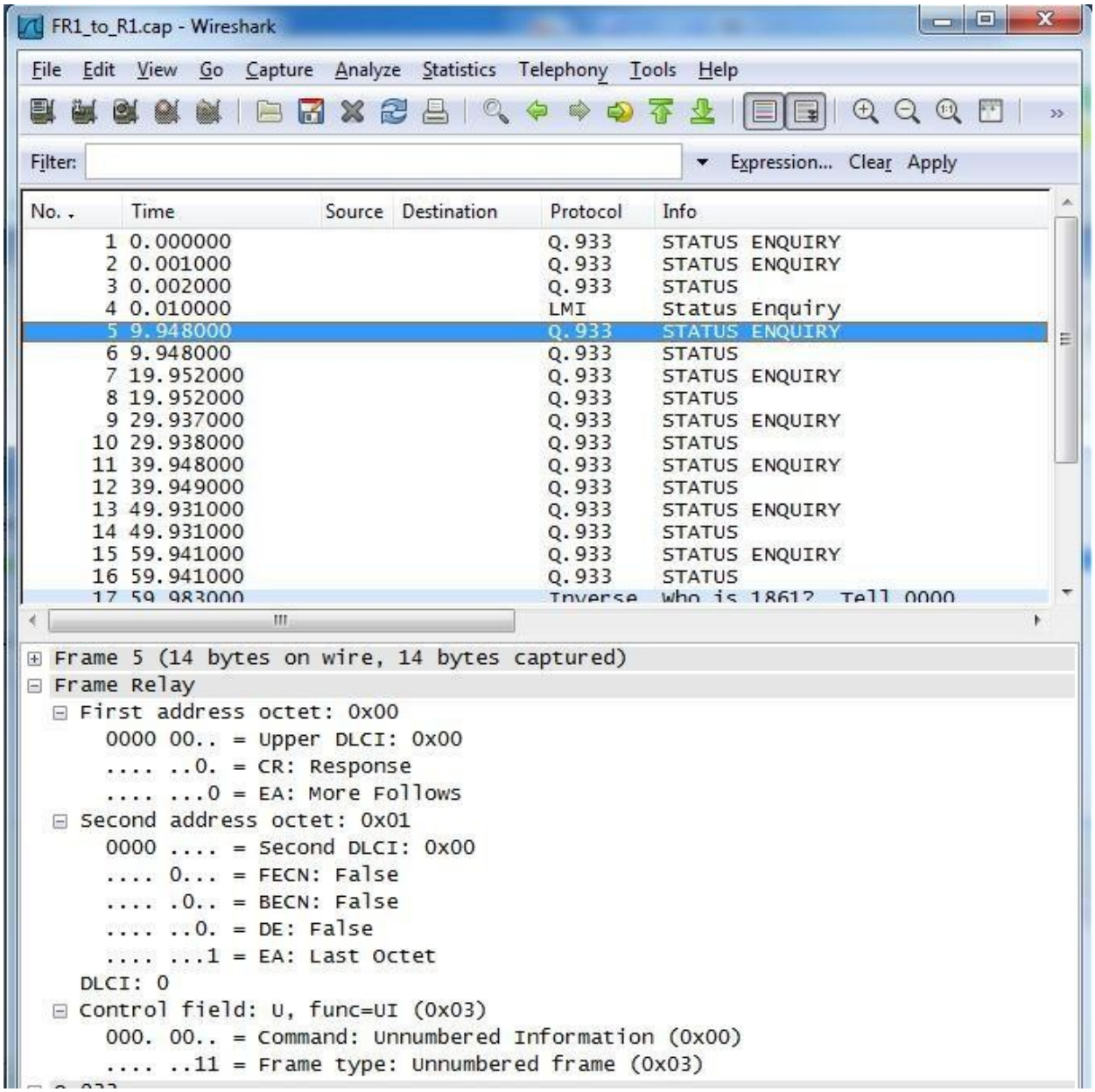
Drawing 17 - Interface team lines router

For settings interface s1/0 router R1 on work With protocol Frame Relay enter next commands:

R1>enable
R1#configure terminal
R1(config)#int s1/0
R1(config-if)#encapsulation frame-relay
ietfR1(config-if)#ip address 1.0.0.1
255.0.0.0 R1(config-if)#no shutd

How visible the only one team, which forces interface work V mode Frame Relay is encapsulation frame relay ietf, The ietf parameter specifies that after the Frame Relay frame header there should be go to the pointer to the higher-level protocol according to the recommendation committee IETF RFC 2427.

After entering the last command that enables the interface, no shutd In the WireShark program, click the refresh button , after which the program will lead out list messages, which exchanged between by yourself router And switch By interface LMI (Local Management Interface
- interface local management), How shown on drawing 18.



Drawing 18 - Capture message interface LMI

Please note the Status messages that repeat periodically. (state) And Status Inquiry (request states). At this router sends messages Status Inquiry, A switch answers on them Status message.

Format messages Status Inquiry (Request states):

```
Frame 35: 14 bytes on wire (112 bits), 14 bytes captured (112 bits)
Frame Relay
   First address octet: 0x00
   Second address octet: 0x01
   DLCI: 0
   Control field: U, func=UI (0x03)
```

```
Q.933
    Protocol discriminator: Q.933
    Call reference value length: 0
    Message type: STATUS ENQUIRY (0x75)
    Locking shift to codeset 5: Information elements for national use
    Report type (ANSI)
        Information element: Report type (ANSI)
        Length: 1
        Report type: Link verify (1)
    Keep Alive (ANSI)
        Information element: Keep Alive (ANSI)
        Length: 2
        TX Sequence: 21
        RX Sequence: 20
```

Format messages Status:

```
Frame 36: 14 bytes on wire (112 bits), 14 bytes captured (112 bits)
Frame Relay
    First address octet: 0x00
    Second address octet: 0x01
    DLCI: 0
    Control field: U, func=UI (0x03)
Q.933
    Protocol discriminator: Q.933
    Call reference value length: 0
    Message type: STATUS (0x7d)
    Locking shift to codeset 5: Information elements for national use
    Report type (ANSI)
        Information element: Report type (ANSI)
        Length: 1
        Report type: Link verify (1)
    Keep Alive (ANSI)
        Information element: Keep Alive (ANSI)
        Length: 2
        TX Sequence: 21
        RX Sequence: 21
```

These two types of messages are needed to verify the integrity of the physical channel connections between router And switchboard Frame Relay. For tracking integrity connections V these messages provided fields transmitted And accepted messages TX And RX respectively. The number of the transmitted Status Enquiry message must match number received Status message, in this case the router in the message Status Inquiry indicates on That, What He transmits TX=21 message Status Inquiry And to this accepted RX=20 message Status, on What switch answers transmitted message TX=21 And That, What message under Status Inquiry With number RX=21 was accepted.

After five transferred messages Status Inquiry, routertransmits message Status Inquiry With request full condition.

Message Status Inquiry With request complete states:

```
Frame 71: 14 bytes on wire (112 bits), 14 bytes captured (112 bits)
Frame Relay
   First address octet: 0x00
   Second address octet: 0x01
   DLCI: 0
   Control field: U, func=UI (0x03)
Q.933
   Protocol discriminator: Q.933
   Call reference value length: 0
   Message type: STATUS ENQUIRY (0x75)
   Locking shift to codeset 5: Information elements for national use
   Report type (ANSI)
      Information element: Report type (ANSI)
      Length: 1
      Report type: Full Status (0)
   Keep Alive (ANSI)
      Information element: Keep Alive (ANSI)
      Length: 2
      TX Sequence: 37
      RX Sequence: 36
```

In response to a full status request, the switch transmits a message Full Status (full state), V which indicates existing virtual channels.

Message Full Status:

```
Frame 72: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
Frame Relay
   First address octet: 0x00
   Second address octet: 0x01
   DLCI: 0
   Control field: U, func=UI (0x03)
Q.933
   Protocol discriminator: Q.933
   Call reference value length: 0
   Message type: STATUS (0x7d)
   Locking shift to codeset 5: Information elements for national use
   Report type (ANSI)
      Information element: Report type (ANSI)
      Length: 1
      Report type: Full Status (0)
   Keep Alive (ANSI)
      Information element: Keep Alive (ANSI)
      Length: 2
      TX Sequence: 37
      RX Sequence: 37
   PVC Status (ANSI)
      Information element: PVC Status (ANSI)
      Length: 3
      DLCI: 102
      Status: Active
   PVC Status (ANSI)
```

```
Information element: PVC Status (ANSI)
Length: 3
DLCI: 103
Status: Active
```

Configuration routers For work V fully connected networksFrame Relay.

Besides Togo What necessary ask type encapsulation on serial interfaces of routers must also be created routing tables for connecting all networks to each other, for these purposes we will use protocol dynamic routing RIP, like this way full configuration everyone routers indicated below:

```
R1>enable
R1#configure terminal
R1(config)#int s1/0
R1( config-if)#encapsulation frame-relay
ietfR1(config-if)#ip address 1.0.0.1
255.0.0.0 R1(config-if)#no shutd
R1( config-if)#int f0/0
R1( config-if)#ip address 2.0.0.1
255.0.0.0R1(config-if)#no shutd
R1( config-if)#exit
R1(config)#router rip
R1(config-router)#netw
R1( config-router)#network 1.0.0.0
R1( config-router)#network 2.0.0.0
```

Setting up router R2

```
R2>enable
R2#configure terminal
R2(config)#int s1/0
R2( config-if)#encapsulation frame-relay
ietfR2(config-if)#ip address 1.0.0.2
255.0.0.0 R2(config-if)#no shutd
R2( config-if)#int f0/0
R2( config-if)#ip address 3.0.0.1
255.0.0.0R2(config-if)#no shutd
R2( config-if)#exit
R2(config)#router
rip
R2( config-router)#network 1.0.0.0
R2( config-router)#network 3.0.0.0
```

Setting up router R3

R3>enable
R3#configure terminal
R3(config)#int s1/0
R3(config-if)#encapsulation frame-relay
ietfR3(config-if)#ip address 1.0.0.3
255.0.0.0 R3(config-if)#no shutd
R3(config-if)#int f0/0
R3(config-if)#ip address 4.0.0.1
255.0.0.0R3(config-if)#no shutd
R3(config-if)#router rip
R3(config-router)#network 1.0.0.0
R3(config-router)#network 4.0.0.0

After Togo How were configured All interfaces on routers and via the LMI interface in the message the full status was received identifiers DLCI active virtual channels, routers should were exchange messages InARP For Togo to create a table of correspondence between the IP addresses of routers and identifiers virtual channels. Using program WireShark, intercept InARP request messages and the response to it in an InARP message reply.

InARP request	InARP reply
Frame Relay First address octet: 0x18 Second address octet: 0x61 DLCI: 102 Control field: U, func=UI (0x03) Padding NLPID: SNAP (0x80) Organization Code: Encapsulated Ethernet (0x000000) Type: ARP (0x0806) Address Resolution Protocol (inverse request) Hardware type: Frame Relay DLCI (15) Protocol type: IP (0x0800) Hardware size: 2 Protocol size: 4 Opcode: inverse request (8) [Is gratuitous: [False] Sender hardware address: 0000 Sender IP address: 1.0.0.2 (1.0.0.2) Target hardware Address: 3091 Target IP address: 0.0.0.0 (0.0.0.0)	Frame Relay First address octet: 0x18 Second address octet: 0x61 DLCI: 102 Control field: U, func=UI (0x03) Padding NLPID: SNAP (0x80) Organization Code: Encapsulated Ethernet (0x000000) Type: ARP (0x0806) Address Resolution Protocol (inverse reply) Hardware type: Frame Relay DLCI (15) Protocol type: IP (0x0800) Hardware size: 2 Protocol size: 4 Opcode: inverse reply (9) [Is gratuitous: [False] Sender hardware address: 0000 Sender IP address: 1.0.0.1 (1.0.0.1) Target hardware Address: 3091 Target IP address: 1.0.0.2 (1.0.0.2)

According to this ARP request, router R2 found out What on opposite side channel 201 located router With IP address

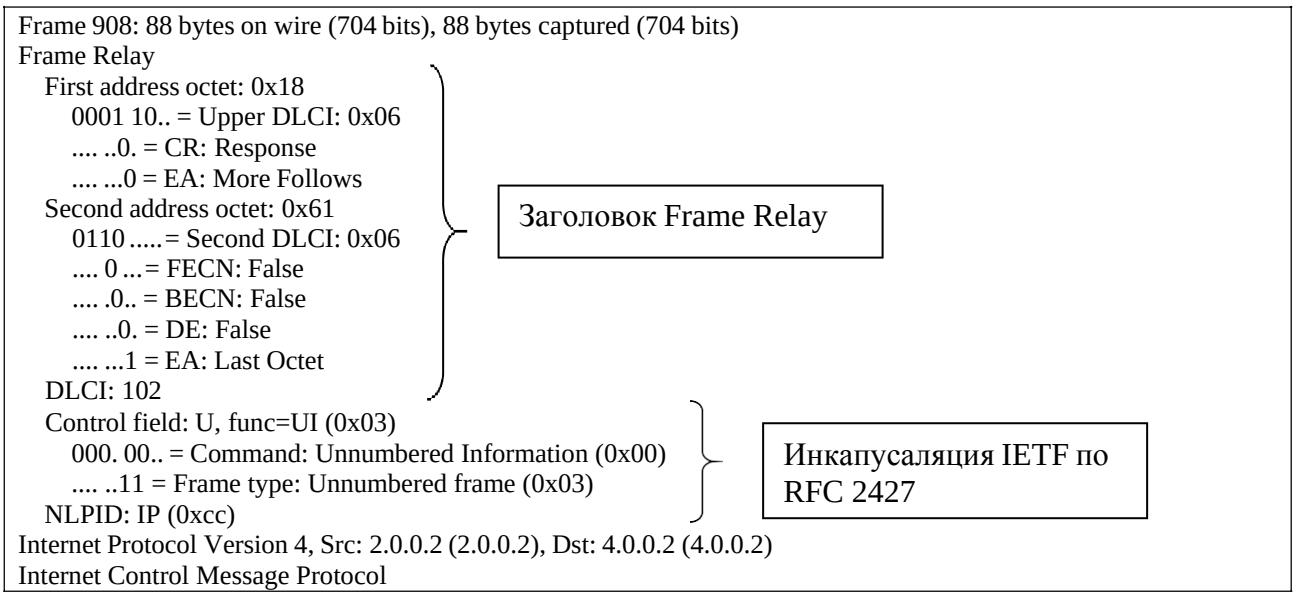
1.0.0.1. Channel ID 201 is encrypted in the Target hardware address field: 3091h InARP reply messages, the point is that in the Target hardware address field It is not a specific DLCI number that is specified, but the entire Frame Relay frame header. Like this in this way, to understand identifier DLCI necessary 3091h introduce in binary form 3091h= 0011 00 00 1001 0001, myself same DLCI is located in the first six bits of the first octet and in the first four bits second octet, therefore, the identifier DLCI=0011001001=201.

For Togo to to know what table permissions addresses compiled the router must be in privileged mode and the command must be entered show frame relay map.

```
R1#show frame relay map
Serial1/0 (up): IP 1.0.0.2 dlci 102(0x66,0x1860),
        dynamic,broadcast ,
        IETF, status defined, active
Serial1/0 (up): IP 1.0.0.3 dlci 103(0x67,0x1870),
        dynamic,broadcast ,
        IETF, status defined, active
```

How visible from conclusion this teams router R1 installed correspondence: IP 1.0.0.2 – DLCI 102; IP 1.0.0.3 – DLCI 103. Also pay attention to the keyword broadcast, this means that through these virtual channelsallowed broadcast multicast And broadcast messages, therefore, the transmission of RIPv1 protocol announcements is possible over these virtual channels.

To check if the configuration is correct, use the ping utility with Linux_PC1 For checks availability Linux_PC3 (4.0.0.2). WITH help programs WireShark intercept messages ICMP, below shown message ICMP echo request.



Analysis work protocol RIP

As is known to prevent route loops that can arise at the entrance work protocols dynamic routing, V routers provided mechanism divisions horizon, according to which the router should not announce through the interface those networks, which were received on this interface. Like this in this way, If method Split Range Enabled Router R1 must advertise through its serial interface only network 2.0.0.0 in the intercepted same message protocol RIP visible the opposite, That There is method divisionshorizon disabled.

Announcement protocol RIP:

```
Frame Relay
    First address octet: 0x18
    Second address octet: 0x61
    DLCI: 102
    Control field: U, func=UI (0x03)
    NLPID: IP (0xcc)
Internet Protocol Version 4, Src: 1.0.0.1 (1.0.0.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
    Command: Response (2)
    Version: RIPv1 (1)
    IP Address: 1.0.0.0, Metric: 1
    IP Address: 2.0.0.0, Metric: 1
    IP Address: 3.0.0.0, Metric: 1
    IP Address: 4.0.0.0, Metric: 1
```

Для того чтобы включить метод разделения горизонта необходимо в mode configurations each interface enter team IP split-horizon.

```
R1( config)#int s1/0
R1(config-if)#ip split-
horizon

R2( config)#int s1/0
R2(config-if)#ip split-
horizon

R3( config)#int s1/0
R3(config-if)#ip split-
horizon
```

IN result capture announcement RIP Togo same router R1 will at allanother:

```
Frame Relay
   First address octet: 0x18
   Second address octet: 0x61
   DLCI: 102
   Control field: U, func=UI (0x03)
   NLPID: IP (0xcc)
Internet Protocol Version 4, Src: 1.0.0.1 (1.0.0.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
   Command: Response (2)
   Version: RIPv1 (1)
   IP Address: 2.0.0.0, Metric: 1
```

Study work protocol RIP V topology dot - manypoints and one subnet.

IN under study topology on drawing 13 on channel level wasa fully meshed topology is configured, which means that each router has virtual channel To to everyone to another router, But such topology Not Always are justified, There are also often situations where only one router is connected to all the rest routers virtual channels (Hub and Spoke topology). Let Now Not exists virtual channel from router 2 to router 3, thus the switching table switch frame Relay will look like next way:

Таблица 3 - Таблица коммутации

	Port	DLCI	Port	DLCI
1	1	102	2	201
2	1	103	3	301

For deletions records, delete switch Frame Relay And create table switching according to the table 3.

Use the show frame-relay map command to verify that router R2 and R3 have only one active virtual channel, and the router R1 two virtual channel.

```
R1#show frame relay map
Serial1/0 (up): IP 1.0.0.2 dlci 102(0x66,0x1860), dynamic,
        broadcast,
        IETF, status defined, active
Serial1/0 (up): IP 1.0.0.3 dlci 103(0x67,0x1870), dynamic,
        broadcast,
        IETF, status defined, active

R2#show frame relay map
Serial1/0 (up): ip 1.0.0.1 dlci 201(0xC9,0x3090),
        dynamic ,broadcast,
        IETF, status defined, active

R3#show frame relay map
Serial1/0 (up): IP 1.0.0.1 dlci 301(0x12D,0x48D0),
        dynamic,broadcast,
        IETF, status defined, active
```

Because method divisions horizon included, That Now router R2 will not receive an advertisement about network 4.0.0.0, and router R3 will not will receive an announcement about the 3.0.0.0 network, since according to the split horizon rule router R1 Not will their announce through mine interface, A there is no virtual channel between R2 and R3. Using teams show IP route check tables routing on each from routers. For route entries to appear in the R3 and R2 tables, networks 3.0.0.0 And 4.0.0.0 respectively, necessary turn off method division of the range on router R1, then the announcements it receives about networks 3.0.0.0 And 4.0.0.0 on interface s1/0 will be announced through him

маршрутизаторам R3 и R2. Для отключения разделения диапазона введите в mode configurations interface team no IP split-horizon.

```
R1(config)#int s1/0
R1( config-if)#no IP split-horizon
```

Then check the router routing tables again. R2 And R3.

Change methods encapsulation And Creation subinterfaces

For the network to function properly, each virtual channel must be configured on mine method encapsulation, under encapsulation the mechanism of pointing to a higher level protocol is understood, which is in the LAPF frame, Cisco routers use by default branded method encapsulation, But Also exist Andstandardized methods encapsulation, For example, By RFC 2427. For There are several ways to specify a particular encapsulation method, depending on the interface operating mode. The interface can operate in two point-to-point modes And multipoint (dot - many points). The point-to-point mode assumes that only one device will be connected to the interface. one virtual channel, V mode multipoint With interface Maybe be more than one virtual channel is associated. By default, all interfaces are working in mode multipoint.

For tasks method encapsulation V mode point-to-multipoint exists two options:

1. Specify one view encapsulation, For everyone virtual channels, using the encapsulation frame-relay [cisco | ietf] command. This command is introduced V mode configurations interface.
2. Specify For each virtual channel mine method encapsulation, using team frame relay map IP [ip address] [DLCI] [cisco | [ietf], this

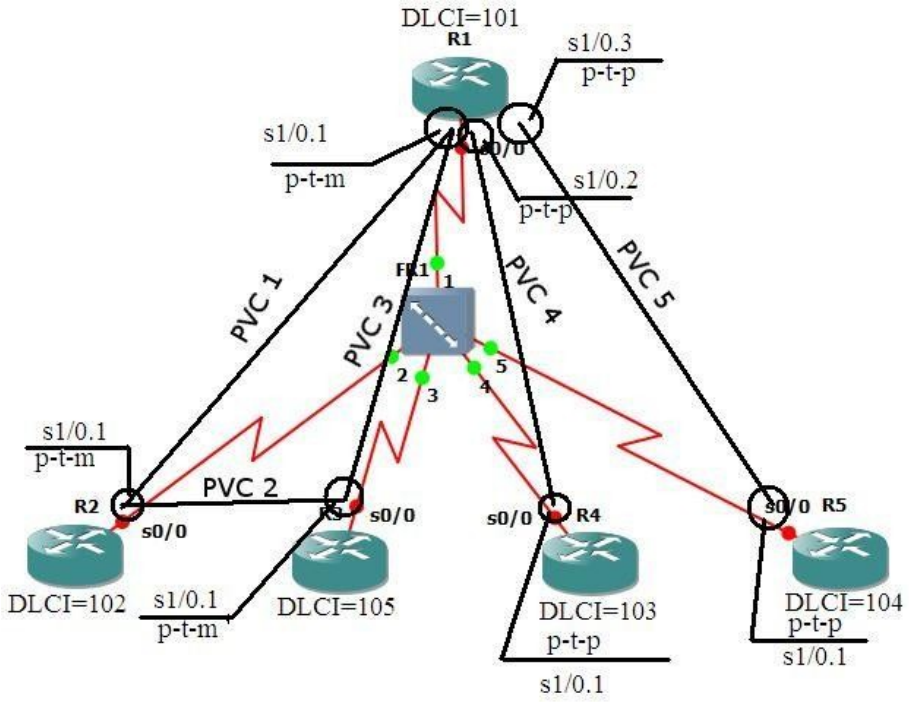
команда одновременно используется также для статического transformations identifier DLCI V IP address.

For tasks method encapsulation V mode point-to-point existsAlso two options:

1. Specify For each virtual channel mine method encapsulation?using team frame relay interface-dlci [DLCI] [cisco | [ietf]
2. Specify For each virtual channel mine method encapsulation, using team frame relay map IP [ip address] [DLCI] [cisco | [ietf].

Configuration routers For work V networks FrameRelay with non-fully connected topology And fully connected plots.

Collect next topology V GNS3, drawing 19.



Drawing 19 - Topology under study

Table 4 – IP addresses interfaces

R1	R2	R4	R7	R9
s0/1.1 - 1.0.0.1 s0/1.2 - 2.0.0.1 s0/1.3 - 3.0.0.1	s0/1 - 1.0.0.2	s0/1 - 1.0.0.3	s0/1.1 - 2.0.0.2	s0/1.1 – 3.0.0.2

Configuration router R1

```
R1#
R1(config)#int s0/0
R1( config-if)#encapsulation frame-relay
ietfR1(config-if)#no shutd
R1(config)#int s0/0.1 multipoint
R1( config-subif)#ip address 1.0.0.1 255.0.0.0
R1( config-subif)#frame-relay interface-dlci
102R1(config-fr-dlci)#exit
R1( config-subif)#frame-relay interface-dlci
103R1(config-fr-dlci)#exit
R1( config)#int s0/0.2 point-to-point
R1(config-subif)#ip address 2.0.0.1
255.0.0.0
R1( config-subif)#frame-relay interface-dlci 104
ietfR1(config-fr-dlci)#exit
R1( config-subif)#exit
R1( config)#int s0/0.3 point-to-point
R1(config-subif)#ip address 3.0.0.1
255.0.0.0
R1( config-subif)#frame-relay interface-dlci 105
ietfR1(config-fr-dlci)#exit
```

Configuration router R2

```
R2#config t R2(
config)#int s0/0
R2(config-
if)#encap
R2( config-if)#encapsulation fram
R2( config-if)#encapsulation frame-relay
ietfR2(config-if)#no shutd
R2( config-if)#int s0/0.1 multipoint
R2( config-subif)#ip address 1.0.0.2 255.0.0.0
R2( config-subif)#frame-relay interface-dlci
101R2(config-fr-dlci)#exit
R2( config-subif)#frame-relay interface-dlci
103R2(config-fr-dlci)#exit
R2( config-subif)#exit
R2(config)#
```

Configuration router R3

```
R3#
R3#config t
R3(config)#int
s0/0
R3( config-if)#encapsulation frame-relay
ietfR3(config-if)#no shutd
R3( config-if)#int s0/0
R3(config)#int s0/0.1 multipoint
```

```
R3( config-subif)#ip address 1.0.0.3 255.0.0.0
R3( config-subif)#frame-relay interface-dlci
101R3(config-fr-dlci)#exit
R3( config-subif)#frame-relay interface-dlci
102R3(config-fr-dlci)#exit
R3( config-subif)#exit
R3(config)#exit
R3#
```

Configuration router R4

```
R4#config t
R4(config)#int
s0/0
R4( config-if)#encapsulation frame
relayR4(config-if)#no shutd
R4( config)#int s0/0.1 point-to-point
R4(config-subif)#ip address 2.0.0.2
255.0.0.0
R4( config-subif)#frame-relay interface-dlci 101
ietfR4(config-fr-dlci)#exit
R4( config-subif)#exit
R4(config)#exit
R4#
```

Configuration router R5

```
R5#
R5#config t
R5(config)#int
s0/0
R5( config-if)#encapsulation frame
relayR5(config-if)#no shutd
R5(config)#int s0/0.1 point-to-point
R5( config-subif)#frame-relay interface-dlci 101
ietfR5(config-fr-dlci)#exit
R5( config-subif)#ip address 3.0.0.2
255.0.0.0R5(config-subif)#exit
R5(config)#exi
tR5#
```

After configuration everyone routers V R1 enter team showframe relay map.

```
R1#show frame relay map
Serial0/0.1 (up): IP 1.0.0.2 dlci 102(0x66,0x1860), dynamic,
        broadcast,
        IETF, status defined, active
Serial0/0.1 (up): IP 1.0.0.3 dlci 103(0x67,0x1870), dynamic,
        broadcast,
        IETF, status defined, active
Serial0/0.3 (up): point-to-point dlci, dlci 105(0x69,0x1890), broadcast, IETF
```

```
        status defined, active
Serial0/0.2 (up): point-to-point dlci, dlci 104(0x68,0x1880), broadcast, IETF
        status defined, active
```

As you can see, the router knows about all DLCI identifiers and their connections to each subinterface and IP address. Please also note the broadcast keyword for each virtual channel, this means that through each virtual channel it is allowed to transmit multicast and broadcast traffic.

It is also clear from the output of this command that using the protocol InARP received DLCI permissions to IP addresses for network 1.0.0.0/8, but There are cases when the InARP protocol can be disabled, in this case necessary create static records permissions addresses.

Configuration routers without support protocolinARP

Turn it off protocol InARP on router R1, R2, R3 usingteam no frame relay inverse-arp V configuration mode interface.

```
R1( config-if)#no frame-relay inverse-
arp R2(config-if)#no frame-relay
inverse-arp R3(config-if)#no frame relay
inverse-arp
```

And in order for dynamic records of address resolution to be faster disappeared from tables turn on And turn off interface.

After Togo How protocol InARP will disabled connection With routers, located V networks 1.0.0.0/8 will lost. For recovery connections Can configure static records address resolution using the following command in configuration mode corresponding subinterface/interface:

```
frame relay map IP [ip address ] [DLCI] ietf broadcast
```

ietf and broadcast parameters are options To basic frame- command relay map ip [ip address] [DLCI]. Using this command, we will create a static permission addresses on routers R1, R2, R3.

Configuration router R1

```
R1(config)#int s0/0.1 multipoint
R1( config-subif)#frame-relay map IP 1.0.0.2 102 ietf
broadcastR1(config-subif)#frame-relay map IP 1.0.0.3 103 ietf
broadcast
```

Configuration router R2

```
R2( config-if)#int s0/0.1 multipoint
R2( config-subif)#frame-relay map IP 1.0.0.1 101 ietf
broadcastR2(config-subif)#frame-relay map IP 1.0.0.3 103 ietf
broadcast
```

Configuration router R3

```
R3(config)#int s0/0.1 multipoint
R3( config-subif)#frame-relay map ip 1.0.0.1 101 ietf
broadcastR3(config-subif)#frame-relay map IP 1.0.0.2 102 ietf
broadcast
```

Now after input teams show frame relay map, records will be havestatus static.

```
R1#show frame relay map
Serial0/0.1 (up): ip 1.0.0.2 dlci 102(0x66.0x1860), static
        ,broadcast,
        IETF, status defined, active
Serial0/0.1 (up): ip 1.0.0.3 dlci 103(0x67.0x1870), static
        ,broadcast,
        IETF, status defined, active
Serial0/0.3 (up): point-to-point dlci, dlci 105(0x69,0x1890), broadcast, IETF
      status defined, active
Serial0/0.2 (up): point-to-point dlci, dlci 104(0x68,0x1880), broadcast, IETF
      status defined, active
```

Content report:

1. Both topology drawing 13 And drawing 19;
2. Listing settings routers For each topology, For topology on drawing 19 should be used static transformations addresses;

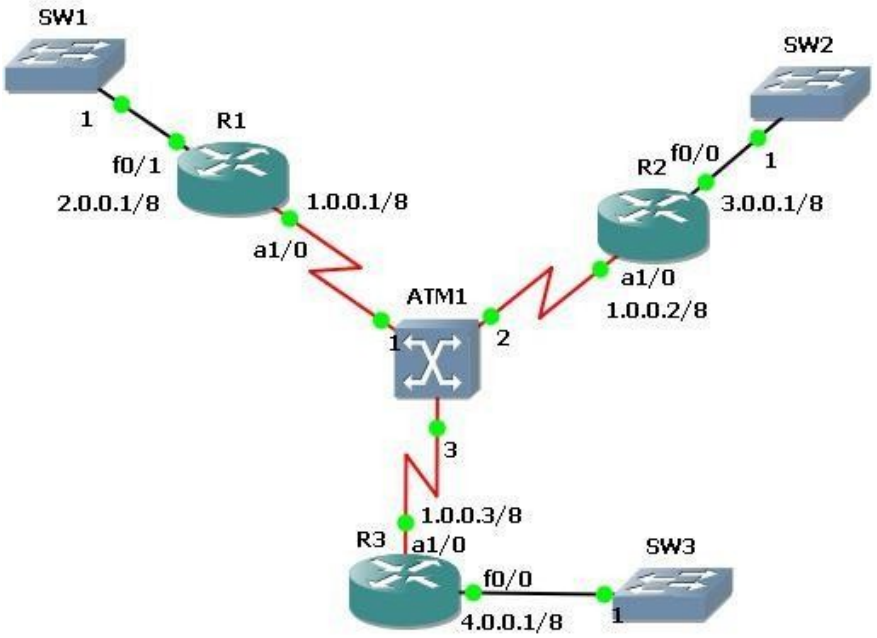
3. LMI Protocol Message Captures: Status Request, Status, Request full condition, full condition, - with a description of the purpose of each messages;
4. Capture frame Frame Relay With decryption fields title;
5. Capture messages inARP protocol;
6. Explanation of the procedure for transmitting a packet from host Linux_PC1 to Linux PC_2, drawing 13.

Control questions:

1. structure frame Frame Relay;
2. appointment interface LMI;
3. algorithm work protocol inARP;
4. Please explain V what kind cases necessary turn off, A V what kind include methoddivisions horizon online Frame Relay;
5. Please explain difference V algorithms work interfaces point-to-point Andmultipoint;
6. Structure tables switching switch Frame Relay;
7. State it content RFC 2427.
8. Please explain appointment key words broadcast V team frame relay mapIP [ip address] [DLCI] ietf broadcast.

Practical class No. 17 - Network Layer Protocols (Part 8).

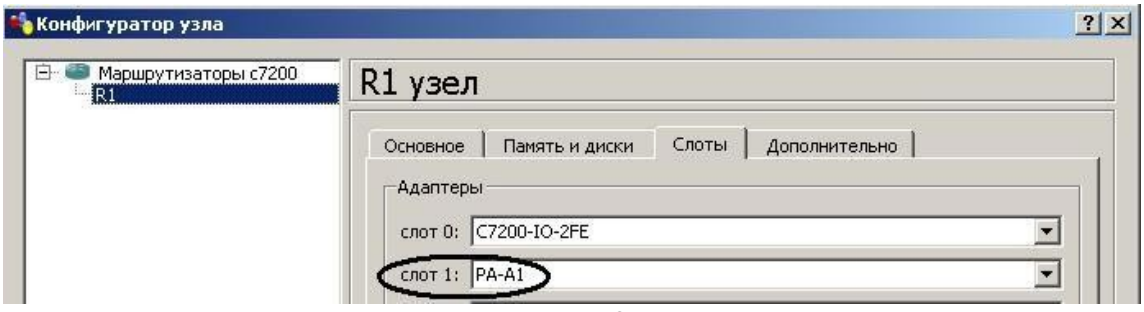
1. Make up topology, indicated on drawing 20.



Drawing 20 - Topology networks ATM

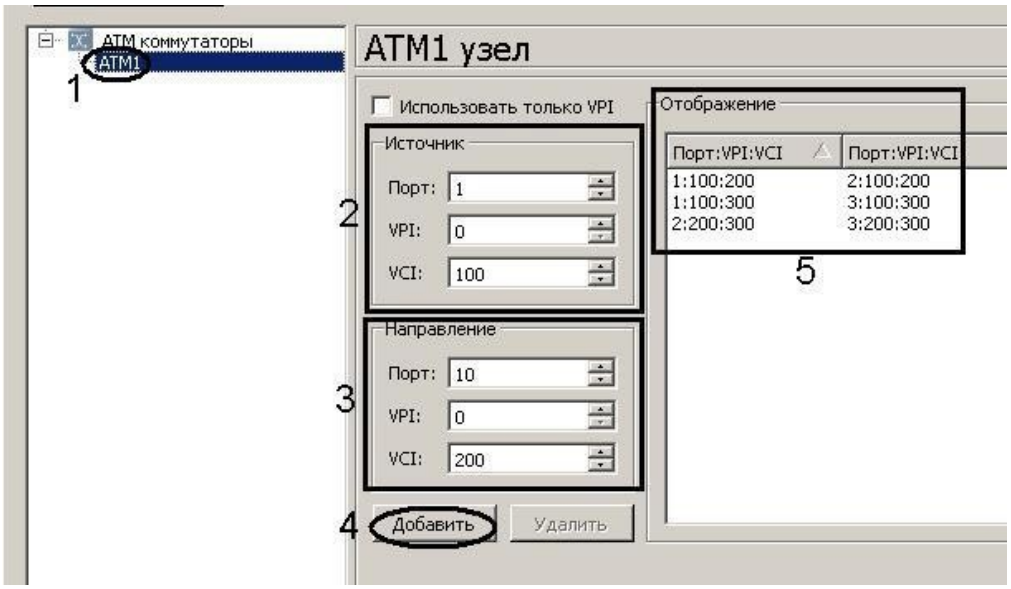
For routers, please use the c7200 model. To work with ATM network, use the PA-A1 slot as shown in Figure 21, for this click right button mice on router And select paragraph

"configure", then, in the "Node Configuration" window that opens, go to tab "Slots".



Drawing 21 - window Configurator node" router

2. For settings switch ATM open window Configurator node"



Drawing 22 - window Configurator node" switch ATM

First, select the ATM node as shown under number 1 in Figure 22,then make a switching table using the fields under numbers 2, 3, 4 on Figure 3, as a result you should get the same switching table How under digital 5. You you can use their values VPI/VCI. For example let's consider, How add first recording V table switching.

In field 2 “Source” select the port value equal to 1, VPI value 100, VCI – 200; In field 3 “Direction” select the port value equal to 2, meaning VPI 100, VCI - 200. After what click button "Add". Added recording means following: If on port 1 arrives ATM cell with fields VPI=100, VCI=200, then it must be redirected to the port 2, and the VCI/VPI field values remain the same. The same applies in reverse, If on port 2 arrives cell With fields VPI=100, VCI=200, That her necessary redirect on port 1, A meaning fields VCI/VPI leave the same. Likewise add the rest records V table switching.

Configuration routers

Main idea settings router consists of V settings two permanent virtual channels on interface ATM each router, those the most is being created fully connected topology on second level. To everyone interface router Also necessary appropriate

IP address, while in this configuration all router interfaces belong one IP subnets. Also every virtual channel between two routers must be configured to their own encapsulation type and adaptation level, in this case aal5SNAP. The default ATM network Not is broadcast, That's why V mode settings each virtual channel Can enter team **broadcast** , those the most Allows sending packets with broadcast and multicast IP address, This necessary do If on routers launched protocols routing.

Setting up router R1

```
R1>ena
config t
int a1/0
IP address 1.0.0.1 255.0.0.0
PVC 100/200
encapsulation aal5snap
broadcast
exit
PVC
100/300
broadcast
encapsulation aal5snap
exit
no shutd
R1(config-
if)#^Z
```

Setting up router R2

```
R2>ena
config t
int a1/0
IP address 1.0.0.2 255.0.0.0
PVC 100/100
broadcast
encapsulation aal5snap
exit
PVC
100/300
broadcast
encapsulation aal5snap
exit
no shutd
R2(config-
if)#^Z
```

Setting up router R3

```
R3>ena
config  t
int a1/0
IP address 1.0.0.3 255.0.0.0
PVC 100/100
broadcast
encapsulation aal5snap
exit
PVC 100/200
encapsulation aal5snap
broadcast
exit
no shutd
R3(config-
if)#^Z
```

For viewing information O work ATM take advantage commands:

```
Show  atm  PVC
Show atm map
Show running-
configShow
interface  a1/0Debug
atm arp
```

Content report:

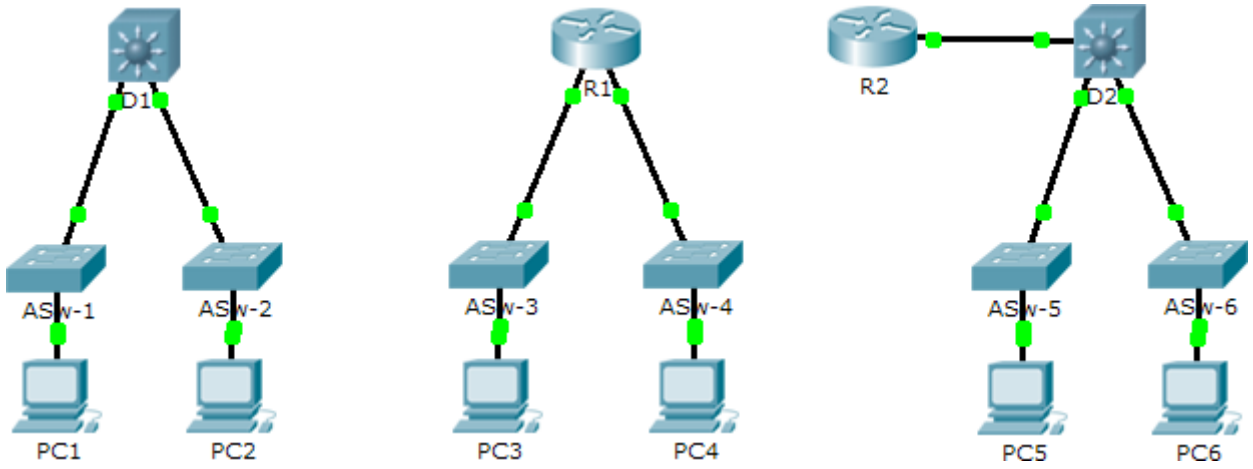
1. Topology, drawing 20;
2. Configuration each router And table switchingswitch;
3. Conclusions commands : Show atm PVC, Show atm map, Debug atm arp.

Control questions:

1. Structure cells ATM;
2. Purpose level adaptations AAL1;
3. Purpose level adaptations AAL2;
4. Purpose level adaptations AAL3/4;
5. Purpose level adaptations AAL5;
6. Purpose protocol InARPATM.

Practical class No. 18. Transport layer.

Topology



Task

Part 1. Comparison switches 2nd And 3rd levels
Part 2. Comparison switch 3rd level And router

General intelligence

IN framework this interactive tasks to you to come use various teams For checks three different switching topologies, and compare the similarities and differences between the switches 2960 And 3560. Besides this, to you to come compare table routing router 1941
With similar table switch 3560.

Part 1: Compare switches 2nd And 3rd levels

a. Study physical characteristics devices **D1** And **ASw-1** .
How many physical interfaces are installed in each individual switch? How many interfaces Fast

Ethernet And Gigabit Ethernet has every from switches?

_____

Please specify speed transmissions data on interfaces Fast Ethernet And Gigabit Ethernet of each switch.

_____

Is whether any from switches modular? _____

b. Interface switch 3560 is possible set up in interface quality 3rd level by entering **no switchport** commands in interface configuration mode. This allows specialistsassign an IP address and subnet mask to a switch interface in the same way as setting up data parameters on router.
IN how consists of difference between switchboard 2nd level And switchboard 3rd level?

_____

Author's right © companies Cisco And (or) her subsidiaries companies, 2021 G. All rights protected. IN this document contains publicly available information companies Cisco.

IN how consists of difference between physical interface switch And interface VLAN?

On what kind levels are in effect switches 2960 And 3560?

Do it team **show run,** to check settings switches **D1** And **ASw-1.** Noticed whether You between any of them differences?

Display table routing on both switches With help teams **show IP route.**
Explain, Why this team Not works on **ASW-1** , But works on **D1** ?

Part 2: Compare switch 3rd level With router

a. Until recently, switches and routers were devices with different set functions. Term "switch" was reserved for hardware device, which operates at layer 2. On the other hand, routers are devices that make forwarding decisions based on Layer 3 information. are used routing protocols for exchanging routing information and connections with others routers. Layer 3 switches, such as the 3560, can be configured to forward packets at Layer 3. Running the **ip routing command** in global configuration mode allows the use of routing protocols on Layer 3 switches, thus providing support for some router functions. Despite some functional similarity, switches differ By many to others aspects.
Open tab Physical on D1 And R1. Noticed whether You any differences or similarities V these tables? Do you notice? whether You any differences between these two devices?

Do it team **show run,** to check settings R1 And D1. Noticed whether You any differences or similarities V settings these switches?

WITH help Which teams Can appoint IP address on one from physical interfaces D1?

Do it team **show IP route** on both devices. Noticed whether You any differences or similarities V these tables?

Author's right © companies Cisco And (or) her subsidiaries companies, 2021 G. All rights protected. IN this document contains publicly available information companies Cisco.

Now analyze tables routing R2 And D2. Which information Not was displayed
V current configurations R1 And D1, however became obvious after analysis tables routing?

b. Check it out, is whether each topology fully related, having completed next tests:
   - Send echo request With **PC1** on **PC2**
   - Send echo request With **PC3** on **PC4**
   - Send echo request With **PC5** on **PC6**

IN each from three examples computers are located V different networks. Which device is used For provision connections between networks?

Why sending echo requests through networks was successful, despite on absence routers V networks?

Proposed way counting points

Chapter exercises	Question	Maximum quantity points	Earnednye points
Part 1. Comparison switches 2nd and 3rdlevels	a	IN this example — 20.	
	b	40	
Part 1. Total		**60**	
Part 2. Comparison Layer 3 switchAnd router	a	30	
	b	10	
Part 2. Total		**40**	
General number points		**100**	

Author's right © companies Cisco And (or) her subsidiaries companies, 2021 G. All rights protected. IN this document contains publicly available information companies Cisco.

Practical lesson #19. Upper layers of the OSI, TCP/IP models.

Topology

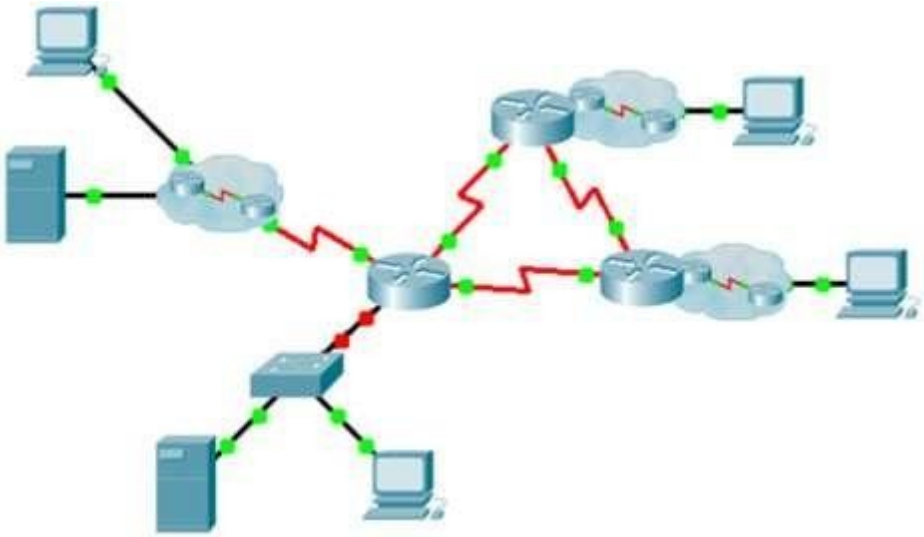


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
	G0/0.15			——
	G0/0.30			——
	G0/0.45			——
	G0/0.60			——
	S0/0/0		255.255.255.252	——
	S0/0/1		255.255.255.252	——
	S0/1/0		255.255.255.252	——
	G0/0			——
	S0/0/0		255.255.255.252	——
	S0/0/1		255.255.255.252	——
	G0/0			——
	S0/0/0		255.255.255.252	——
	S0/0/1		255.255.255.252	——
	VLAN 60			
	NIC	Appointed DHCP	Appointed DHCP	Appointed DHCP

Table networks VLAN And appointments ports

Number VLAN networks — Name	Purpose ports	Net
15 — Servers	F0/11 — F0/20	
30 — PCs	F0/1 — F0/10	
45 — Native	G0/1	
60 — Management	VLAN 60	

Scenario

While completing this interactive task you will need to use a lot of skills acquired during the CCNA course. First, you need to document themnetwork. You will need a printed copy of these instructions. During the implementation phase, you will set up The switch has VLANs, trunking, port security, and remote access. SSH protocol. Then you organize routing between VLANs and NAT translation on router. Finally, using the documentation, you will test this routing by way testing connections between final devices.

Documentation

You should fully document net. To you will be needed printout these instructions, including diagram topologies without signatures:

- Please note all device names, network addresses and other important information that is output.Packet Tracer.
- Fill in the Addressing Table and the VLANs and Port Assignments table. Table (Table networks VLAN And appointments ports).
- Please fill in all blanks in **the Implementation** and **Verification sections** . This information is providedat launch tasks Packet Tracer.

Implementation

Note . All devices V topology fully configured, for exception _____, _____and _____. You do not have access to other routers. You canget access ko to everyone servers And computers For execution checks.
Using documentation, implement given below requirements:

_____

- Set up access To remote management device, V volume number IP addressing And SSH:
  - Domain — cisco.com
  - Enable secret ciscoenpass
  - User _____with password _____
  - Length key encryption makes up 1024 bat
  - Protocol SSH versions 2 With limitation on two attempts checks authenticity And time expectations 60 seconds
  - Open passwords should be encrypted.
- Configure VLANs, name them, and assign them. Ports need to be configured.manually How ports access.

- Set up trunking.
- Set up safety ports.
  - For F0/1, allow 2 MAC addresses that will be automatically added to the configuration fileupon detection. In the event of a security breach, the port should not be shut down, but should be recorded message system log.
  - Turn it off All unused ports.

_____

- Set up routing between VLAN.
- Configure DHCP service for VLAN 30. Use the word **LAN** as the pool name (taking into accountregister)
- Implement routing:
  - Use RIPv2.
  - Set up one instructions network For total address spaces _____.
  - Turn it off interfaces, which Not should send messages RIPv2.
  - Set up route V Internet By default.
- Set up transformation NAT:
  - Configure a standard ACL with the number 1 containing one entry. All IP addresses are allowed,belonging address space _____.
  - WITH help documentation set up static NAT For file servers (File Server).
  - Set up dynamic broadcast NAT With using PAT, indicating selected Name pool, mask /30 And next two public addresses:

    _____

_____

Make sure, what _____did you receive ? all information about addressing from _____.

Examination

Now All devices should successfully send ping requests to others devices. IN otherwise case complete debugging. List of tests.

- Check remote access To _____, using SSH on PC.
- Make sure, What networks VLAN appointed correct ports, A protection ports works.
- Check it out table routing after filling.
- Check it out statistics And transformations NAT.
  - **External knot (Outside Host)** must have access To **file server (File Server)** By public address.
  - For internal computers must be allowed access To server **Web Server** (Web server).
- **troubleshooting documentation** table below , document All malfunctions, With which You collided, A Also methods their elimination.

Documentation search And elimination problems

Problem	Solution

Proposed way counting points

Score Packet Tracer: 75 points. For documentation is given 25 points.

Practical class №3. Setting up networks VLAN, VTP and DTP

Topology

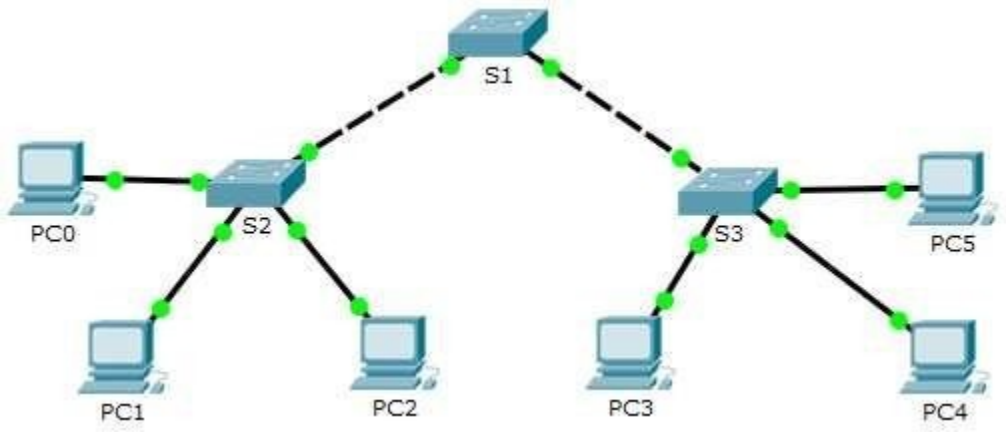


Table addressing

Device	Interface	IP address	Mask subnets
PC0	NIC	192.168.10.1	255.255.255.0
PC1	NIC	192.168.20.1	255.255.255.0
PC2	NIC	192.168.30.1	255.255.255.0
PC3	NIC	192.168.30.2	255.255.255.0
PC4	NIC	192.168.20.2	255.255.255.0
PC5	NIC	192.168.10.2	255.255.255.0
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0

Goals

Part 1. Setting up And examination dynamic protocol trunking (DTP)Part 2. Setting up and examination protocol VTP

General information/script

By measure increases quantities switches V networks becomes more complicated administration And control VLANs and trunks. To simplify some VLAN configurations, the VTP protocol allows the network administrator to automate the management of VLAN networks. Negotiation highways between network devices controlled dynamic protocol trunking (DTP) And automatically included on Catalyst switches 2960 And Catalyst 3560.

In this task, you will configure trunk links between switches. You will need to tune server And clients VTP V one domain VTP. Also You you will observe behavior VTP,

When switch located V transparent mode. You appoint ports For networks VLAN And check through connection to this same VLAN.

Part 1: Setting up And examination DTP

IN parts 1 You set up main channels between switches, A Also set up VLAN 999 How VLAN With untagged traffic.

Step 1: Check it out configuration networks VLAN.

Check it out configured networks VLAN on switches.

a. On S1 click tab **CLI** . By request enter **enable** , A then team **show vlan brief** , to check configured VLAN networks on S1.
S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
99	Management	active	
999	VLAN0999	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

b. Repeat step a) on switches S2 And S3. Which networks VLAN configured on these switches?

_____

Step 2: Set up highways on switches S1, S2 And S3.

Dynamic Trunking Protocol (DTP) manages trunk links between switches Cisco. IN real moment All switching ports are located V mode trunking By by default, i.e. "dynamic auto". At this step, you need to change the trunking mode to "dynamic desirable" for channel between switches S1 and S2. For the channel between switches S1 and S3, mode static highways. IN this topology use VLAN 999 V quality networks VLAN
With untagged traffic.

a. On switches S1 And S2 translate main channel V mode dynamic desirable on interface Gigabit Ethernet 0/1. Configuration switch S1 shown below.
S1(config)# **interface g0/1**
S1(config-if)# **switchport mode dynamic desirable**

b. For main channel between switches S1 And S3 install mode static main channel on interface GigabitEthernet 0/2.
S1(config)# interface g0/2 S1(config-if)# switchport
mode trunk

```
S3(config)# interface g0/2
```
S3(config-if)# switchport mode trunk

c. Make sure, What mode trunking included on everyone switches, having completed team **showinterfaces trunk** .

S1# **show interfaces trunk**

Port	Mode Encapsulation	Status	Native VLANGig0/1	
	desirablen-802.1qtrunking1			
Gig0/2	on802.1qtrunking1			
Port	Vlans allowed on trunk			
Gig0/1	1-1005			
Gig0/2	1-1005			
Port	Vlans allowed and active in management domainGig0/1			
	1,99,999			
Gig0/2	1,99,999			
Port	Vlans in spanning tree forwarding state and not prunedGig0/1		none	
Gig0/2	none			

Which net VLAN With untagged traffic Now is used For these highways? _____

d. Set up VLAN 999 How net VLAN With untagged traffic For main channels on S1.
S1(config)# **interface range g0/1 - 2**
S1(config-if-range)# **switchport trunk native vlan 999**
Which messages were received on S1? How would You corrected this one mistake?

_____

_____

e. On switches S2 And S3 set up VLAN 999 How net VLAN With untagged traffic.

f. Make sure that trunking mode is successfully configured on all switches. You should be able to send ping requests between switches in the topology using IP addresses configured oninterface SVI.

Part 2: Setting up And examination VTP

Switch S1 will be configured as a VTP server and switch S2 will be configured as a VTP client. All switcheswill be enter V domain VTP **CCNA** And use password **Cisco** For VTP.
Networks VLAN Can create on server VTP And distribute on other switches V domain VTP. IN this parts necessary will create 3 new networks VLAN on server VTP — S1. Networks VLAN will be distribute on S2 through VTP. Please pay attention attention on That, How works transparent mode VTP.

Step 1: Set up S1 How VTP server.

Set up S1 How VTP server in domain **CCNA** with a password **cisco** .

a. Set up S1 How server VTP.
S1(config)# **vtp mode server**

```
Setting device to VTP SERVER mode.
```

b. Install **CCNA** V quality domain name VTP.
   S1(config)# **vtp domain CCNA**
   Changing VTP domain name from NULL to CCNA
c. Install **Cisco** V quality password VTP.
   S1(config)# **vtp password Cisco**
   Setting device VLAN database password to Cisco

Step 2: Check it out VTP on S1.

a. Use team **show vtp status** on switches, to make sure, What mode And domain VTP configured Right.
   S1# **show vtp status**

VTP Version	: 2
Configuration Revision	: 0
Maximum VLANs supported locally : 255Number of	
existing VLANs	: 7
VTP Operating Mode	: Server
VTP Domain Name	: CCNA
VTP Pruning Mode	: Disabled
VTP V2 Mode	: Disabled
VTP Traps Generation	: Disabled
MD5 digest	: 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63 0x17

   Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
   Local updater ID is 192.168.99.1 on interface Vl99 (lowest numbered VLAN interfacefound)
b. To check password VTP, use team **show vtp password** .
   S1# **show vtp password**
   VTP Password: Cisco

Step 3: Add switches S2 And S3 V domain VTP.

In order for switches S2 and S3 to accept VTP advertisements from switch S1, they must belong To alone domain VTP. Set up switch S2 V quality client VTP With domain **CCNA** name on VTP and **Cisco** password For VTP. Remember, what domain VTP names are entered
With taking into account register.

a. Set up S2 How VTP client V domain **CCNA** with a password **cisco** .
   S2(config)# **vtp mode client** Setting device to
   VTP CLIENT mode.S2(config)# **vtp domain**
   CCNA
   Changing VTP domain name from NULL to CCNAS2(config)# **vtp**
   password Cisco
   Setting device VLAN database password to Cisco
b. To check password VTP, use team **show vtp password** .
   S2# **show vtp password**
   VTP Password: Cisco

c. Configure switch S3 as part of the **CCNA** VTP domain with password **cisco** on the VTP domain. Switch S3 will configured V mode transparent VTP.
S3(config)# **vtp mode Transparent**
S3(config)# **vtp domain CCNA**
Changing VTP domain name from NULL to CCNAS3(config)# **vtp**
password Cisco
Setting device VLAN database password to Cisco

d. To answer on next question, enter team **show vtp status** on everyone switches.
Please note that the configuration revision number is 0 on all three switches. Giveexplanation.

_____

_____

_____

Step 4: Create additional networks VLAN on S1.

a. On S1 create net VLAN 10 With name Red.
S1(config)# **vlan 10**
S1(config-vlan)# **name Red**

b. Create networks VLAN 20 And 30 according to next table.

Number VLAN	Name VLAN
10	Red
21	Blue
30	Yellow

c. Check it out successful addition new networks VLAN. Enter **show vlan brief** in privileged EXEC mode.Which networks

VLAN configured on S1?

_____

d. Check it out changes configurations, having completed team **show vtp status** on switches S1 And S2, to ensure that the VTP mode and domain are configured correctly. Output for S2 given below:
S2# **show vtp status**
VTP Version : 2
Configuration Revision : 6
Maximum VLANs supported locally : 255Number of
existing VLANs : 10
VTP Operating Mode : Client
VTP Domain Name : CCNA
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xE6 0x56 0x05 0xE0 0x7A 0x63 0xFB 0x33Configuration
last modified by 192.168.99.1 at 3-1-93 00:21:07

How many networks VLAN configured on S2? On S2 configured those same networks VLAN, What And on S1? Give it to me explanation.

Step 5: Please pay attention attention on That, How works transparent mode VTP.

S3 Now translated V transparent mode VTP.

a. To answer on next question, use team **show vtp status** .
How many networks VLAN Now configured on S3? Which number versions configurations? Please explain mine answer.

How would You changed quantity networks VLAN on S3?

b. Change mode VTP switch S3 on client.
Use teams show For checks changes regime VTP. How many networks VLAN Now present on S3?

Note: VTP advertisement flooding occurs across the management domain every fiveminutes or whenever VLAN network configurations are changed. To speed up this process, you can switch between real-time and simulation modes until the next cycle updates. You may need to do this several times, since each time the Packet clock Tracer will only be moved forward 10 seconds. Alternatively, you can move one of client switches V transparent mode, A then back V client.

Step 6: Purpose networks VLAN ports

Use team **switchport mode access** , to ask mode access For channels access. Use **the switchport access vlan** *vlan-id command* to assign a VLAN to port access.

Ports	Tasks	Net
S2 F0/1 – 8S3 F0/1 - 8	VLAN 10 (Red)	192.168.10.0 /24
S2 F0/9 - 16 S3 F0/9 - 16	VLAN 20 (Blue)	192.168.20.0 /24
S2 F0/17 - 24 S3 F0/17 - 24	VLAN 30 (Yellow)	192.168.30.0 /24

a. Assign networks VLAN ports on S2, using given table appointments.
S2(config-if)# **interface range f0/1 - 8** S2(config-if-range)# **switchport mode access** S2(config-if-range)# **switchport access vlan 10**

S2(config-if-range)# **interface range f0/9 -16** S2(config-if-range)# **switchport mode access** S2(config-if-range)# **switchport access vlan 20** S2(config-if-range)# **interface range f0/17 - 24**S2(config-if-range)# **switchport mode access** S2(config-if-range)# **switchport access vlan 30**

b. Assign networks VLAN ports on S3, using given table appointments.

Step 7: Check it out through connection.

a. Send ping request With PC0 on PC5.
b. Send ping request With PC1 on PC4.
c. Send ping request With PC2 on PC3.

Practical class No. 19. Search and eliminationVTP problems And DTP

Topology

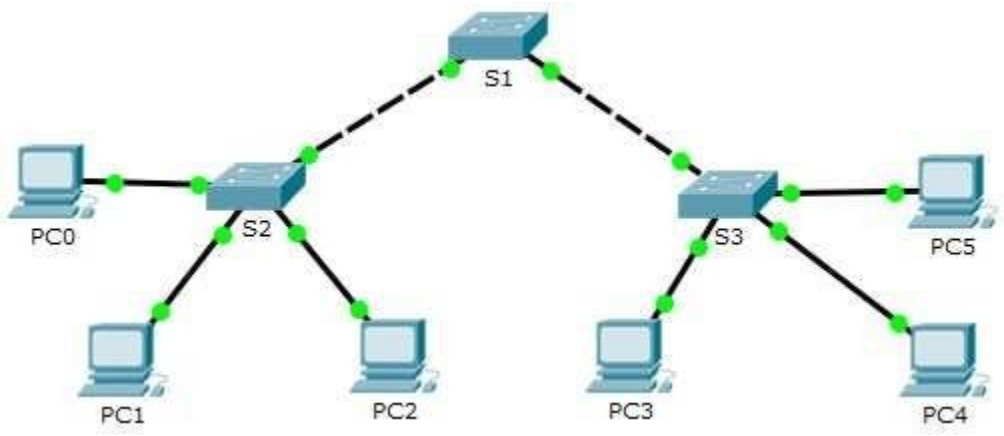


Table addressing

Device	IP address	Mask subnets
PC0	172.16.10.1	255.255.255.0
PC1	172.16.20.1	255.255.255.0
PC2	172.16.30.1	255.255.255.0
PC3	172.16.30.2	255.255.255.0
PC4	172.16.20.2	255.255.255.0
PC5	172.16.10.2	255.255.255.0
S1	172.16.99.1	255.255.255.0
S2	172.16.99.2	255.255.255.0
S3	172.16.99.3	255.255.255.0

Tasks

Part 1: Troubleshooting DTPPart 2. Search And

elimination problems VTP

General information/script

IN this task switches S2 And S3 Not apply information VTP. To you will need to check right settings configurations DTP And VTP. After elimination everyone problems computers

V one networks VLAN will be able to exchange data Friend With friend.

Part 1: Search And elimination problems DTP

In Part 1, you will troubleshoot trunk links between switches. will be required make sure, What between switches are used constant main channels.

a. Enter **the show interfaces trunk command** in privileged command mode.lines on all switches to determine the status of trunk channels. How many main channels configured on given moment?

_____

b. Enter **the show interfaces g0/1 switchport command** in privileged executive mode.command lines on switchboard S1. Repeat For interface g0/2 on switchboard S1.
IN what mode are working interfaces Gigabit Ethernet on switchboard S1?

c. Repeat these teams For interface g0/1 on switchboard S2 And g0/2 on S3.
Correct it settings main channels. Write it down teams, used For elimination problems trunking.

_____

_____

_____

_____

d. Check it out main channels With help teams **show** .

Part 2: Search And elimination problems V work VTP

Switch S1 will be configured as a VTP server. Switches S2 and S3 will be configured as VTP clients.and will receive VTP updates from switch S1. The VTP domain should be **CCNA** , and the password VTP — **cisco** . At this moment moment All required VLAN networks already tuned to switchboard S1.

Step 1: Check it out information O networks VLAN

Use team **show vlan brief** on everyone switches. U everyone whether switches the same quantity networks VLAN? How many networks VLAN at each switch?

_____

Step 2: Check it out configurations VTP.

Use teams **show vtp status** And **show vtp password** on everyone switches For checks states VTP.
Write it down information O condition VTP V table below.

Device	Domain Name (Name domain)	Operating Mode (Mode work)	Password VTP
S1			
S2			
S3			

Step 3: Correct it configurations VTP.

Write it down teams, used For corrections configurations VTP.

_____

Step 4: Check it out appointment ports.

Ports switching, pluggable To computers, follows tune V faithful networks VLAN, to computers could exchange data friend With friend.

Use team **show vlan brief** on switches S2 And S3, to define, appointed whether networks VLAN ports switching. Which net VLAN connected With these ports switching?

ports	Tasks	Net
S2 F0/1 S3 F0/8	VLAN 10 (Staff)	172.16.10.0/24
S2 F0/9 S3 F0/16	Net VLAN 20 (students)	172.16.20.0 /24
S2 F0/17 S3 F0/24	Net VLAN 30 (teachers)	172.16.30.0 /24

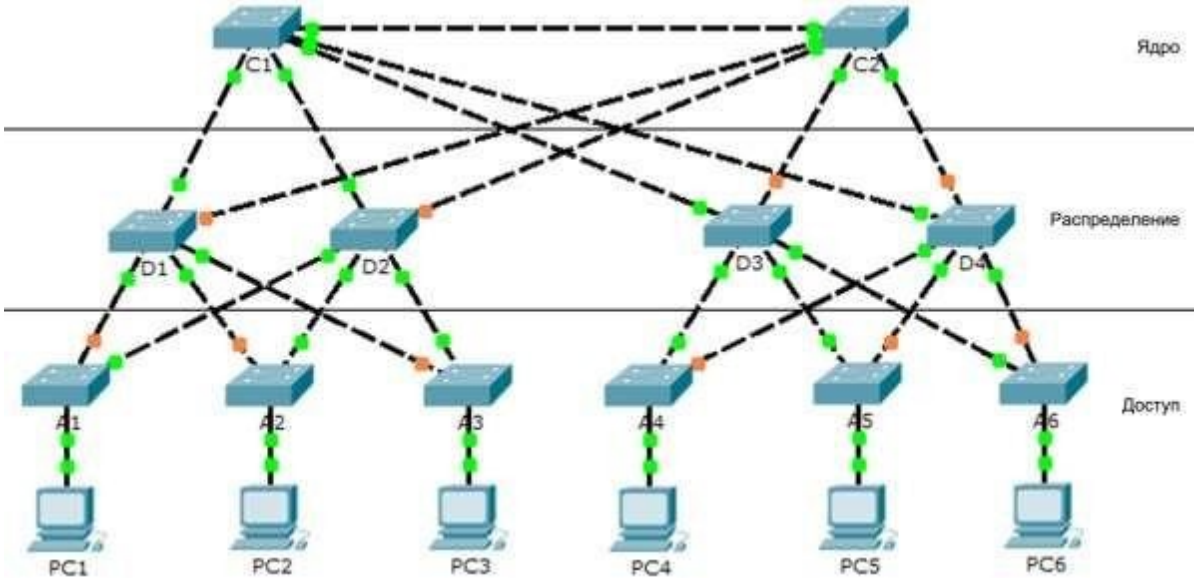
WITH help tables higher fix it appointments networks VLAN on switches S2 And S3. Write it down configurations appointments following VLAN networks.

Step 5: Check it out through connection.

a. Send ping request With PC0 on PC5.
b. Send ping request With PC1 on PC4.
c. Send ping request With PC2 on PC3.

Laboratory Job No. 19. Study designwith reservation

Topology



Tasks

Part 1. Examination convergence STP

Part 2. Examination process ARP

Part 3. Examination redundancy V dial-up networks

General intelligence

In this interactive activity, you will observe the default STP protocol in operation and its behavior V case failure. Switches added To networks automatically. Switches Cisco can connect to the network without any additional actions from the network administrator. To do this exercises priority bridge was changed.

Part 1: Check convergence STP

By completion convergence STP, are being created next conditions:

- On everyone switched ports PC indicators activities channel are burning green light.
- Access layer switches have one uplink transmit channel (green light indicator) To switchboard level distribution And one blocking ascending channel (yellow light indicator) ko to the second switchboard level distribution.
- Switches level distribution have one transmitting ascending channel (green light indicator) to the core switch and one blocking uplink (yellow light) indicator) ko to the second level switch nuclei.

Part 2: Check process ARP

Step 1: Go to simulation mode. Step 2: Send

echo request from PC1 on PC6.

a. Use tool **Add Simple PDU** (Add simple PDU) For creation PDU from **PC1** to **PC6** . Make sure ARP and ICMP are selected in **Event** List Filters. Click **Capture/Forward** (Capture/Forward), to check process ARP V moment receipt dial-up network MAC addresses **PC1** And **PC6** . Please pay attention attention, What All possible loops
stopped by means of blocking ports. TO for example, ARP request from **PC1** transmitted from **A1**
To **D2,** To **C1,** To **D1** And then back To **A1** . However in view of Togo, What STP blocks channel between **A1** And **D1** , loop Not is formed.

b. Please pay attention attention, What ARP response from **PC6** transmitted By to that same paths. Why?

_____

c. Write it down loopless path between **PC1** And **PC6** . _____

Step 3: Again check process ARP.

a. Under drop-down list **Scenario 0** (Scenario 0) click **New** (Create), to create **Scenario 1** : Test the ARP process again by pinging the two different PC.

b. Which Part paths has changed With moment dispatches latest echo requests? _____

Part 3: Check redundancy V dial-up networks

Step 1: Delete the channel between A1 And D2.

Go to V mode **real time** . Delete channel between **A1** And **D2** . For achievements convergence STP and creating a new, loop-free path may take some time. Since the changesIf only **A1 is affected** , you will see the yellow indicator light on **A1** and **D1** change to green. For acceleration process convergence STP click **Fast Forward Time** (Speed up).

Step 2: Send echo request With PC1 on PC6.

a. After inclusions channel between **A1** And **D1** (is determined green light indicator) go to **Simulation** mode and create **Scenario 2.** Resend the echorequest With **PC1** to **PC6** .

b. Write it down new loopless path. _____

Step 3: Delete the channel between C1 And D3.

a. **real-time** mode . Note that the channel indicators between ports **D3** And **D4** And port **C2** are burning yellow color. Delete channel between **C1** And **D3** . For It may take some time for STP to converge and create a new, loop-free path. Pay attention to the behavior of the **D3** and **D4 indicators** . To speed up the STP convergence processclick **Fast Forward Time** (Speed up).

b. Which channel Now is active channel To **C2** ? _____

Step 4: Send echo request With PC1 on PC6.

a. Go to V mode **Simulation** And create **Scenario 3 (Scenario 3)** . Send echo request With **PC1** on **PC6** .

b. Write it down new loopless path. _____

Step 5: Remove D4.

real-time mode . Note that **A4** , **A5** , and **A6** forward traffic to**D4** . Remove **D4** . To achieve STP convergence and create a new, loop-free path, It may take some time. Watch how the channel indicators from **A4** , **A5** , **A6** to **D3** change the light to green (enter the transmitting state). Now all three switches should forward traffic on **D3** .

Step 6: Send echo request With PC1 on PC6.

a. Switch to **Simulation mode** and create Scenario **4** .Send echo request With **PC1** on **PC6** .

b. Write it down new loopless path. _____

c. How is different this new path?

_____

Step 7: Remove C1.

Go to **real-time mode** . Note that **D1** and **D2** forward traffic to **C1** .Remove **C1** . It may take some time to achieve STP convergence and create a new, loop-free path. for some time. Watch as the channel indicators from **D1** and **D2** to **C2** go into a state transmission (the light will change to green). Upon completion of convergence, both switches should successfully forward traffic on **C2** .

Step 8: Send echo request With PC1 on PC6.

a. Switch to **Simulation mode** and create Scenario **5** .Send echo request With **PC1** on **PC6** .

b. Write it down new loopless path. _____

Proposed way counting points

Chapter exercises	Question	Maximum quantity points	Earnedpoints
Part 2. Verification process ARP	Step 2b	5	
	Step 2c	15	
	Step 3	5	
Part 2. Total		**25**	
Part 3. Verification redundancy in dial-upnetworks	Step 2	15	
	Step 3	5	
	Step 4	15	
	Step 6b	15	
	Step 6c	10	
	Step 8	15	
Part 3. sciences		**75**	
General number points		**100**	

Practical class No. 20. Setting up PVST+

Topology

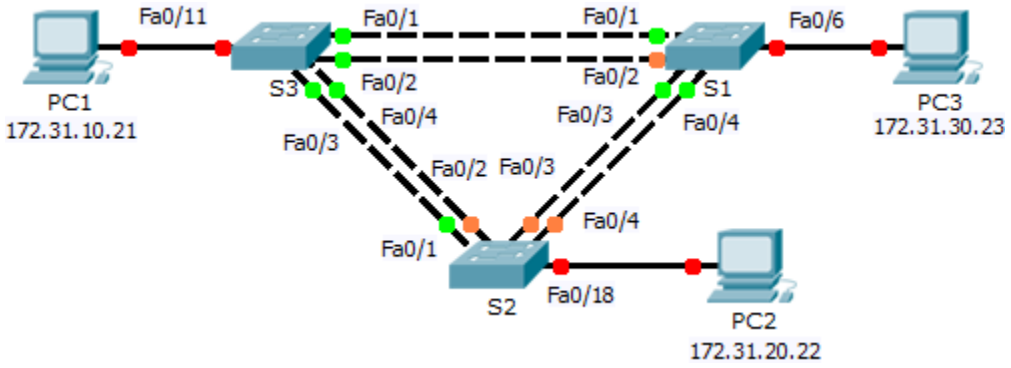


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
S1	VLAN 99	172.31.99.1	255.255.255.0	——
S2	VLAN 99	172.31.99.2	255.255.255.0	——
S3	VLAN 99	172.31.99.3	255.255.255.0	——
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.254
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.254
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.254

Parameters appointments ports switch

ports	Tasks	Net
S1 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S3 F0/11	VLAN 10	172.17.10.0/24

Tasks

Part 1. Setting up networks VLAN

Part 2. Configuring the PVST+ spanning-tree protocol and load balancingPart 3. Setting up PortFast And BPDU Guard

General intelligence

In this task, you will configure VLANs and trunks, configure and learn basic And auxiliary root bridges With help protocol STP. Also You optimize dial-up topology, using PVST+, PortFast and BPDU Guard.

Part 1: Setting up networks VLAN

Step 1: Turn on custom ports on switches S1, S2 And S3 V modeaccess.

Please contact us To given diagram topology, to define which from ports switches (**S1, S2** and **S3**) are enabled for connecting end-user devices. Three ports will be translated V mode access And included With help teams **no shutdown.**

Step 2: Create networks VLAN.

Using the appropriate commands, create VLANs 10, 20, 30, 40, 50, 60, 70, 80, and 99 on all switches.

Step 3: Assign networks VLAN ports switches.

Appointments ports given V table V beginning this tasks. Save settings after appointments ports switches networks VLAN.

Step 4: Check networks VLAN.

Do it team **show vlan brief** on everyone switches, to make sure, What All networks VLAN are displayed V tables VLAN.

Step 5: Assign trunk channels networks native VLAN 99.

Use the appropriate command to configure ports F0/1 - F0/4 on each switch. V quality trunk ports And assign these trunk native ports VLAN 99.

Step 6: Assign addresses administrative interfaces on everyone switches.

Make sure, What switches Right configured, having completed echo requests between each from them.

Part 2: Setting up protocol spanning tree PVST+ And distributionloads

Because For each active networks VLAN exists separate option protocol spanning tree, That For each tree, a root bridge is selected. In the event that when selecting a root bridge the default switch priorities are used for each option protocol spanning tree is selected one And That same root bridge, How was shown higher. This Maybe lead to poor design. Below are some reasons why necessary control choice root switch.

- The root switch is responsible for generating BPDUs for 802.1D STP and is the key means protocol STP For control traffic. Root switch must cope With this additional load.
- The location of the root switch determines the active paths in the network. Random placementswitch often leads to the emergence of suboptimal paths. It is best to place root switch on level distribution.

- Examine the topology given in this task. Traffic is carried on only three of the six configured trunk channels. Although this prevents loops, This configuration also causes unnecessary waste of resources. Due to the fact that the rootswitch Can define, based on from specific VLAN, one And That same port Maybe play role blocking for one VLAN and transmitting for another VLAN. This feature demonstrated below.

Step 1: Set up mode STP.

Do it team **spanning tree mode,** to tune switches For use PVST V quality regime STP.

Step 2: Set up distribution loads By protocol spanning tree PVST+.

a. Configure **S1** as the primary root switch for VLANs 1, 10, 30, 50, and 70. Set up **S3** V quality main root switch networks VLAN 20, 40, 60, 80 And 99. Set up **S2** V quality auxiliary root switch For everyone VLAN.

b. Check it out configurations With help teams **show spanning-tree.**

Part 3: Setting up PortFast And BPDU Guard

Step 1: Set up PortFast on switches.

feature puts a port into forwarding mode, virtually skipping states listening and learning. PortFast allows you to minimizethe amount of time it takes for a server or workstation to come online.Set up function PortFast on interfaces switch, connected To PC.

Step 2: Configure BPDUs guard on switches.

Using the STP PortFast BPDU guard feature allows network designers to enhance security borders domain STP And save predictability used topology. Devices for beyond ports with STP PortFast enabled do not affect the STP topology. After receiving BPDUs The BPDU guard function disables a port on which PortFast has been configured. The BPDU guard function guard puts the port into the err-disable state, and the console displays the corresponding message. Configure the BPDU guard function on the switch interfaces, connected To PC.

Step 3: Check settings.

To check configuration, use team **show running-configuration.**

Practical class No. 21. Setting up Rapid PVST+

Topology

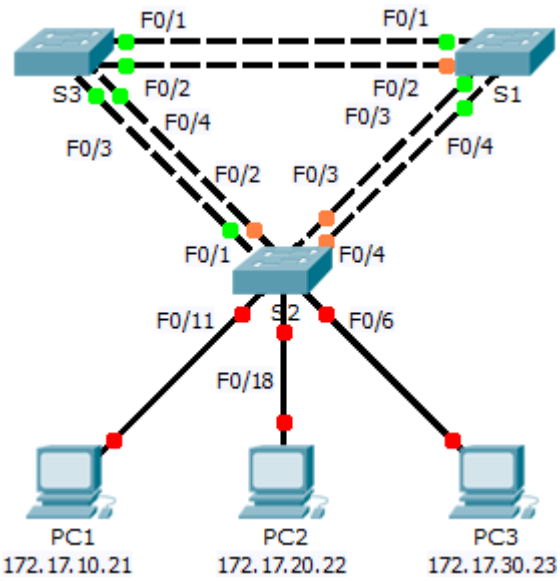


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
S1	VLAN 99	172.17.99.11	255.255.255.0	——
S2	VLAN 99	172.17.99.12	255.255.255.0	——
S3	VLAN 99	172.17.99.13	255.255.255.0	——
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.254
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.254

Parameters appointments ports switch

ports	Tasks	Net
S2 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S2 F0/11	VLAN 10	172.17.10.0/24

Tasks

Part 1. Setting up networks VLAN

Part 2. Configuring load balancing using the Rapid Spanning Tree Protocol (PVST+)Part 3. Setting up PortFast And BPDU Guard

General intelligence

In this exercise you will configure VLANs and trunks, Rapid PVST+, basic And auxiliary root bridges, A Also check results settings. You Also optimize net by way settings PortFast And functions BPDU guard on border ports.

Part 1: Setting up networks VLAN

Step 1: Turn on custom ports on S2 V mode access.

Refer to the topology diagram below to determine which ports on switch **S2** included For connections devices final users. Three port will be translated V mode access And included With help teams **no shutdown.**

Step 2: Create networks VLAN.

Using the appropriate commands, create VLANs 10, 20, 30, 40, 50, 60, 70, 80, and 99 on all switches.

Step 3: Assign networks VLAN ports switches.

Appointments ports given V table V beginning this tasks. Save settings after appointments ports switches networks VLAN.

Step 4: Check networks VLAN.

Do it team **show vlan brief** on everyone switches, to make sure, What All networks VLAN are displayed V tables VLAN.

Step 5: Assign trunk channels networks native VLAN 99.

Use the appropriate command to configure ports F0/1 - F0/4 on each switch. V as trunking And assign these trunks ports native VLAN networks 99.

Step 6: Assign addresses administrative interfaces on everyone switches.

Make sure, What switches Right configured, having completed echo requests between each from them.

Part 2: Setting up distribution loads By fast protocolspanning tree (Rapid) PVST+

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) can be considered rather as an improved version of the 802.1D standard rather than a radically new solution. Overall The 802.1D terminology does not change. Most of the parameters remain the same, so Users familiar with 802.1D will be able to configure the new protocol without any problems. In most In some cases, the RSTP protocol demonstrates better performance than proprietary solutions.Cisco without additional configuration. The 802.1w standard can also function as standard 802.1D, For work With obsolete bridges on separate ports.

Step 1: Set up mode STP.

Use team **spanning tree mode** For choice fast PVST V quality regime STP.

Step 2: Configure load balancing using the Rapid spanning-tree protocol (Rapid)PVST+.

Set up **S1** V quality main root switch networks VLAN 1, 10, 30, 50 And 70. Set up
S3 V quality main root switch networks VLAN 20, 40, 60, 80 And 99. Set up **S2**V quality auxiliary root switch
For everyone networks VLAN.
Check it out completed settings, using team **show spanning-tree.**

Part 3: Setting up PortFast And BPDU Guard

Step 1: Set up PortFast on S2.

feature puts a port into forwarding mode, virtually skipping states listening and learning. PortFast allows you to minimizethe amount of time it takes for a server or workstation to come online.Set up PortFast on interfaces switch **S2,** connected To PC.

Step 2: Set up BPDU guard on S2.

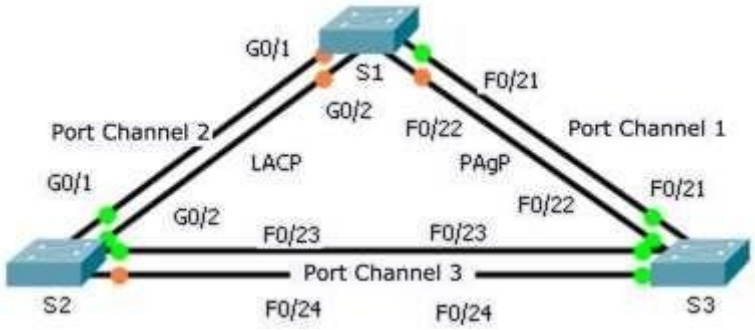
Using the STP PortFast BPDU guard feature allows network designers to enhance security STP domain boundaries and maintain predictability of the topology used. Devices outside ports with STP PortFast enabled do not affect the STP topology. After receiving BPDUs The BPDU guard function disables a port on which PortFast has been configured. The BPDU guard function Guard puts the port into the err-disable state and the following message appears on the console: corresponding message. Configure BPDU guard on the interfaces of switch **S2** connectedTo PC.

Step 3: Check settings.

For checks configurations use team **show run** .

Practical class No. 22. Setting up EtherChannel

Topology



Tasks

Part 1. Setting up basic parameters switch
Part 2. Setting up EtherChannel With protocol aggregation ports Cisco (PAgP)
Part 3. Setting up channel EtherChannel With protocol management aggregation channels(LACP) 802.3ad
Part 4. Setting up excess channel EtherChannel

General intelligence

Three switches have just been installed. Redundancy is configured between the switches. channels. Usually, only one of these channels can be used, otherwise a loop may occursecond level models OSI. However at operation one channel is used only half available bandwidth. EtherChannel allows you to combine up to eight redundant channels into one logical channel. In this lab, you will configure the protocol Port Aggregation Protocol (PAgP), Cisco EtherChannel Protocol, and Aggregation Control Protocol channels (LACP), version EtherChannel open standard IEEE 802.3ad.

Part 1: Setting up main parameters switch

Step 1: Set up main parameters switch.

a. Assign to everyone switchboard Name node V in accordance With diagram topology.
b. Depending on the connections between devices, configure all required ports astrunk.
Note : If the ports are configured in dynamic automatic mode and you have not configured mode ports on trunk connection, channels Not will form trunks And will remain ports access. By default on switchboard 2960 configured dynamic auto mode (dynamic auto).

Part 2: Set up EtherChannel With help protocol Cisco PAgP

Note . At setting channels EtherChannel recommended turn off physical ports before by combining them into channel groups. Otherwise, the Etherchannel Misconfig Guard protection mechanismMaybe translate these ports V state shutdowns V result mistakes (err-disabled). By completion settings EtherChannel ports And aggregated channels Can turn on again.

Step 1: Set up created interface Port Channel 1.

a. The first EtherChannel created for this exercise aggregates ports F0/22 and F0/21.between switches **S1** and **S3** . Use the **show interfaces trunk command** to verify V availability active trunk channel For these two channels.

b. On both switches, add ports F0/21 and F0/22 to the created Port Channel 1 interface with using **the channel-group 1 mode desirable command** . The **desirable mode parameter** (recommended) mode) allows switchboard perform V roles active participant For creation channel PAgP.

c. Set up logical interface V quality trunk. For this at first enter team **interfaceport-channel** *number* **,** and then the **switchport mode trunk command** . Configure both in this way. switch.

Step 2: Check the condition created interface Port Channel 1.

a. To check the functionality of EtherChannel on both switches, run the command**show etherchannel summary** . This command displays the EtherChannel type and the ports used.And states ports.

b. If EtherChannel is not enabled, disable the physical interfaces on both ends of the EtherChannel.And turn on their again. For this on interfaces necessary apply team **shutdown** ,
A through some seconds — team **no shutdown** .
The show interfaces trunk and **show spanning-tree** commands also display aggregated ports.How one logical channel.

Part 3: Set up EtherChannel LACP 802.3ad

Step 1: Set up created interface Port Channel 2.

a. In 2000, the IEEE released 802.3ad , the open standard version of EtherChannel. previous teams, set up channel between switches **S1** And **S2** on ports G0/1 And G0/2
as an EtherChannel using the LACP protocol. On switch **S1,** the number should not be used aggregated channel 1, since you used this number in the previous step. For Use the configuration mode command to configure LACP port aggregation settings . interface **channel-group** *number* **mode active** . Active mode (active) means that the switchactively is trying approve this channel, How LACP V opposite To PAgP.

Step 2: Check state created interface Port Channel 2.

a. Use the **show command** from step 2 of Part 1 to check the status of Port Channel 2. Determine protocol, used each port.

Part 4: Setting up excess channel EtherChannel

Step 1: Set up created interface Port Channel 3.

Enter team **channel-group** *number* **mode** Can differently:

S2(config)# **interface range f0/23 - 24**
S2(config-if-range)# **channel-group 3 mode ?**

Active	Enable LACP unconditionally
auto	Enable PAgP only if a PAgP device is detecteddesirable Enable PAgP unconditionally
on	Enable Etherchannel only
passive	Enable LACP only if a LACP device is detected

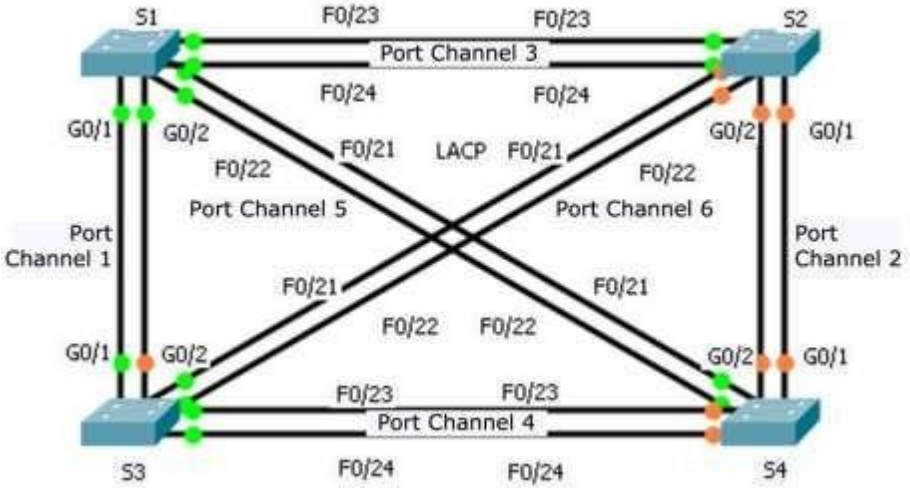
a. On switch **S2,** add ports F0/23 and F0/24 to the created interface Port Channel 3 with help teams **channel-group 3 mode desirable** . Parameter **passive** means, What to you need to, so that the switch only uses LACP if another device is detected. Statically set up created interface Port Channel 3 V quality trunk interface.
b. On switch **S3,** add ports F0/23 and F0/24 to the created interface Port Channel 3 with help teams **channel-group 3 mode active** . Parameter **active** means, What to you need to, to The switch used LACP unconditionally. Statically configure the created Port interface. Channel 3 V as a trunk interface.

Step 2: Check the condition created interface Port Channel 3.

a. Use team **show** from step 2 parts 1, to check state created interface Port Channel 3. Determine protocol, used each port.
b. The created interface Port Channel 2 is not working because the STP protocol has established some ports into blocking mode. Unfortunately, these ports turned out to be gigabit ports. To restore work these ports, set up switch **S1** V quality **primary** (primary) root switch For networks VLAN 1 or install priority on **24576** .

Practical class No. 23. Search And elimination malfunctions EtherChannel operation

Topology



Tasks

Part 1. Examination physical level And elimination problems regime port switchPart 2. Identification and troubleshooting, related With settings Port Channel

Part 3. Identification And elimination problems With protocol aggregation channels

General intelligence

Recently, a junior technician configured four switches. Users were unhappy.slow work networks And asked find you problem.

Part 1: Check physical level And elimination problems,related With modes switch ports

Step 1: Find ports access.

Review the switch configurations. When physical ports are assigned to an EtherChannel port, they work, How one port. Each one pair ports Maybe be or included, or turned off. Their it is forbidden confuse, because the situation is when the indicator on one port is green, and the indicator on the otherport — orange, impossible.

Step 2: Set up ports V mode trunk connections.

a. Make sure, What All physical ports V topology configured on trunk connection. Set up V trunk mode All ports, which are working V quality ports access.
b. If any ports EtherChannel Not configured on trunk mode, fix it This.

Part 2: Identification And elimination problems, relatedWith settings Port Channel

Step 1: Study settings Port Channel.

Topology illustrates physical ports And result their aggregation at creation EtherChannel. Make sure, What switches configured in accordance With topology.

Step 2: Enter adjustments V settings Port Channel.

Conduct adjustment settings ports For corrections mistakes, related With belonging physical port corresponding EtherChannel.

Part 3: Identification And elimination problems With protocol

Step 1: Identify problems With protocol.

IN 2000 year IEEE released 802.3ad (LACP) — version EtherChannel open standard. For provision compatibility team designers decided use LACP By all networks. All ports, tied To channel EtherChannel, should actively approve channel V quality LACP,
as opposed to PAgP. Make sure the physical ports are configured accordingly.With topology.

Step 2: Eliminate problems With protocol.

If any ports switch Not agreed upon With using LACP, fix it This.

Practical Lesson #24: Troubleshooting malfunctions work sequential interfaces

Topology

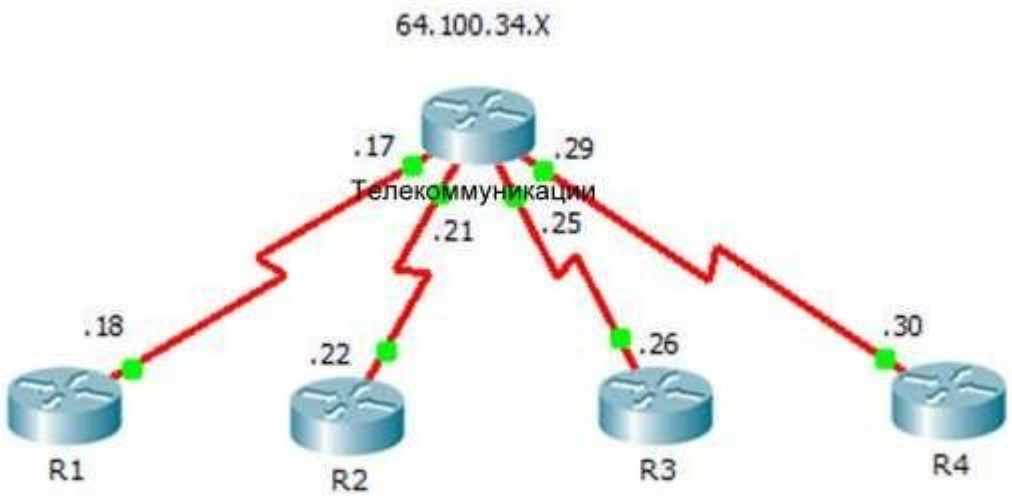


Table addressing

Device	Interface	IP address	Mask subnets	Route by default
Telco	S0/0/0 (DCE)	64.100.34.17	255.255.255.252	N/A (not available)
	S0/0/1 (DCE)	64.100.34.21	255.255.255.252	N/A (not available)
	S0/1/0 (DCE)	64.100.34.25	255.255.255.252	N/A (not available)
	S0/1/1 (DCE)	64.100.34.29	255.255.255.252	N/A (not available)
R1	S0/0/0	64.100.34.18	255.255.255.252	64.100.34.17
R2	S0/0/1	64.100.34.22	255.255.255.252	64.100.34.21
R3	S0/0/0	64.100.34.26	255.255.255.252	64.100.34.25
R4	S0/0/1	64.100.34.30	255.255.255.252	64.100.34.29

Tasks

Part 1. Diagnostics And elimination problems on physical levelPart 2. Diagnosing and Troubleshooting at the Data Link Layer Part 3. Diagnostics And troubleshooting on network level

Scenario

The local telephone company (**Telco**) has asked you to debug your connections.WAN: Telco router needs to connect to four remote nodes, but none of them connections are not working. Use your knowledge of the OSI model and general rules to identify And elimination mistakes V networks.

Part 1: Diagnostics And elimination problems on physical level

Step 1: Diagnostics And elimination problems V system cables.

a. Study table addressing, to define location connections DCE.
b. U everyone sequential connections There is DTE And DCE. To define, connected whether
To interfaces **Telco** correct cables, take a look on third line conclusion teams **showcontrollers** .
Telco# **show controllers** [*interface_type interface_num*]
c. If any cables connected incorrect the end, fix it This.
Note : In real network settings, the DCE parameter (sets the clockfrequency) usually CSU/DSU is indicated.

Step 2: Diagnostics And elimination mistakes connections between ports.

a. Study table addressing on correspondence each port router correct port
Telco .
b. Point pointer mice on every from wires, to make sure, What They connected due way. If this is not So, contribute corrections.

Step 3: Diagnostics And elimination malfunctions turned off ports.

a. Take it out brief description interface each router. Make sure, What no one from ports, which should work, Not was disabled administratively.
b. Turn on ports, disabled administrator.

Part 2: Diagnostics And elimination problems on channel level.

Step 1: Check And set up clock frequencies on equipment DCE.

a. All DCE cables must be connected to **Telco interfaces** . Display the current configuration **Telco** , to make sure, What V each interface installed clock frequency.
b. Install clock frequency on everyone sequential interfaces, Where This required.

Step 2: Check encapsulation on equipment DCE.

a. All serial interfaces must use HDLC as the encapsulation type.Check it out setting protocol sequential interfaces.
Telco# **show interface** [*interface_type interface_number*]
b. Change type encapsulation on HDLC For everyone interfaces, V which installed another type.

Part 3: Diagnostics And elimination problems on network level

Step 1: Check right IP addresses.

a. Print a brief description of each router's interface. Check the IP addresses by addressing table and make sure that they belong to the correct subnet with the appropriateinterface connections.
b. Correct it All IP addresses, which intersect or match With addresses hosta or broadcasts.

Step 2: Check availability connections between by everyone routers.

Practical lesson #25. WAN concepts. Development of complex practical skills

Tasks

In this activity, you will explore different types of WANs by examining the topology usingvarious technologies connections.

- Describe various parameters connections To global networks.

General intelligence And scenario

You will learn about WAN technologies that are used to connect business users anddomestic users To transmission services data.

Note. IN this task No counting points.

Instructions

Part 1. Study technologies WAN For domestic And mobile devices.

Step 1. Study technologies WAN For users.

On this stage You study three technologies WAN For users And home networks.

a. Look at two home networks. Which

technologies WAN are used?

b. Check the connections used in the network topology by selecting the Connections icon (arrow(in the form of an orange lightning bolt) in the PT devices menu. Hover over the media icons todisplay their names V white field in lower parts windows PT.
Which Wednesday handed over data is used For connections two domestic networks To to the supplier Internet services? Which devices in home networks are directly connected to the Internet? to the provider?

c. Click DSL modem And open tab Physical.
Which ports available on device And What To him connected?

What is it? function DSL modem?

What type connections between network ISP/Telco/Cable Company And home cable network? For what needed splitter?

d. Take a look on ports cable modem.
What does cable modem? Which at him connections?

TO which one port connects cable cable modem on home wireless router? Where took on IP address interface?

e. Look on smartphone.
What his IP address? Where took on IP address?

Which one? service transmissions data uses mobile telephone V present time (cellular data or Wi-Fi)?

Step 2. Check it out With business WAN

On this stage You you will be research business WAN. Business is retail store tires. He has a local headquarters where most business functions take place and three stores, which connected to business global networks.

a. Take a look on menu Connections.
Which types connections You you see V business networks?

b. Open physical performance For switch StoreNet.
Which types interfaces presented? Maybe, to you will be required increase And scroll view, to see.

Which interfaces And carriers are used For connections networks stores To networks Business Headquarters? Why This was done?

Which type services WAN is used For connections router Business Headquarters To to the supplier services Internet?

Part 2. Studying opportunities connections

Ping devices V networks Business WAN And Consumer WAN. Also ping between networks And between networks And web server. They can whether All hosts send echo requests Friend to a friend And web server?

Practical class No. 26. Setting up protocol GRE

Topology

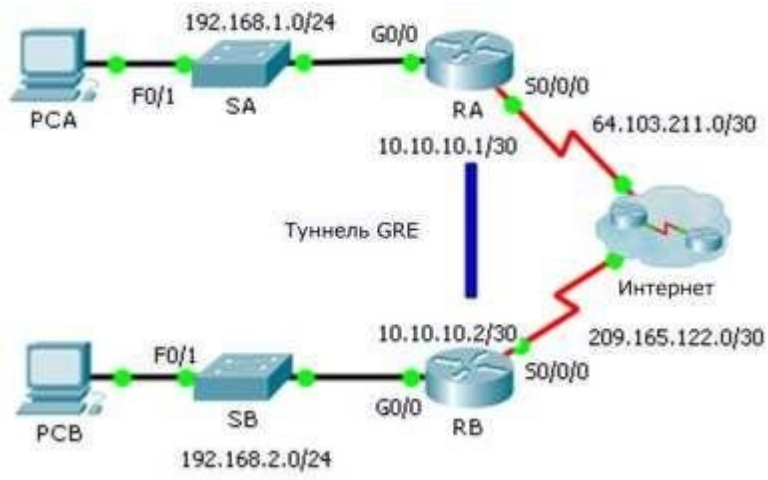


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
RA	G0/0	192.168.1.1	255.255.255.0	N/A (not available)
	S0/0/0	64.103.211.2	255.255.255.252	N/A (not available)
	Tunnel 0	10.10.10.1	255.255.255.252	N/A (not available)
RB	G0/0	192.168.2.1	255.255.255.0	N/A (not available)
	S0/0/0	209.165.122.2	255.255.255.252	N/A (not available)
	Tunnel 0	10.10.10.2	255.255.255.252	N/A (not available)
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Tasks

Part 1. Examination connections routerPart 2. Setting up tunnels GRE

Part 3. Examination connections computer

Scenario

You are a network administrator for a company that needs to set up a GRE tunnel to a remote location's network. office. The local configurations of both networks are configured, and only the parameters need to be set tunnel.

Part 1: Check connections router

Step 1: Execute ping request RA With RB.

a. Use team **show IP interface brief** on router **RA** , to define IP address port S0/0/0.

b. Send With router **RB** ping request on IP address interface S0/0/0 router **RA.**

Step 2: Send echo request With PC B on PC A.

Try it send With **PC B** ping request on IP address computer **PC A** . We let's repeat this test after settings tunnel GRE.
What are results ping request? Why?

Part 2: Setting up tunnels GRE

Step 1: Set up interface tunnel 0 on router RA.

a. Log in V mode settings tunnel 0 on router **RA** .
RA(config)# **interface tunnel 0**

b. Set up IP address according to table addressing.
RA(config-if)# **IP address 10.10.10.1 255.255.255.252**

c. Set up source And recipient For terminal devices tunnel 0.
RA(config-if)# **tunnel source s0/0/0**
RA(config-if)# **tunnel destination 209.165.122.2**

d. Set up tunnel 0 For transmissions traffic IP By GRE.
RA(config-if)# **tunnel mode gre IP**

e. Interface tunnel 0 must be already included. If This Not So, customize his So, How And any another interface.
RA(config-if)# **no shutdown**

Step 2: Set up interface tunnel 0 on router RB.

Repeat steps 1a–1e for the router **RB** . Make sure, that the IP addressing has changed due way.

Step 3: Setting up route For private traffic IP.

Install route between networks 192.168.XX, using net 10.10.10.0/30 V quality networks appointments.
RA(config)# **IP route 192.168.2.0 255.255.255.0 10.10.10.2**
RB(config)# **IP route 192.168.1.0 255.255.255.0 10.10.10.1**

Part 3: Check connections router

Step 1: Send echo request With PC B on PC A.

Try pinging **the PCA's** IP address from **the PCB** . These pings should return a response.answers.

Step 2: Do it tracing from PC A to PC B.

Try to trace from **PC A** to **PC B.** Note the absence of public IPs.addresses V withdrawn data.

Practical class No. 27. Debugging GRE

Topology

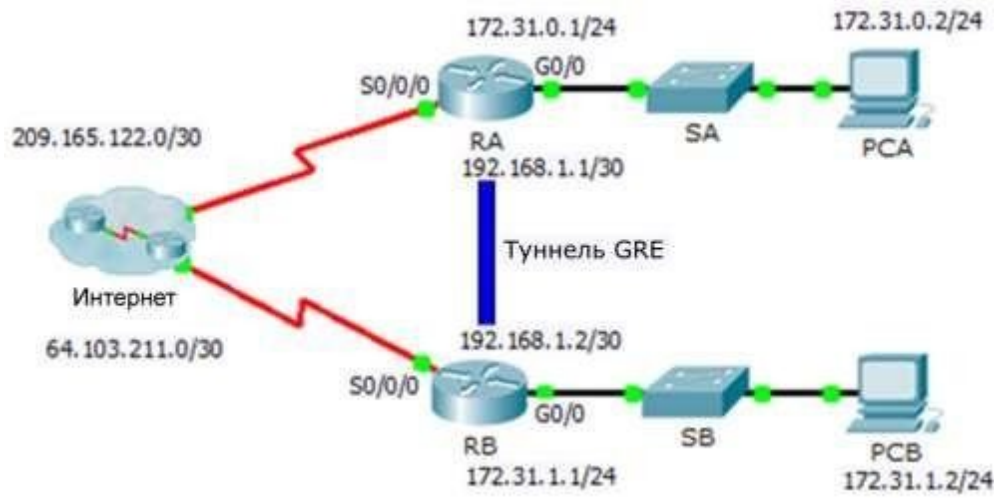


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
RA	G0/0	172.31.0.1	255.255.255.0	——
	S0/0/0	209.165.122.2	255.255.255.252	——
	Tunnel 0	192.168.1.1	255.255.255.252	N/A (not available)
RB	G0/0	172.31.1.1	255.255.255.0	——
	S0/0/0	64.103.211.2	255.255.255.252	——
	Tunnel 0	192.168.1.2	255.255.255.252	——
PC-A	NIC	172.31.0.2	255.255.255.0	172.31.0.1
PC-C	NIC	172.31.1.2	255.255.255.0	172.31.1.1

Tasks

- Find And fix it All mistakes V networks
- Examination connections

Scenario

For settings tunnel GRE between two objects was hired younger network administrator, But He Not coped With task. You asked correct mistakes V setting networks.

Part 1: Find and fix it All mistakes online

Device	Error	Correction

Part 2: Check connections

Step 1: Send echo request With PC B on PC A.

Try it send With **PC B** echo request on IP address computer **PC A** . Must come answers on ping requests.

Step 2: Do it tracing from PC A to PC B.

Try to trace from **PC A** to **PC B.** Note the absence in the resultspublic IP addresses.

Practical class No. 28. Setting up extendedcontrol lists access.

Scenario 8

Topology

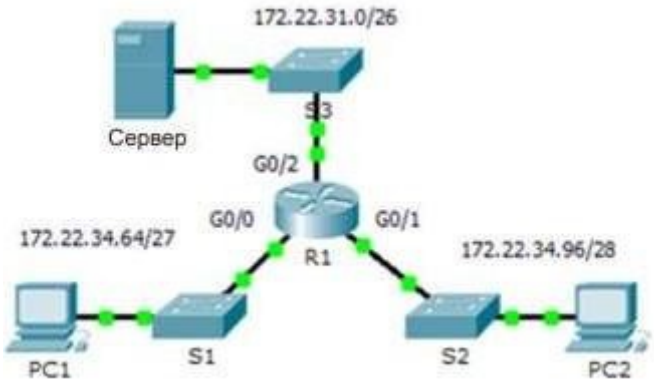


Table addressing

Device	Interface	IP address	Mask subnets	Gateway by default
R1	G0/0	172.22.34.65	255.255.255.224	——
	G0/1	172.22.34.97	255.255.255.240	——
	G0/2	172.22.34.1	255.255.255.192	——
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Tasks

Part 1: Configuring, Applying, and Verifying an Extended Numbered ACLPart 2. Setting up, application And examination extended named ACL list

General information/script

Two employees enterprises required access To services, provided this server. Node **PC1** only needs FTP access, while **PC2** only needs web access. Both computer can send echo requests server, But not a friend to a friend.

Part 1: Setting up, application and verification extendednumbered ACL list

Step 1: Set up ACL list on permission FTP And ICMP.

a. IN mode global configurations on router **R1** enter next team, to define first acceptable number For extended list access.

R1(config)# **access list ?**

<1-99> Standard list control access By protocol IP

<100-199> Extended list control access By protocol IP

b. Add **100** To team, A then put interrogative sign.

R1(config)# **access list 100 ?**

deny Specify packages For ban

permit Please specify packages For redirects

remark Comment To records list control access

c. To allow traffic FTP, enter **permit** , after whom put interrogative sign.

R1(config)# **access list 100 permit ?**

ahp Protocol title authentication

eigrp Protocol routing EIGRP companies Ciscoesp Encapsulating protective useful loadgre Tunnel GRE companies Cisco

ICMP Protocol ICMP

IP Any protocol IP

ospf Protocol routing OSPF

TCP Protocol management transmission data

UDP Protocol custom datagram

d. This ACL list permits FTP And ICMP. ICMP included V list, specified higher, V difference from FTP, which uses the TCP protocol, requires you to enter TCP. Enter **tcp** , to update ACL list.

R1(config)# **access list 100 permit tcp ?**

ABCD Address source

any original knot

host Separate original knot

e. Please pay attention attention, What Can use filtration only For **PC1** , using key the word **host,** or allow any host (**any**). In this case, access is allowed to anyone device with an address belonging to the network 172.22.34.64/27. Enter the network address with the sign question V at the end.

R1(config)# **access list 100 permit tcp 172.22.34.64 ?**

ABCD Bits special symbol source

f. Calculate a wildcard mask that determines the binary opposite of the subnet mask.

11111111.11111111.11111111.111 00000 = 255.255.255.224 00000000.00000000.00000000.000 **11111** = 0.0.0.31

g. Enter network address, A after him — sign question.

R1(config)# **access list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

ABCD Address appointments

any knot appointments
eq C compare only packages With specified number portgt Match only packets with a high port number host Separate knot appointments
lt Match only packets with a lower port number neq Match only packets with a different port number range Match only packages V range numbers ports

h. Set up address destination node. IN this scenarios We filtering traffic V benefit only one addressee — servers. Enter key word **host** , A after him — IP address servers.
R1(config)# **access list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?**
dscp C compare packages with given meaning dscp
eq C compare only packages With specified number port
established installed
gt C м юставят only packages With big number port lt Match only packets with a lower port number neq Match only packets with a different port number precedence
Match packets with the given precedence value range Match only packages V range numbers ports
<cr>

i. Note the **<cr>** (carriage return) parameter. In other words, you can press press **ENTER** , and the rule will allow all TCP traffic. However, we want allow only traffic FTP. That's why enter key word **eq** , after whom put question mark to display the available options. Then type **ftp** and press key **Enter** .
R1(config)# **access list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?**
<0-65535> Port number
FTP Protocol FTP (21)
pop3 Protocol POP3 (110)
SMTP Protocol SMTP (25)
telnet protocol Telnet (23)
www World Wide Web (HTTP, 80)
R1(config)# **access list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

j. Create second rule list access, permissive transmission traffic ICMP (echo request etc.) from **PC1** to **the server.** Please note that the access list number remains unchanged, A specific type traffic ICMP Not requires definitions.
R1(config)# **access list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62**

k. The rest traffic prohibited By default.

Step 2: Apply the ACL on corresponding interface For filtrationtraffic.

From the perspective of router **R1** , the traffic to which ACL 100 applies isincoming from the network connected to the Gigabit Ethernet 0/0 interface. Enter setup modeinterface And apply ACL list.

R 1(config)# **interface Gigabit Ethernet 0/0**
R1(config-if)# **IP access group 100 in**

Step 3: Check work ACL list.

a. Send a ping request from **PC1** to **the server** . If the ping requests are unsuccessful, check the IPaddresses before the way continue work.
b. Send FTP traffic from node **PC1** on **server** . Name user And password — **cisco** .
PC> **ftp 172.22.34.62**
c. Go out from services FTP on **server** .
ftp> **quit**
d. Ping from **PC1** to **PC2** . The destination host should be unreachable becauseabsent obvious permission traffic.

Part 2: Setting up, application And examination extendednamed ACL list

Step 1: Set up ACL list on permission HTTP access And ICMP.

a. Named ACLs begin with the **ip keyword** . In global configuration mode router **R1** enter next team, after which put interrogative sign.
R1(config)# **IP access list ?**
extended Extended list control access
standard Standard list control access
b. You can configure named standard and extended ACLs. By doing this access lists filter both source and destination IP addresses; thusThus, the list should be extended. Enter **HTTP_ONLY** as the name. (For To get more points when working in Packet Tracer, you need to specify a name,sensitive To register).
R1(config)# **IP access list extended HTTP_ONLY**
c. The command line will change. The named advanced configuration mode is now activated. ACL list. All devices on the local network of host **PC2** require TCP access. Enter the networkaddress with familiar question V at the end.
R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**
ABCD Bits special symbol source
d. Another way calculation template masks consists of V subtraction masks subnets from 255.255.255.255.
255.255.255.255
- 255.255.255.240

= 0. 0. 0.15

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 ?**

e. Please finish writing rule, having determined address servers How V parts 1, And having set up filtration traffic **www** .
R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

f. Create second rule list access, permissive transmission traffic ICMP (echo request
And etc.) from **PC2** on **server.** Note. Command line Not changes, ask specific type traffic ICMP no need.
R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

g. The rest traffic prohibited By default. Go out from regime settings named extended ACL list.

Step 2: Apply the ACL on corresponding interface For filtrationtraffic.

From the perspective of router **R1 , traffic to which the HTTP_ONLY** ACL applies , is incoming from the network connected to the Gigabit Ethernet 0/1 interface. Enter the modesettings interface And apply the ACL.

R 1(config)# **interface Gigabit Ethernet 0/1**
R1(config-if)# **IP access group HTTP_ONLY in**

Step 3: Check work ACL list.

a. Send a ping request from **PC2** to **the server** . If the pings are unsuccessful, check the IPaddresses before the way continue work.

b. Send FTP traffic from **PC2** on **server** . Connection Not should be successful.

c. Open web browser on computer **PC2** And enter IP address servers (**Server**) V quality URL- addresses. Connection should be successful.

Practical class No. 29. Search And eliminationproblems. Documentation networks

Topology

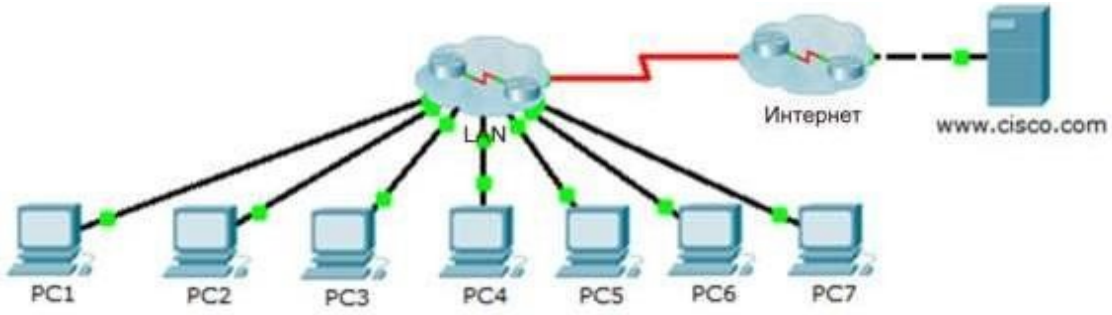


Таблица адресации

Device	Interface	IP address	Mask subnets	Gateway by default
PC1	**NIC**			
PC2	**NIC**			
PC3	**NIC**			
PC4	**NIC**			
PC5	**NIC**			
PC6	**NIC**			
PC7	**NIC**			

Задачи

Part 1. Examination connections
Part 2. Search information O configurations PC
Part 3. Search information O configurations gateway By defaultPart 4.

Searching for routers and neighboring devices on the network Part 5. Drawing

up a topology networks

General information/script

This exercise covers actions, performed For detection networks before total With help Telnet And teams **show cdp neighbors detail** And **show IP route** . This first Part tasks, consisting from two parts. Part II is called **Packet Tracer. Troubleshooting - Using documentation For elimination problems** .

Topology, which You you see, opening given interactive exercise Packet Tracer, displays Not All network information was hidden in Packet Tracer using the clustering feature. The network infrastructure has been collapsed and the topology shows only end devices. YourThe task is to use your knowledge of network organization and the help of commands detection find out And document complete topology networks.

Part 1: Check connections

Cisco Packet Tracer doesn't take long for the network to converge. Send ping requests betweencomputers and the www.cisco.com server to check convergence and test the network. All PCs must receive responses to echo requests from each other and from the server. For successful communication checks Maybe be required send several ping requests.

Part 2: Search information O configurations PC

Step 1: Open the command prompt line on PC1.

Select **PC1** , tab **Desktop** (Worker table), A then open **Command Prompt** (command line).

Step 2: Determine intelligence about addressing For PC1.

To determine the current IP addressing configuration, enter the **ipconfig /all command** . **Note** . IN Cisco

Packet Tracer necessary enter space between **ipconfig** And **/all** .

Step 3: Enter information For PC1 V table addressing.Step 4:

Repeat steps with 1 By 3 on PC2–PC7.

Part 3: Search information O configurations gateway By default

Step 1: Check connection between PC1 And his gateway By default.

From PC1, ping the default gateway to verify that it is available. connections.

Step 2: Connect To gateway By default With help Telnet.

Use team **telnet** *IP address* . IP address Here refers to To gateway By default. IN answer on request password enter **cisco** .

Шаг 3: Просмотрите текущие настройки интерфейсов.

a. To define current settings interfaces, use **show** commands **IP interface brief** And **show protocols** .

b. Document intelligence O mask subnets, output By team **show protocols** .

Step 4: Document Name hosta And interface setting router gatewayfor PC1 V table addressing.

Part 4: Search routers And neighboring devices V networks

Step 1: On router gateway For computer PC1, display tablerouting.

a. Display table routing, using team **show IP route** . You should see 5 connected routes And 6 routes, discovered With help EIGRIP, one from which is route By default.

b. In addition to the routes, write down any other useful information contained in the table.routing, to simplify further study networks And her documentation.

c. Determine, exist whether more any IP addresses, To which Can connect With help telnet, to continue network discovery.

Step 2: Find directly connected devices Cisco.

On the gateway router for PC1, use the **show cdp neighbors detail command** to discover others directly connected devices Cisco.

Step 3: Document intelligence O neighboring devices And check opportunityestablishments connections.

Team **show cdp neighbors detail** outputs intelligence about one neighboring device, including his IP- address. Document the hostname and IP address of the neighboring device and ping it.IP address to test connectivity. The first two or three ping requests will not receive responses until ARP permits MAC address.

Step 4: Try connect To neighboring device With help Telnet And finddirectly connected devices Cisco.

a. Connect To neighboring device With help Telnet And use team **show cdpneighbors detail** For detection others directly connected devices Cisco.

b. IN this once You should see three devices. Router gateway PC1 Maybe be shown For each subordinate interface. **Note** : Run **the show interfaces** command on the switches to determine the information.O mask subnets.

Step 5: Document names hosts And IP addresses neighboring devices And check connection.

Document this data and ping the newly discovered neighbors. devices. Remember that the first two or three ping requests will not receive responses until ARP resolvesMAC addresses.

Шаг 6: Попытайтесь подключиться с помощью Telnet ко всем соседним устройствам And check availability additional devices Cisco.

Install connection By Telnet With each discovered neighboring device And use team **show cdp neighbors detail** For search others devices Cisco. Password For access — **cisco.**

Step 7: Continue process research And documentation networks.

Close sessions Telnet, to return To router gateway By default For computer PC1: From this router, establish Telnet sessions to other devices on the network to continue discovering devices and documenting your network. Don't forget to use **show ip route** and **show cdp neighbors** commands to determine the IP addresses that can be use For connections via Telnet.

Note : Run **the show interfaces** command on the switches to determine the information.O mask subnets.

Step 8: At necessity repeat steps With 1 By 7 For research topology allnetworks.

Part 5: Compilation topology networks

Step 1: Draw topology.

Once you have discovered all the network devices and documented their addresses, create a diagramtopology By information from addressing tables.

Advice. IN center networks located cloud Frame Relay.

Step 2: Save this one documented information.

a. Show me to the instructor my diagram topology, A Also table addressing For checks.
b. These diagram topology And table addressing will be required V parts II this exercises.

Proposed way counting points

Chapter exercises	Question	Maximum quantity points	Earnedpoints
Part 5. Compilation topology networks	Step 2-a	100	
Part 5. Final		100	
Score Packet Tracer		**0**	
General number points		**100**	

LITERATURE

1. Melehin, V. F. Computing systems and networks: textbook for universities / V. F. Melekhin, E.G. Pavlovsky. - Moscow: Academy, 2013. - 207, [1] p. : ill . ; 22. - (Higher Professional education. Automation and control. Bachelor's degree). - Bibliography: p.205-206. - ISBN 978-5-7695-9663-6

2. Pyatibratov, A.P. Computing systems, networks and telecommunications / A.P. Pyatibratov; L.P. Gudyno; A.A. Kirichenko. - 4th ed., revised. and additional - Moscow: FinanceAnd statistics, 2013. - 736 With. - ISBN 978-5-279-03285-3

3. Olifer, V. G. Computer networks: principles, technologies, protocols: textbook . special for universities / V. G. Olifer, N. A. Olifer. - 4th ed. - St. Petersburg [and others]: Piter, 2014. - 944 pp. : ill. - (Textbook for universities). - Grif: Rec. MO. - Bibliography: p. 917. - Alf. decree: p. 918-943. - ISBN 978-5-469-00004-8

4. Shubin, IN. AND. Wireless networks transmissions data: textbook. allowance / V.I. Shubin,O.S. Krasilnikova. - 2nd ed. - M.: Vuzovskaya kniga, 2013. - 104 p.: ill. - On the textbook vulture: Additional UMO. - Bibliography: With. 101. - ISBN 978-5-9502-0725-9

5. Sklyarov, O. K. Fiber-optic networks and communication systems: textbook . p individual / O.K.Sklyarov. - 2nd ed., reprinted - St. Petersburg : Lan, 2010. - 272 p.: ill. - (Textbooks for universities. Special literature). - Bibliographer: pp. 252-261. - ISBN 978-5-8114-1028-6

6. Computer Telecommunications / Yu.Yu. Gromov. - Tambov: Publishing HouseFederal State Budgetary Educational Institution VPO TSTU, 2012. - 224 With.

7. Computer and systems architecture / Yu.Yu. Gromov. - Tambov: Publishing house of the Federal State Budgetary Educational InstitutionHigher Professional Education "TSTU", 2012. - 200 With.

8. Akulinichev, Yu. P. Theory and technology of information transmission / Yu. P. Akulinichev;A.S. Bernhardt. - Tomsk : Tomsk State University of Control Systems and radio electronics, 2012. - 209 With. - ISBN 978-5-4332-0035-7

9. Velichko, V. V. Fundamentals of infocommunication technologies: [study . [p individual] / V.V. Velichko, G.P. Katunin, V.P. Shuvalov. - M .: Goryachaya Liniya-Telecom, 2009. - 712 p.:ill. - The textbook has the following stamp: Rec. UMO. - Bibliography: With. 687-689. - ISBN 978-5-9912-0055-4

10. Karlashchuk, V. I. (North Caucasus Federal University). Fundamentals transmission of discrete messages: Practical training: textbook: Direction of training 210700 - Infocommunication technologies And systems connections. Bachelor, Master's degree / V. I.Karlashchuk, S. V. Yakovlev; North - Cav. federal univ. - Stavropol : NCFU, 2013. - 309 p. - Vulture: Rec. UMO. - ISBN 978-5-9296-0665-6

11. Karlashchuk, V. I. Electronic laboratory on IBM PC. Laboratory practical training on Electronics Workbench and VisSim on elements of telecommunications systems / Karlashchuk V. I. - Moscow : SOLON-PRESS, 2008. - 480 p. - The book is in basic versions EBS IPRbooks. - ISBN 5-98003-211-8

12. Telecommunications systems And networks: studies . p individual For stud. universities connections Andcolleges: in 3 volumes / G. P. Katunin [et al.]; edited by V. P. Shuvalov, Volume 2, Radiocommunications, Radio broadcasting, television. - 2nd edition, corrected and supplemented. - M.: Goryachaya Liniya-Telecom, 2005. - 672 With. : ill. - Bibliography at the end Ch. - ISBN 5-93517-089-2

13. Vasin , N. N. Fundamentals of network technologies based on switches and routers: tutorial / N.N. Vasin. - Moscow: Internet University information technology : Binom. Knowledge Laboratory, 2011. - 270 p : ill. - (Fundamentalsinformational technologies). - Bibliography: With. 253. - ISBN 978-5-9963-0489-9

14. Semenov Yu. A. Telecommunications technologies [electronic resource] // http://book.itep.ru/.

15. Sokolov N. A. Networks subscriber access. Principles constructions - Permian,

Enter-Profi, 1999 [electronic resource] // http://nicksokolov.narod.ru/.
16. Sokolov N. A. Telecommunications networks. - M.: Alvarez Publishing, 2004 [electronic resource] // http://nicksokolov.narod.ru/.
17. NetCracker Professional Users Guide and Reference Manual [electronic resource] //

http://www.netcracker.com/.

Technological map of independent student work

Codes of implemented competencies, indicator(s)	Type of student activity	Assessment tools and technologies	Volume of hours, including		
			SRS	Contact work with the teacher	Total
ID-2 $_{\text{OPK-1}}$ ID-3 $_{\text{OPK-2}}$ UK-1 UK-2	Preparation for laboratory work	Interview	26:00	2.00	36.00
ID-2 $_{\text{OPK-1}}$ ID-3 $_{\text{OPK-2}}$ UK-1 UK-2	Independent study of literature	Interview	26:00	2.00	36.00
		Total	52.00	4.00	72.00