

MINISTRY SCIENCES AND HIGHER EDUCATION RUSSIAN FEDERATION
FEDERAL STATE AUTONOMOUS EDUCATIONAL INSTITUTION OF HIGHER
EDUCATION
« NORTH CAUCASUS FEDERAL UNIVERSITY »

METHODOLOGICAL INSTRUCTIONS

By completion of practical exercises

By discipline

**Computer Communications and Networks/ Computer
Communications and Networking »**

for students in the field of study

11.03.02 Infocommunication technologies And systems connections Direction
(profile)

"Intellectual processing data V infocommunication systems and
networks"

CONTENT

1. Creation straight And crossed cables "unshielded twisted pair".
2. Studying software simulator work networks Cisco Packet Tracer
3. Definition parameters network adapter And settings protocol IP
4. Planning subnets.....
5. Modeling networks With using topological structures general tire and star
.....
6. Study communication equipment Switch 2960
7. Lists management access ACL
8. Transformation network addresses NAT
9. Virtual local networks VLAN
10. Static routing
11. Dynamic routing
12. Study protocol RRR
13. Study technologies Frame Relay
14. Study technologies ATM
15. Comparison switches series 2960 And 3560.
16. Designing a Local Area Network. Practicing
 Comprehensive Practical Skills.
.....
17. Setting up networks VLAN, VTP And DTP.
18. Search And elimination problems With VTP And DTP.....
19. Study design With reservation.
20. Setting up PVST+.
21. Setting up Rapid PVST+.
22. Setting up EtherChannel
23. Search And elimination problems V work EtherChannel
24. Debugging sequential interfaces.
25. Concepts WAN. Working off complex practical skills
26. Setting up GRE.
27. Debugging GRE
28. Setting up extended lists control access.
29. Search And elimination problems. Documentation networks
30. Studying networks computer With using systemic utilities

Practical lesson No. 1.

Creation straight And crossed cables "unshielded twisted pair"

Educational questions:

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

Goals

Create and test direct and crossed unshielded twisted pair (UTP) cable for Ethernet network.

General provisions

On this laboratory lesson required do straight connecting cables And crossed cables For Ethernet. IN direct cable color The color of the wire for contact 1 at one end matches the color of the wire for contact 1 at the other end of the cable. The situation is similar for the remaining seven contacts.

The cable will be based on the TIA/EIA T568A or T568B standard for Ethernet, which defines colors wires for each contact. Direct connecting cables usually are used For direct connecting the node to a hub or computer, or to a wall mount in the 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. The pinouts of this cable comply with the T568A standard at one end and the T568B standard at the other end. on friend. Crossed cables usually are used For connections To concentrators And switches or direct connections two nodes to create a simple network.

The following resources will be required: two pieces of cable 0.6 - 0.9 m long (2 - 3 feet) categories 5 or 5e; Not less four connectors RJ-45 (Maybe - more may be needed if the wires are connected incorrectly); RJ-45 crimping pliers; Ethernet cable tester; wire cutters.

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 Ethernet cable

Step 1: receiving And Preparation cable

a. Determine the required cable length. This may be the distance from the device, such as a computer, to the device to whom it connects (such as a hub or switch), or between the device and an RJ-45 plug. Add at least 1 foot (30.48 cm) to this distance. 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 off piece cable required lengths. For connecting cables (cables between end network devices, such as a PC, and an RJ-45 connector), twisted cable called " unshielded twisted pair " is commonly used because such cables last longer when repeatedly bent . They are called twisted because each of the wires in the cable is made from several veins from clean copper, A Not from one single-core wire . Single-core the wire is used for cable routes between RJ-45 connector and mounting block.

V. WITH help tool For removals isolation clean from sheath both ends of the cable by 5.08 cm.

Step 2: Preparation And insert wires

A. Determine, Which standard will be used. [T568A | T568B]

b. Determine correct table on basis used wire connection standard .

V. Expand couples cables And put it in order their approximately V in the required order based on the selected standard.

G. Unbraid short plot steam And put it in order their V in order, exactly corresponding to the standard.

Very important untwist How Can less plot. Twisting is very important as it provides interference suppression.

d. Straighten it out And smooth out wires between your own big And with the index fingers.

e. Make sure, What order wires cable All more corresponds standard .

g. Cut the straight section of cable 1.25 – 1.9 cm (1/2 – 3/4") from the edge of the cable jacket. If you leave a longer section, the cable will receptive To cross interference (interference, created with adjacent wires).

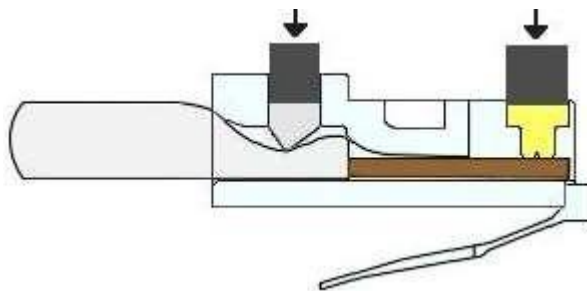
z. When inserting the wires, the protrusion (the pin sticking out of the RJ-45 connector) should be With reverse sides And be directed down. Insert the wires into the RJ-45 connector as far as they will go, all wires should fit into the connector to their maximum length.

Step 3: inspection, bending And repeated cable inspection

A. Take a look cable And check right color code at connecting the wires to the correct contact numbers.

b. Take a look end connector. Eight wires should be tightly compressed at the end of the RJ-45 connector. Some of the cable sheath should extend V connector. This weakens voltage cable. If shell comes in the connector is not deep enough, then in this may ultimately lead to due to cable damage .

V. If All Right aligned And inserted, insert RJ-45 connector and the cable into the crimping pliers. The crimping pliers will crimp the RJ-45 connector with two plungers.



Drawing 1. Connector RJ-45 And cable V crimping pliers

G. Again take a look connector. IN case incorrect installations trim the end and repeat the process.

Step 4: processing another end cable

A. Do it previously described actions, to install RJ-45 connector on the other end of the cable.

b. Again take a look connector. IN case incorrect installations trim the end and repeat the process.

Step 5: testing cable

a. Use a cable tester to check the functionality of the direct cable. If cable Not passed test, again complete given laboratory work .

2. Creation And testing crossed cable Ethernet

Step 1: receiving And Preparation cable

A. Determine required length cable. This Maybe be distance between concentrators, from concentrator to switch, between switches , from a computer to a router, or between computers. Add at least 1 foot (30.48 cm) to this distance.

b. Cut off piece cable required lengths And With help Using a wire stripper, strip 2 inches (5.08 cm) of the sheath from both ends of the cable.

Step 2: Preparation And insert reasons V in accordance with T568A standard

A. Please contact us To table T568A.

b. Expand couples cables And put it in order their approximately V in the required order based on the T568A standard.

v. Unbraid Unravel a short section of pairs and arrange them in an order that closely follows the standard. It's very important to unravel as small a section as possible. Twisting Very important, So how is it provides suppression interference .

G. Straighten it out And smooth out wires between your own big And with the index fingers.

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

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

and. When inserting the wires, the protrusion (the pin sticking out of the RJ-45 connector) should be With reverse sides And be directed down. Insert the wires into the RJ-45 connector as far as they will go, all wires should fit into the connector to their maximum length.

Step 3: inspection, bending And repeated cable inspection

A. Take a look cable And check right color code at connecting the wires to the correct contact numbers.

b. Take a look end connector. Eight wires should be tightly compressed on at the end connector RJ-45. Some Part shells cable should - enter the connector. This relieves the tension on the cable, which can ultimately lead to damage to the cable.

V. If All Right aligned And inserted, insert RJ-45 connector and the cable into the crimping pliers. The crimping pliers will crimp the RJ-45 connector with two plungers.

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

A. Do it previously described actions (But using table And standard T568B) to install an RJ-45 connector on the other end of the cable.

b. Again take a look connector. IN case incorrect installations trim the end and repeat the process.

Step 5: testing cable

A. WITH help cable tester check performance crossed cable. If cable Not passed test, run it again this laboratory work.

3. Testing And definition character malfunctions cable - lay Ethernet .

Define character malfunctions proposed For Cable examination. Describe the nature of the faults.

Questions:

1. Which standard [T568A | [T568B] better use Houses, If Do you have a home network or do you need to create one?
2. Which Part process creation such cables turned out to be the most difficult? Compare your opinion with the opinions of your fellow students.
3. Which length cable chosen And Why?
4. All whether four couples cables twisted the same? Discuss reasons in each case.
5. Many technicians include a crossed cable in mine tools. How You do you think, When follows use What is a crossed cable and in what situations is such a cable used by a network technician ?

Practical lesson No. 2

Studying software simulator work networks Cisco Packet Tracer Study

Questions:

1. Studying opportunities Packet Tracer .
2. Job With files in the simulator.

Theoretical Part

Packet software products Tracer allows you to create network topologies from a wide range of Cisco routers and switches, workstations and Ethernet network connections , Serial , ISDN , Frame Relay . This function can be performed both for training and for work, for example, to configure the network at the planning stage or to create a copy of the working network for the purpose of eliminating malfunctions.

To run Cisco Packet Tracer needs to call the executable file, PacketTracer5.exe. General view programs presented on rice. 1.1.

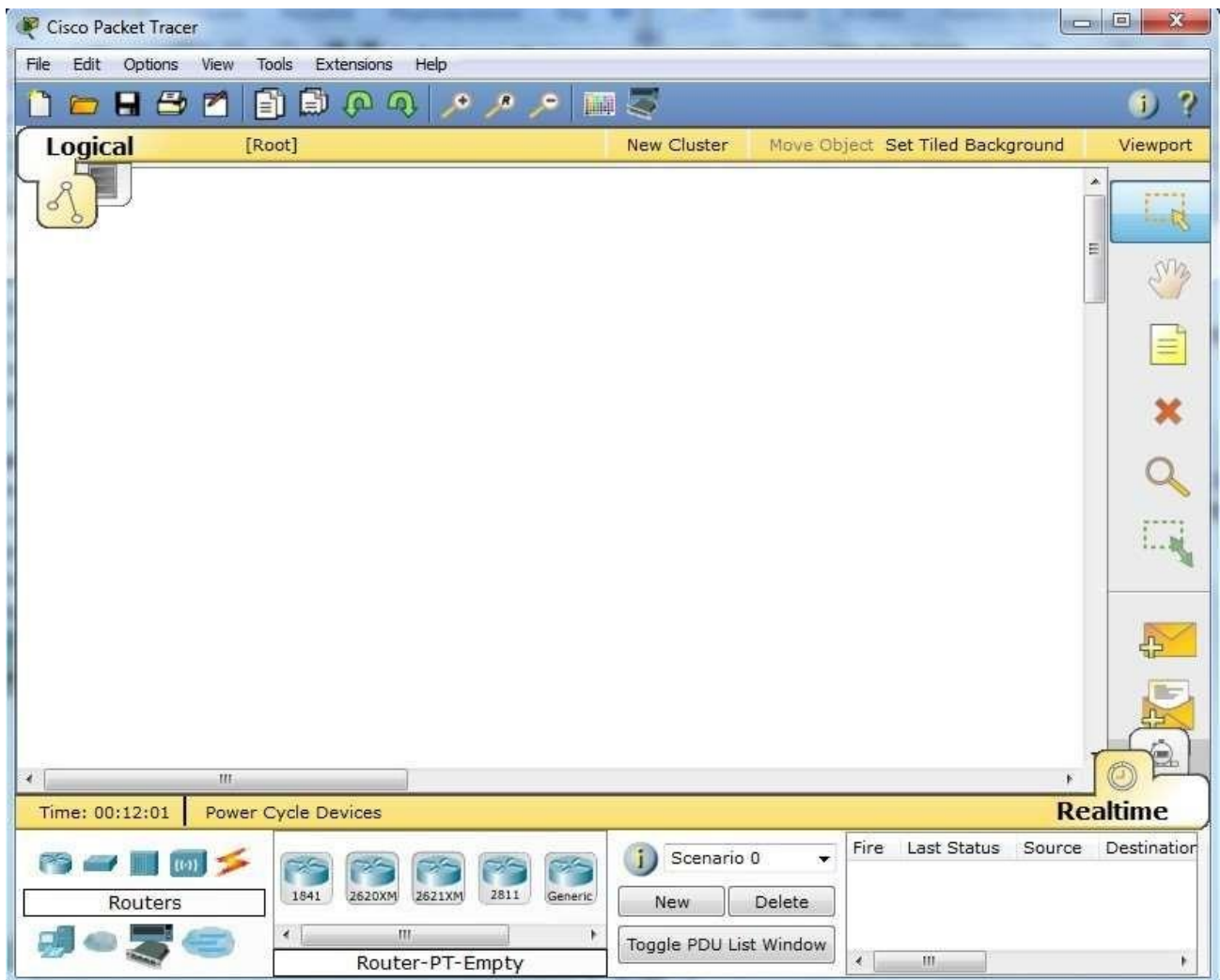


Figure 1.1. General view of the Packet program Tracer Working region windows programs consists of from following elements:

- 1 **Menu Bar** - panel, which contains menu File, Edit, Options, View, Tools, Extensions, Help.
- 2 **Main Tool Bar** - contains graphic images labels For access to the File, Edit, View , and Tools menu commands , and Also Network button Information .
- 3 **Common Tools Bar** – a panel that provides access To most used tools programs : Select, Move Layout, Place Note, Delete , Inspect, Add Simple PDU and Add Complex PDU.
- 4 **Logical / Physical Workspace and Navigation Bar** - panel, which makes it possible to switch the work area: physical or logical , and also allows you to move between levels cluster.

5 **Workspace** – the area in which the network is created, observations of the simulation are carried out and various information and statistics .

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

7 **Network Component Box** – this is the area in which devices are selected And connections For placements their on working space. She contains Device-Type Selection and Device-Specific areas Selection.

8 **Device Type Selection Box** – the area contains the available types of devices and connections in Packet Tracer . Device-Specific Area Selection varies depending on the device selected .

9 **Device-Specific Selection Box** – the area is used to select specific devices and connections required to build a network in the workspace.

10 **User Created Packet Window** – This window manages the packets that were created on the network during the simulation scenario.

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

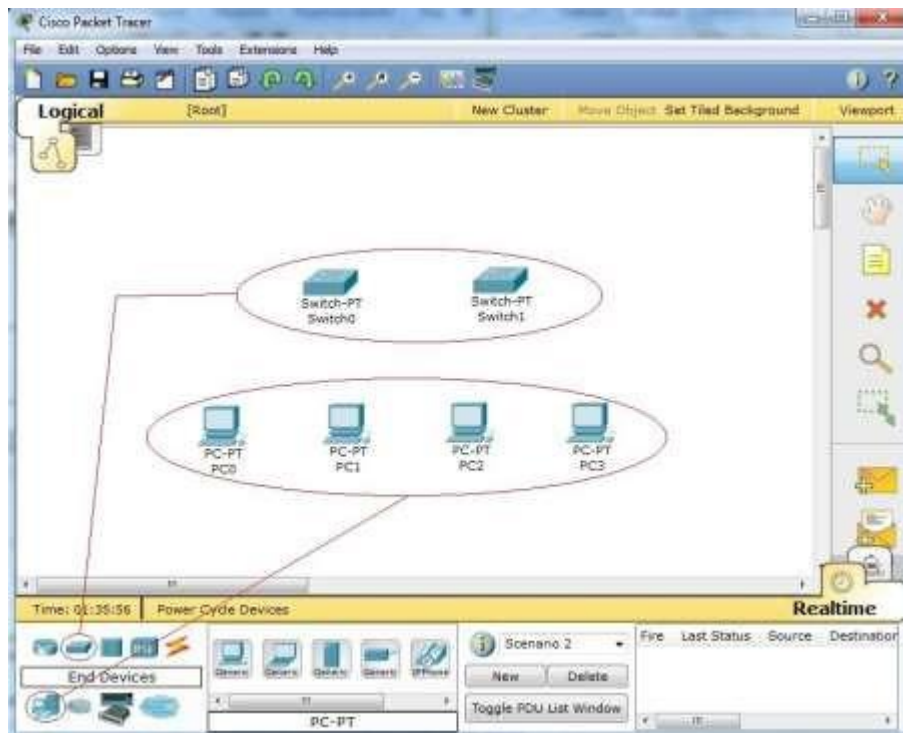
To quickly create multiple instances of the same device, hold down the Ctrl key and click on the device in the Device-Specific area. Selection and release the Ctrl key. After this, you need to click the mouse several times in the work area to add copies of the device.

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 router - tor ;
- devices - cloud, DSL modem And cable modem.

Let's add the necessary elements to the program's workspace as shown in Fig.

1.2.



Drawing 1.2. Addition elements networks

When adding each element, the user has the opportunity Give it a name and set the necessary parameters. To do this, left-click on the desired element and go to the **Config tab in the device dialog box** .

Dialogue window properties each element has two tabs:

- Physical - contains graphic interface devices And allows simulate working with it at the physical level.
- Config - contains All necessary parameters For settings device-

state And has comfortable For this interface.

, depending on the device, the properties may have an additional tab to control the operation of the selected element: Desktop (if an end device is selected) or CLI (if a router is selected) and etc.

To remove unnecessary devices from the program's workspace , use the Delete (Del) button .

We'll connect the added elements using connection links. To do this, select the **Connections tab.** from the Network panel Component Box . We will see all possible types of connections between devices. Let's select suitable Cable type. Indication mice will change on The " connection " cursor (looks like a connector). Click on the first device and select the corresponding interface to which you want to connect, then click on the second device, performing the same operation. You can also connect network elements using **Automatically. Choose Connection Type** (automatically connects elements in the network). Select and click on each of the devices that need to be connected. A cable connection will appear between the devices, and the indicators at each end will show the connection status (for interfaces that have indicator).



Drawing 1.3. Supported V Packet Tracer types cables

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

Table 1. Types connections V Packet Tracer

Type cable	Description
Console 	A console connection can be established between a PC and routers or switches. Certain requirements must be met for a console session to work with a PC: the connection speed must be the same on both ends, there must be 7 data bits (or 8 bits) for both ends, the parity must be the same, and there must be 1 or 2 stop bits for both ends.
Copper Straight - through 	This type of cable is a standard Ethernet transmission medium for connecting devices, which operates at different OSI layers. It should be connected to the following port types: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet), and copper 1000 Mbps (Gigabit Ethernet).
Copper Cross - over 	This type of cable is an Ethernet transmission medium for connecting devices that operate at the same OSI levels. It can be connected to the following port types: copper 10 Mbps (Ethernet), copper 100 Mbps (Fast Ethernet) , and copper 1000 Mbps (Gigabit Ethernet).
Fiber 	Fiber optic Wednesday is used For connections between optical ports (100 Mbit/s or 1000 Mbit/s).
Phone 	Compound through telephone line Maybe be implemented only between devices, having modems ports. Standard performance modem connections - This end device (For example, PC), dialing to the network cloud.
Coaxial 	is used for connections between coaxial ports, such as a cable modem connected to a Packet cloud Tracer .
Serial DCE and DTE 	Serial port connections are often used for WAN links. To configure such connections, synchronization must be set on the DCE side of the device. DTE synchronization is optional. The DCE side can be identified by the small "clock" icon next to the port. When selecting the Serial DCE connection type, the first device to which the connection is applied becomes the DCE device, and the second automatically becomes the DTE side. The reverse is also possible if the Serial connection type is selected. 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 topology has the extension *. pkt .

Packet Tracer allows you to simulate the work with the command line interface (CLI) of the IOS operating system installed on all switches and routers of the company. Cisco.

Once connected to the device, we can work with it as if we were on a console. real device. The simulator provides support almost all commands available on real devices.

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

To simulate the command line on the end device (computer), you need to select the Desktop tab in the properties and then click on the Command shortcut Prompt .

Job With files V simulator

Packet Tracer allows the user to store the configuration of some devices, such as routers or switches, in text files. For this necessary go to To properties necessary devices and in the Config tab , click the “ Export ...” button to export the Startup configuration Config or Running Config . Thus, we will get a dialog box for saving the required configuration to a file that will have the extension * .txt . Text The device configuration file running-config.txt (default name) appears to be similar to the information text obtained using the show command running-config in iOS devices.

Necessary note, that the configuration of each device is saved in a separate text file. The user also has the ability to change the configuration in the saved file manually using a custom text editor. To provide the device with saved or

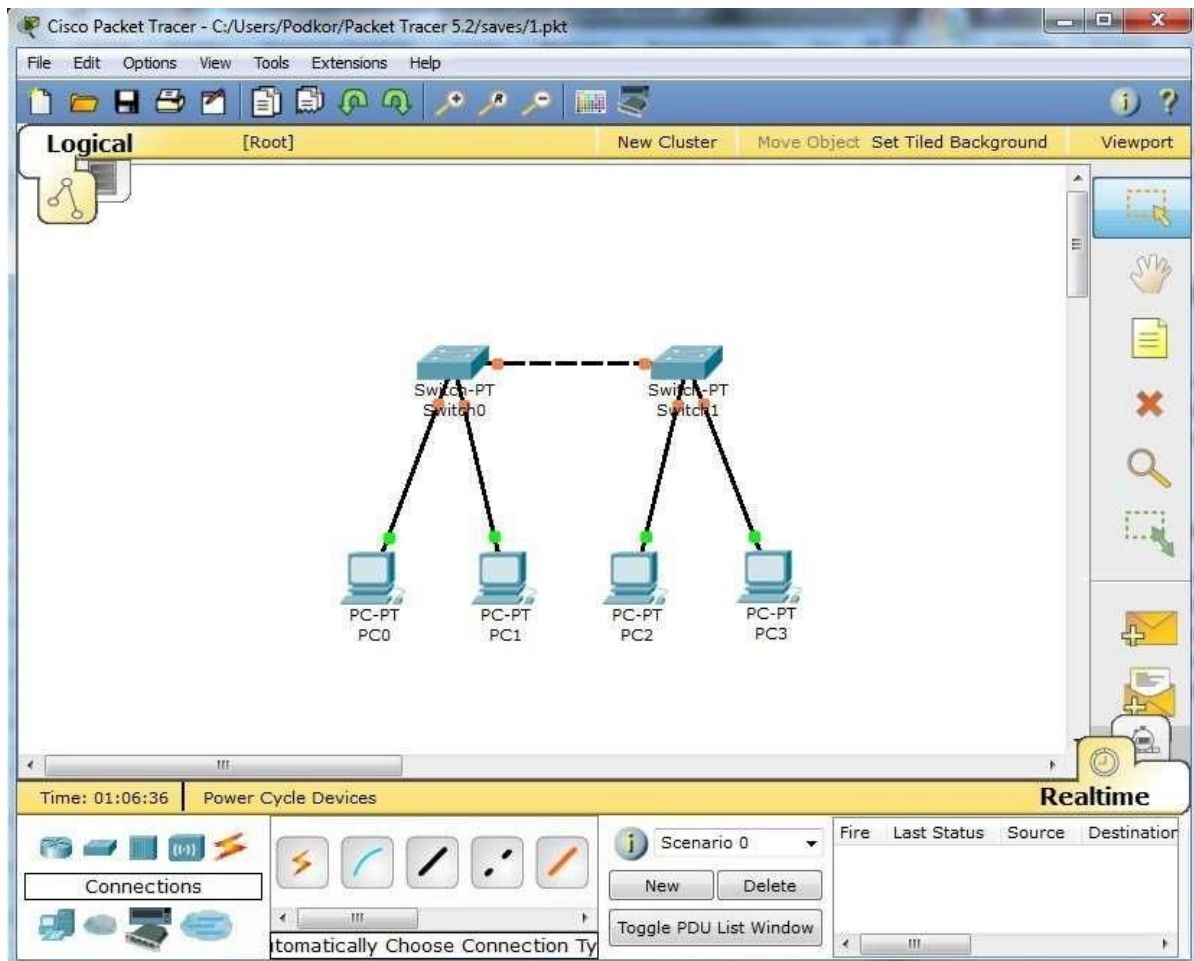
edited settings, you need to click the button in the Config tab “ Load ...” to load the required Startup configuration Config or the “ Merge ...” button to load the Running configuration Config .

Practical Part

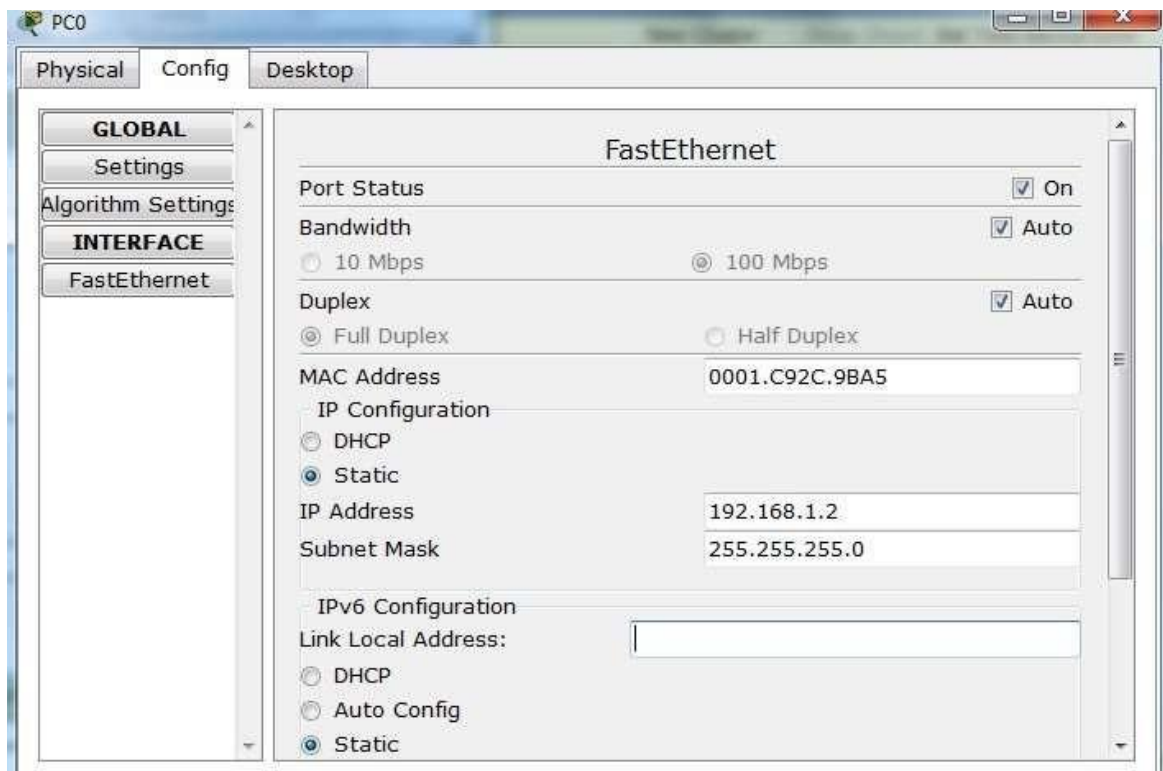
1. Let's add it to the workflow region Switch 2 programs -PT. By default, they are named Switch0 and Switch1.
2. Let's add V working field four computer With names By default PC0, PC1, PC2, PC3.
3. Let's connect devices V net Ethernet, How shown on Fig.1.4.
4. Let's save it created topology, by clicking button Save (V menu File - > Save).
5. Let's open it properties devices PC0 by clicking mouse By his image - niyu . Let's move on To tab Desktop And we simulate work run by clicking Command Prompt .
6. We will get a list of commands if we enter the command ? and press Enter. To configure computer let's take advantage with the ipconfig command from command line, 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 the device's convenient graphical interface (see Fig. 1.4 and Fig. 1.5). In the DEFAULT GATEWAY field , enter the gateway address; in this case, this information is not important, since the network being created does not require routing.



Drawing 1.4. Created fragment networks



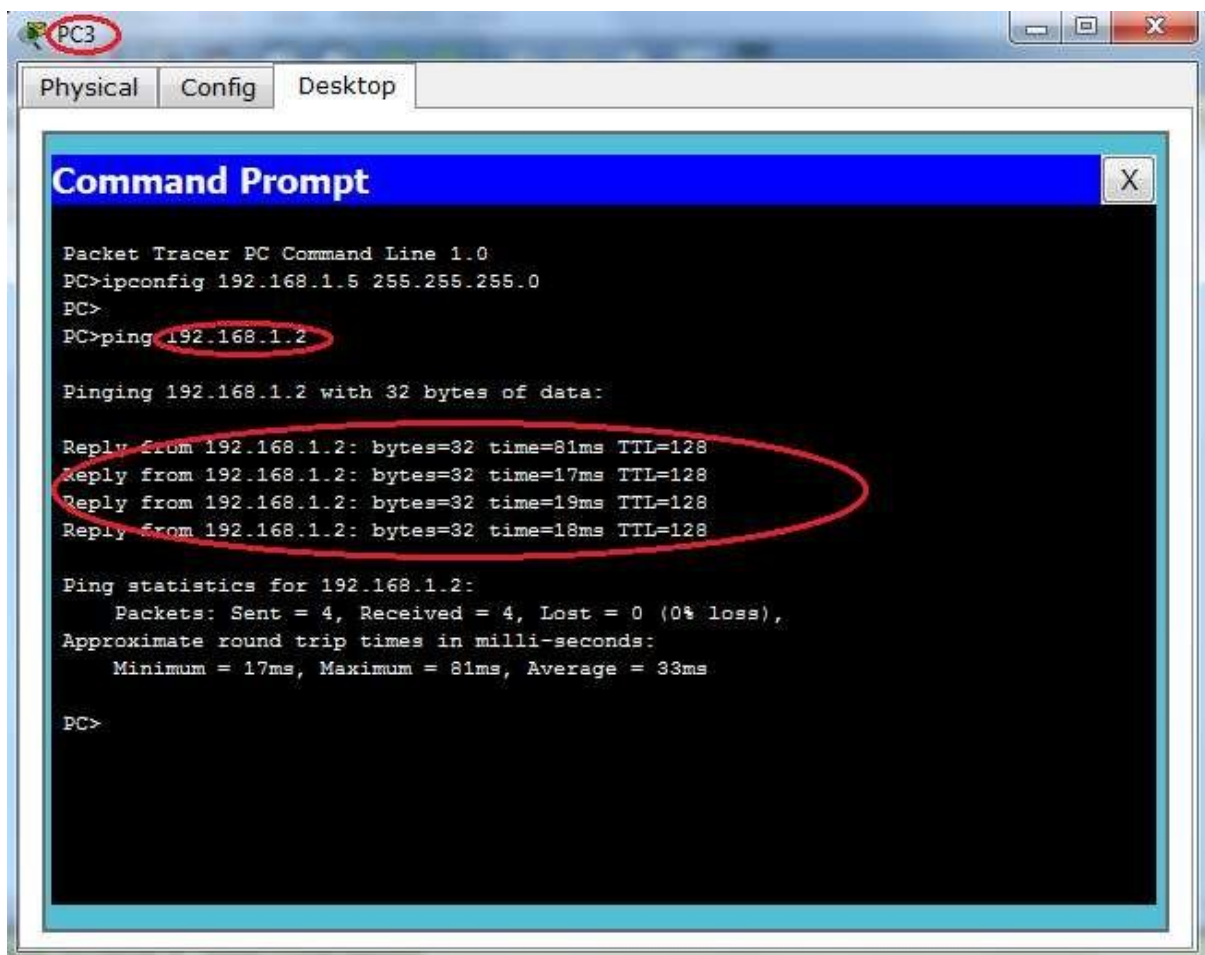
Drawing 1.5. Setting up RS0

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

Table 2. IP addresses And masks computers

Device	IP ADDRESS	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

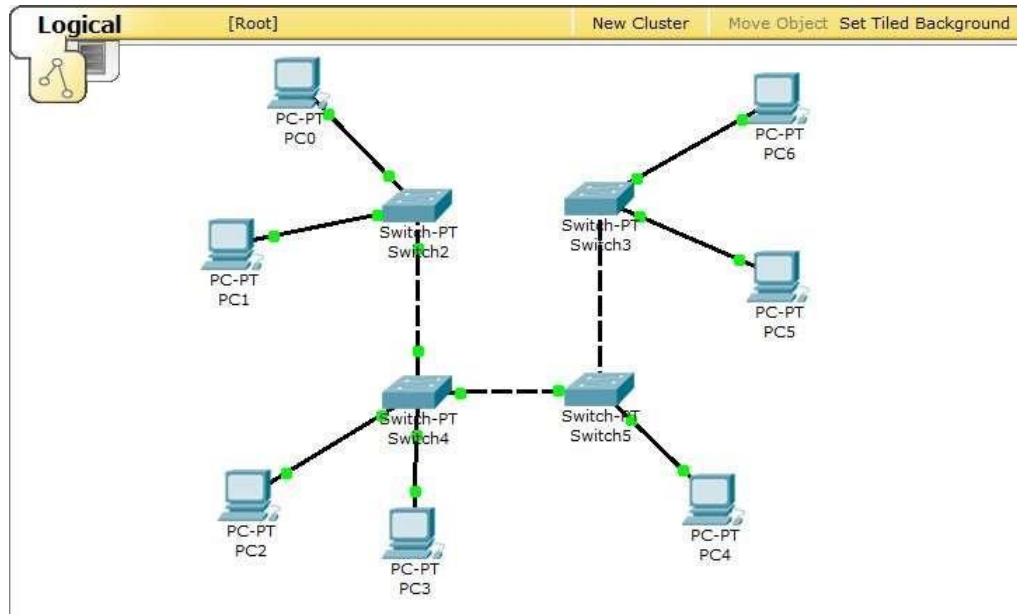
7. On each computer, we will look at the assigned addresses of the command ipconfig without parameters. If everything is done correctly, we will be able to check compound computers With using ping commands . For example, let's log into PC3 and ping it with PC0. We should see a ping report similar to Fig. 1.6.



Drawing 1.6. Report O ping RS3

Exercise For independent work

1. Create topology



Rice 1.7.

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

Table 3. IP addresses and computer masks

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 any computer from any other computer.

Table 4. Options tasks

Option No.	Ping from	Ping V	Variant 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

Supposed, Creation real fragment networks rice. 1.7 And demonstration -

tion teams ping to the teacher according to to his own option.

Order execution And surrender laboratory work

1. Study theoretical And practical Part laboratory work.
2. Submit the theory of work to the teacher by answering the tests questions .
3. Run in Packet Tracer practical part of the laboratory work according to his option.
4. Show your teacher the result of completing the task according to your version. Demonstrate that any computer can be pinged from any computer.
5. Make out And protect report.
6. Report must contain screenshots created topology, A also executing the ping command , according to to his own option.

Control questions:

1. Which maximum quantity devices V networks supports Packet Tracer ?
2. Which types network devices And connections Can use in Packet Tracer ?
3. What way Can go to To interface command device lines .
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. Definition parameters network adapter And IP protocol settings

Target works: Receipt skills V setting network connections V MS Windows XP and in working with the console.

Exercise

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

Brief theoretical intelligence

An IP address (short for Internet Protocol Address) is a unique network address of a node in a computer network built using the IP protocol. When communicating over a network Internet required global uniqueness addresses, V case work V local The network requires uniqueness of the address within the network. It is 4 bytes long. Typically the first and second bytes determine address networks, third byte defines address subnets, A the fourth is the computer's address in the subnet

IP address consists of from two parts: numbers networks And numbers node. IN case For an isolated network, its address can be selected by the administrator from address blocks specially reserved for such networks (192.168.0.0/16, 172.16.0.0/12, or 10.0.0.0/8). If the network is to function as part of the Internet, the network address is assigned by the provider.

The IP protocol's node number is assigned independently of the node's local address. A router, by definition, is a member of several networks. Therefore, each router port has its own IP address. An end node can also be a member of several IP networks. IN this case computer must have some IP addresses, By number of network connections.

Thus, an IP address does not characterize a single computer or router, but a single network connection.

An IP address is called static (permanent, unchangeable) if it is specified in the device settings by the user, or if it is assigned automatically when the device is connected to the network, but is used for an unlimited period of time and cannot be assigned to another device.

An IP address is called dynamic (unstable, changing) if it is assigned automatically when a device connects to the network and is used for a limited period of time, usually until the connection session ends.

Dynamic IP addresses can also be virtual; virtual IP addresses are maintained using NAT technology: users are given the opportunity to freely receive information from the Internet, while any other access is lost. to the computer from the network, so, for example, a computer With like this IP cannot be used as a web server.

Not virtual IP they call real, straight, external, public or public, "white", all such IPs are static.

MAC address (from English Media Access Control - access control to the environment, also Hardware An address is a unique identifier assigned to each piece of computer network equipment. Most data link layer network protocols use one of three IEEE-managed MAC address spaces: MAC-48, EUI-48, and EUI-64. Addresses in each space should theoretically be globally unique. Not all protocols use MAC addresses, and not all protocols that use MAC addresses require these addresses to be unique.

In broadcast networks (such as Ethernet-based networks), the MAC address allows unique identify every knot networks And deliver data only

This node. Thus, MAC addresses form the basis of networks at the data link layer, which is used by higher-level (network) protocols. Special protocols (for example, ARP and RARP in TCP/IP networks) are used to translate MAC addresses into network layer addresses and vice versa.

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

ARP (Address Resolution Protocol) is a low-level protocol used in computer networks, designed to determine addresses channel level By famous address network level. This protocol has become most widespread due to the ubiquity of IP networks built on top of Ethernet, because practically V 100 % cases at such combination ARP is used.

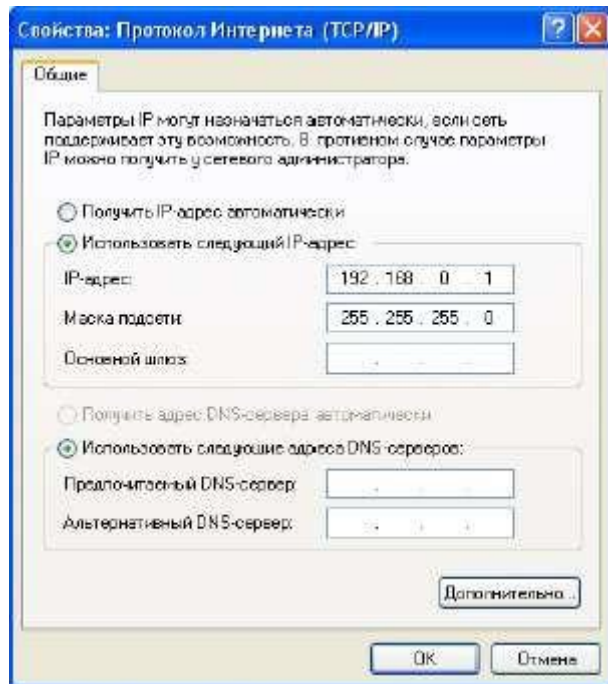
There are the following types of ARP messages: ARP request and ARP reply. (ARP reply). Sender system at help request ARP requests The physical address of the receiving system. The response (the physical address of the receiving node) comes in the form of an ARP response. Before transmitting a network layer packet over an Ethernet segment, the network stack checks the ARP cache to see if the required information about the receiving node is already registered there. If the ARP cache entry is not present, a broadcast ARP request is issued. This request means to devices on the network, "Does anyone know the physical address of the device with the following IP address?" When the recipient with this IP address receives this packet, it should respond, "Yes, that's my IP address. My physical address is: ..." The sender will then update its ARP cache and be able to transmit the information to the recipient. Entries in the ARP cache can be static or dynamic. The example above describes a dynamic cache entry. It is also possible to create static entries in the ARP table. This can be done using the command:

```
arp -s <IP address> <MAC address>
```

Dynamically created ARP table entries remain in the cache for 2 minutes. If data is retransmitted to that address within these two minutes, the cache entry's retention period is extended for another 2 minutes. This procedure can repeat to those pores, Bye recording V cache will exist to 10 minutes. After This entry will be removed from the cache and another ARP request will be sent.

Instructions To performance of work

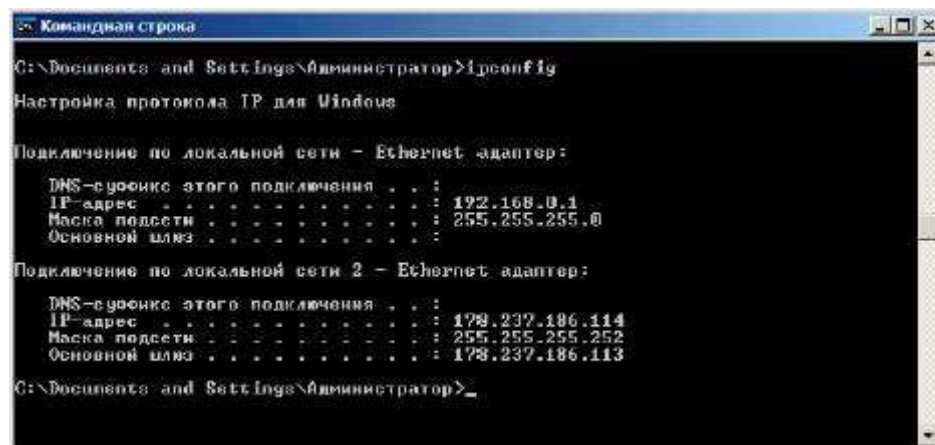
Task 1. Determine the settings of your PC's network adapter. To do this, open the Control Panel window by going to Start - Settings - Control Panel, then clicking the Network Connections shortcut. In the Network Connections window, select the network connection, right-click it, and select Properties from the context menu.



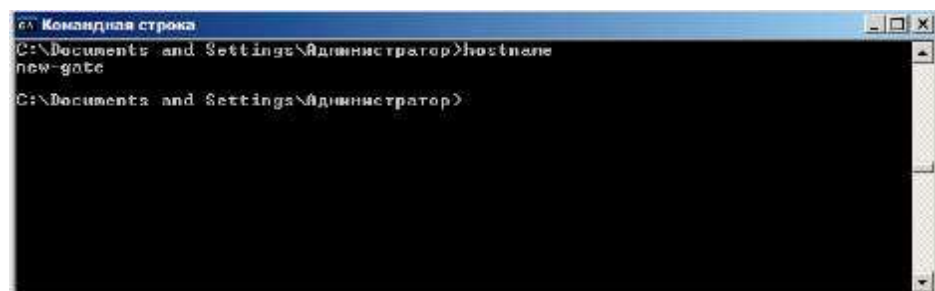
In the Local Area Connection Properties window, select the Protocol component from the list. Internet TCP/IP And click on button "Properties". After this will open Internet Protocol (TCP/IP) Properties window. Record the PC's IP address in the report.

Exercise 2. Determine settings protocol IP of yours computer.

To do this, run the ipconfig program . To access the command prompt, select Programs - Accessories - Command Prompt from the Start menu. In the Command Prompt window, 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 The execution is a table of extended properties of all PC network adapters, including their MAC addresses. These addresses must be reflected in reports.

```
cmd Командная строка
C:\Documents and Settings\Администратор>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : new-gate
Основной DNS-суффикс . . . . . : 
Тип узла . . . . . : неизвестный
IP-маршрутизация включена . . . . . : нет
WINS-прокси включен . . . . . : да

Подключение по локальной сети - Ethernet адаптер:

DNS-суффикс этого подключения . . . : 
Описание . . . . . : Realtek PCIe GBE Family Controller
Физический адрес . . . . . : E8-CB-4E-B4-55-D1
DHCP включен . . . . . : нет
IP-адрес . . . . . : 192.168.0.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 

Подключение по локальной сети 2 - Ethernet адаптер:
NIC
DNS-суффикс этого подключения . . . : 
Описание . . . . . : Realtek RTL8139 Family PCI Fast Ethernet
Физический адрес . . . . . : 00-80-48-22-EF-8F
DHCP включен . . . . . : нет
IP-адрес . . . . . : 178.237.186.114
Маска подсети . . . . . : 255.255.255.252
Основной шлюз . . . . . : 178.237.186.113
DNS-серверы . . . . . : 91.207.136.36
91.207.136.55

C:\Documents and Settings\Администратор>
```

To determine the MAC and IP addresses of PCs located in the same subnet as the one being investigated PC, you need to perform two tasks in sequence console commands: ping [IP] And arp -a. The result execution should become table With data about IP And MAC addresses

```
cmd Командная строка
C:\Documents and Settings\Администратор>arp -a

Интерфейс: 192.168.0.1 --- 0x3
IP-адрес Физический адрес Тип
192.168.0.12 f4-6d-04-99-30-a5 динамический
192.168.0.19 00-1d-92-3b-53-7e динамический
192.168.0.21 6c-f0-49-a3-a1-e9 динамический
192.168.0.22 00-18-f3-0a-d7-71 динамический
192.168.0.23 00-24-1d-c8-8a-24 динамический
192.168.0.28 00-19-db-b7-57-8a динамический
192.168.0.29 00-25-22-81-6a-14 динамический
192.168.0.37 00-21-85-3c-71-51 динамический
192.168.0.39 00-19-db-c3-b6-6b динамический
192.168.0.41 00-1b-11-b2-03-56 динамический
192.168.0.46 00-25-22-85-44-c7 динамический
192.168.0.47 00-1b-11-b2-03-4d динамический
192.168.0.48 00-1d-7d-e9-d1-d6 динамический
192.168.0.49 00-21-85-05-71-50 динамический
192.168.0.50 00-21-85-06-7b-40 динамический
192.168.0.71 00-21-85-06-7b-44 динамический
192.168.0.72 00-21-85-06-72-0f динамический
192.168.0.141 00-19-66-e8-9f-6f динамический
192.168.0.142 70-e6-ba-30-be-0f динамический
192.168.0.181 00-1c-f0-d2-8e-04 динамический

Интерфейс: 178.237.186.114 --- 0x20002
IP-адрес Физический адрес Тип
178.237.186.113 00-26-cb-9d-20-1b динамический

C:\Documents and Settings\Администратор>
```

Bring it in intelligence about addressing others PC subnets V reports. Test questions

1. From what kind parts consists of IP address computer (IPv4)?
2. What what is a MAC address? PC?.
3. List main methods definitions IP And MAC addresses network interfaces.

4. Describe types messages ARP protocol .

Practical lesson #4. Planning subnets

Target and content:

Target

Study methods definitions hosts And discharge subnets

Content

1. Concept IP addressing.
2. Selection subnets.
3. Subnet masks .
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. *An IP address* is a numerical identifier assigned to each computer on an IP network. It reflects the device's location on the network. An IP address is a software address, not a hardware address—the latter is hardcoded into the computer or network interface card.

Hierarchical scheme IP addressing

An IP address contains 32 bits of information, divided into four single-byte (eight-bit) sections, otherwise known as octets. There are three ways to represent IP addresses:

- representation as 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 representations of the same IP address are shown here. The 32-bit IP address has a hierarchical rather than a flat (non-hierarchical) structure. Can to use any scheme addressing, but the hierarchical one is more attractive.

A good example of a non-hierarchical addressing scheme is the numbering of Social Security cards. These numbers do not have any division into sections whose contents would reflect the residence or other characteristics of the cardholder. The advantage of a flat the scheme is a large number of possible addresses, for example, the space of 32-bit addresses, in each position of which there can be 0 or 1, contains 2 or 4.2 billion addresses. The disadvantage of such a scheme is the impossibility of routing, which is why a flat scheme is not used for IP addressing. If all addresses are different, Internet routers would have to remember the addresses of all machines connected to the Internet, which would prevent efficient routing, even when using only a portion of the address space. space.

Therefore, a hierarchical scheme with three levels of hierarchy was chosen for addressing: network, subnet and host. For example let's consider The structure of a telephone number. Its first part (the area code) describes a broad geographic area. The second part (the prefix) narrows this area to the coverage area of the local telephone exchange. The final segment (the phone number itself) identifies a specific connection. With IP addressing Also A three-level scheme is used. Instead of treating the 32-bit combination as a single identifier, the address is divided into parts for the network address and the host address.

A network address uniquely identifies a network. The IP addresses of all machines connected to the same network share the same network address. For example, in the IP address 172.16.30.56, the network address could be 172.16.

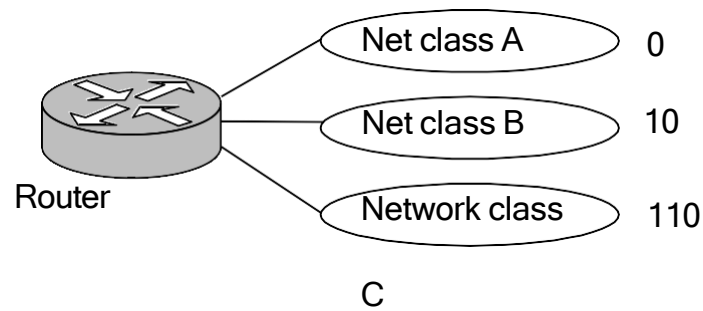
A node address is assigned to each machine on the network. Unlike a network address, which describes a group of devices, a node address is unique and unambiguously identifies a specific machine on the network. A node address is also called a host address. In the example given, the node address is 30.56.

Internet developers decided to create network classes, with a network assigned to a particular class based on its size. *Class A* was created for a small number of networks with a significant number of nodes. *Class C* was reserved for numerous networks with a small number of nodes. *Class B* networks are intermediate-sized networks. The way an IP address is divided into network and host address fields determines the network's class assignment. Table 1.1 provides information about the three network classes.

Table 1.1 - Characteristic classes networks

Class	Format	Started naya bit combinat ion tion	The range of decimal values of the first byte addresses networks	Maximal nye number of networks	Maximum e number nodes in the network
A	Network.Node.Node.N ode	0	1- 127	127	16 777 214
B	Network.Network.Node .Node	10	128- 191	16384	65 534
C	Network.Network.Netw ork.Node	110	192- 223	2097152	254

To ensure efficient routing, Internet designers define a mandatory starting portion of the address for each class. For example, knowing that a Class A network address always begins with 0 allows a router to speed up packet forwarding along the desired route. after recognizing the contents of the first bit of the address. Figure 1.1 shows the correspondence between the network class and the contents of the initial bits of the address.



Drawing 1.1 - Initial bit network combinations

Some IP addresses are reserved for special purposes and are not assigned to network nodes by the network administrator. Reserved addresses are listed in Table 1.2.

Table 1.2 - Reserved IP addresses

Address	Purpose
Network address , consisting from zeros	Interpreted How current net" or "current segment"
Network address , consisting from units	Interpreted How "All networks."
Net 127	Reserved for loopback testing. Designates the local node and is used when the node sends a test plastic bag myself to myself without creation additional traffic
Node address , consisting from zeros	Interpreted How "current knot"
The address of the node consisting of from units	Interpreted as "all nodes" of a particular network; 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 from units (or 255.255.255.255)	Broadcast address (address of messages sent to all nodes of the current network)

Networks class A

In the IP address of class A networks, the first byte is occupied by the network address, and in the next three bytes is located address node. Format IP addresses Class A networks:

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 car this networks should have address networks, equal 49.

The network address is class A and has a length of 1 byte, with the first bit reserved. (cm. table 1.1). This means, What Can create Not more 128 class A networks. Since each of the seven remaining bits can take the value 0 or 1, i.e. there are 2 or 128 different combinations. Was decided, What null address networks (0000 0000) is reserved to indicate the default route (see Table 1.2). Therefore actual number used addresses networks class A is $128 - 1 = 127$.

You you can define This number on one's own. Get Started with lines (with a binary zero and go down the rows, paying attention to the value of the first leftmost bit). The decimal number in the row where this bit first becomes 1 is 127. In other words, Class A network numbers are chosen from the range from 0 to 127. Since address zero is reserved, the range becomes narrower: from 1 to 127. Table 1.2 indicates that network number 127 is also special . Thus, the exact number of Class A networks is 126.

The host address in a Class A IP address is allocated 3 bytes (24 bits). This can accommodate 2^{24} or 16,777,216 different binary combinations or host addresses. Since addresses consisting only of zeros and only of ones, reserved, accurate number nodes V networks class A amounts to 16,777,214.

Networks class IN

In a Class B network IP address, the first two bytes are the network address, and the next two bytes are the host address. The format of a Class B network IP address is:

Network.Network.Node.Node

For example, V IP address 172.16.30.56 address networks equal 172.16, A node address – 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 with the combination 10. Therefore, only 14 bits are left free to form the address; this means that there can be 2 or 16,384 class B networks.

The IP address of class B networks is allocated 2 bytes for the node address. Since addresses consisting of all zeros and all ones are reserved, the exact number of Class B networks is $2^{16} - 2 = 65,534$.

Networks class WITH

The first three bytes of a Class C IP address are occupied by the network address, leaving only one byte for the host address. The format of a Class C IP address is:

Network.Network.Network.Node

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

The first three bits of a Class C network address are occupied by the combination 110. Therefore, only $24 - 3 = 21$ bits remain to form the address. Thus, there can be 2^{21} or 2,097,152 Class C networks.

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 multicast packet distribution.

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

If you don't want to make your life difficult, don't assign nodes addresses from classes D and E in your network.

Subnets

If an organization has many computers or they are located far from each other, it makes sense to break the large network into several smaller ones and connect them via routers. The advantages of this approach include:

- Reduced network traffic. Everyone will feel the reduction in traffic of any kind. type. At this networks remain of the same type. Without routers

Traffic threatens to almost completely slow down the network. And when using them, most traffic remains within the local network; only packets destined for consumers on other networks will be transmitted through the router;

- Network performance optimization. This is a bonus for reducing network traffic;
- Simplified management. It's much easier to identify and resolve problems in a group of small, interconnected networks than in a single large network;
- Simplified coverage of large geographic areas. Wide area network connections are much slower and more expensive than local area network connections. Consolidating numerous smaller networks makes the overall system more efficient.

When an organization with multiple networks receives only one network address from the Network Information Center, various problems arise. The early developers of the IP protocol took into account a significantly smaller The Internet, consisting of dozens of networks and hundreds of hosts, had a separate address for each physical network.

This approach has led to several problems. The first is that the same address is assigned to multiple physical networks. However, an organization can request a separate address for each physical network. If all such requests were granted, the addressing problem would be solved.

The next problem relates to the use of routers. If every router on the Internet had to know about every existing physical network, routing tables would grow enormously. Maintaining such tables would require additional expenses on administration And increase physical

router costs (processor cycle time, memory, disk space, etc.).

An undesirable consequence would be a huge increase in network traffic as routers exchange routing information with each other.

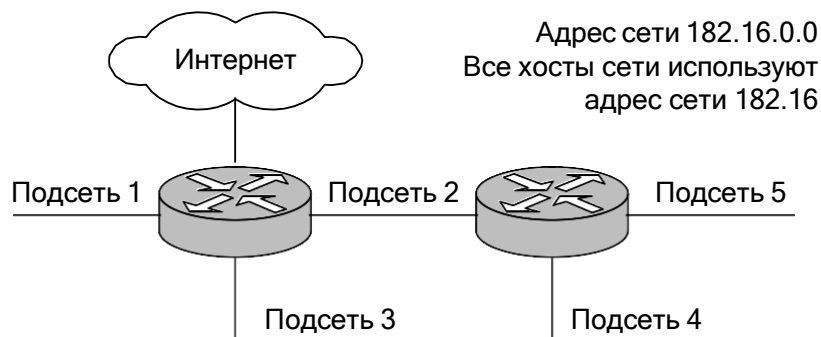
So how do you organize subnets? To create several smaller logical subnets within a single IP network, you can take advantage of a feature of TCP/IP software implementation. This feature is that some bits of the host address in an IP address are allocated to what's known as a subnet address.

Methodology And order execution works:

Methodology

Selection subnets

Subnetting is accomplished by assigning a subnet address to each machine on a given physical network. For example, in Figure 1.2, each machine on subnet 4 has a subnet address of 4.



Drawing 1.2 - Usage subnets

Let's consider the order of placing the subnet address in IP address. Part IP addresses containing the network address cannot be changed because all machines on the network share it. For example, all machines on the Acme network have the address networks, equal 182.16. That's why change Can only the second part of the IP address. IN scheme stations With subnets Part addresses hosta is being considered

How address subnets. On drawing 1.3 shown, How V IP address Maybe The subnet address must be embedded.

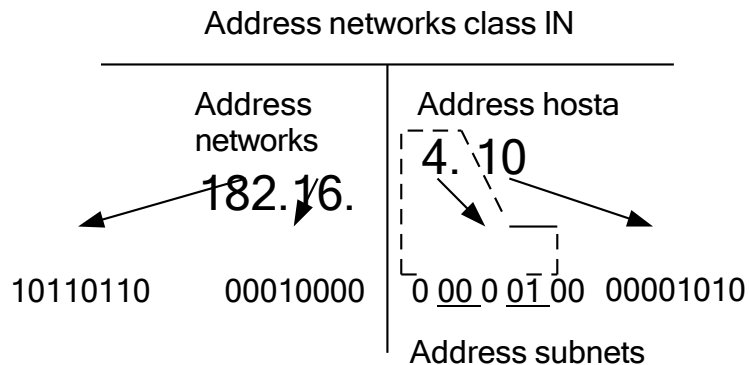
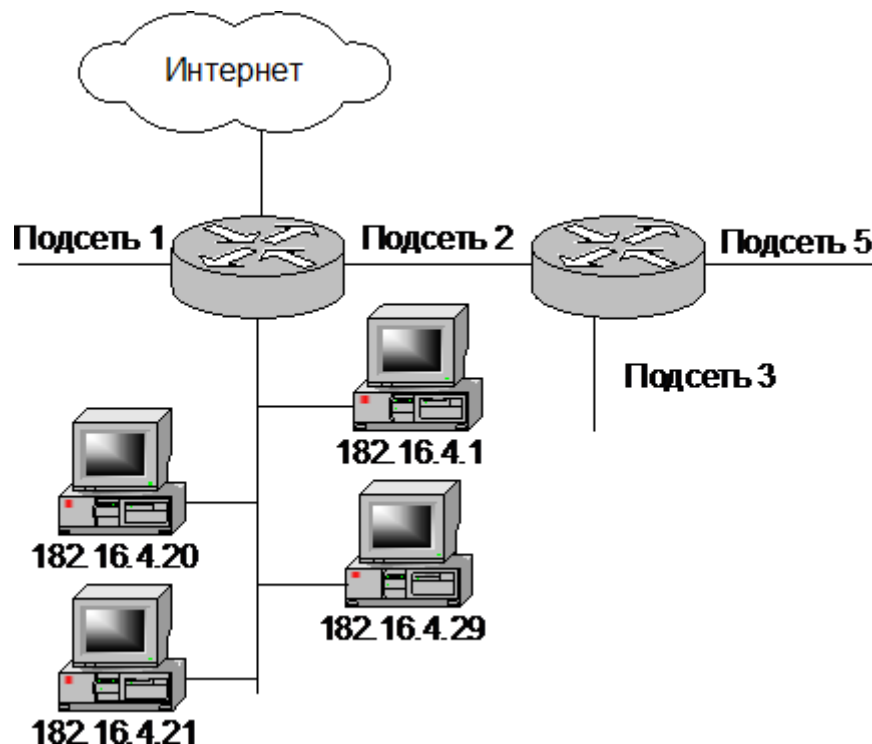


Figure 1.3 – A subnet address can be embedded in an IP address only in the host address portion



Drawing 1.4 - Address networks And subnet address

Because the Acme network is a Class B network, the first two bytes of the IP address contain the network address shared by all machines on the network, regardless of which subnet they belong to. Every machine on subnet 4 must have the number 0000 0100 in the third byte of its address. The fourth byte (host address) contains a unique number identifying a specific host. Thus, an IP address consists of three fields: network address, subnet address, and host address.

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 subnet addressing scheme, each machine on the network must know what portion of the host address is occupied by the subnet address. To do this, each machine creates a subnet mask.

Coding discharges masks subnets

Units marked position addresses networks And subnets Zeros mark the position of the host address

Mask subnets For companies Acme Inc .

11111111 . 11111111	11111111	00000000
Позиция адреса сети	Позиция маски подсети	Позиция адреса хоста

Drawing 1.5 - Subnet mask

The network administrator creates a 32-bit subnet mask consisting of 0 and 1. The ones in the subnet mask mark the positions that belong to Network and subnet addresses. Zeros are entered into the positions allocated for the host address. This idea is illustrated in Figure 1.5.

In the example, the first two bytes of the subnet mask are filled with ones, since the Acme network is a Class B network (the format is Network.Network.Node.Node). The third byte, which typically corresponds to the host address, is the subnet address. Therefore, all its bits are filled with ones. Only the fourth byte stores the unique host address.

The subnet mask can also be represented in decimal format. Binary combination 1111 1111 corresponds decimal number 255. Thus, the subnet mask of our example can be displayed in two ways. This idea is illustrated in Figure 1.6.

Двоичное представление 11111111.11111111.11111111.00000000 Десятичное представление: 255.255.255.0
--

Drawing 1.6 – View IP addresses With help masks subnets

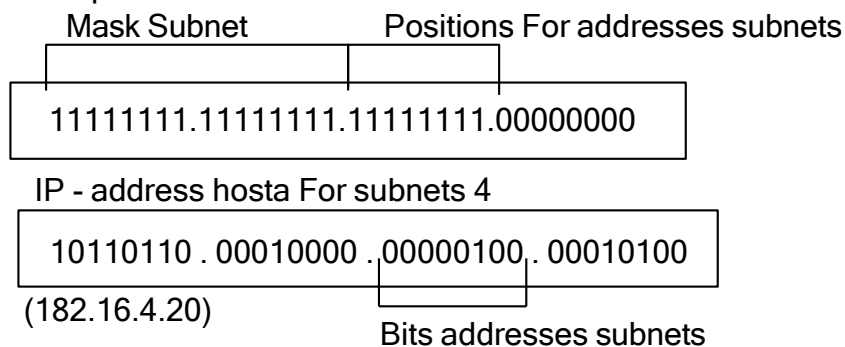
A network does not necessarily have to contain subnets, i.e. a subnet mask may not be used. In such cases, there is a default subnet mask. Default masks for different network classes (see Table 1.3) cannot be changed. In other words, using 255.0.0.0 as a subnet mask is not allowed. The host to which you try to assign such a mask will consider it invalid and will not allow you to complete the operation. For class A networks, the first byte of the subnet mask cannot be changed, so it must start with 255. In addition, the mask 255.255.255.255 is not allowed, since this configuration denotes a broadcast address. The subnet mask for class B networks must start with 255.255, and for class C networks, with 255.255.255.

Table 1.3 - Masks subnets, accepted By default

Class network s	Format addresses	Subnet mask
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

Coding discharges masks subnets

Units marked position addresses networks And subnet Zeros
- the position of the host address



Drawing 1.7 - View IP addresses With help masks subnets

Once the network administrator creates a subnet mask for each machine, software security protocol IP will browse IP-

addresses using the subnet mask to determine the subnet address. The corresponding operation is shown in Figure 1.7.

In this example, the subnet mask is used to programmatically determine that the third byte of the IP address no longer corresponds to the host address, but is occupied by the subnet address of 0000 0100.

Acme network Inc. needs to define subnet 12, in The third byte of the addresses of all machines in this subnet should be set to 0000 1100.

At use total third IP address bytes class IN For subnet addresses, you can create quite a few subnets. Indeed, since the byte consists of from eight bits, Can define $2^8 = 256$ various addresses. Since an address cannot consist solely of ones or zeros, the number of possible subnets is reduced to 254. Thus, in the Acme network Inc. can be allocated up to 254 subnets, each of which will contain up to 254 hosts.

Although the official IP protocol specification limits the use of the zero subnet address, some software products still use this address. same For example, adding special commands to a Cisco router allows for subnets with a zero address, increasing the number of possible subnets to 255. However, by default, such a change is not possible.

IP-адрес: 182.16.52.10	Помеченные биты
Маска подсети: 11111111 . 11111111 . 11110000 . 00000000	
255 . 255 . 224 . 0	

$2^{(\text{число помеченных битов})} - 2 = \text{число подсетей}$ $2^3 - 2 = 6 \text{ подсетей}$

$2^{(\text{число непомеченных битов})} - 2 = \text{число хостов}$ $2^{13} - 2 = 8190 \text{ хостов в подсети}$

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

$$2^{(\text{number of marked bits in the subnet mask})} - 2 = \text{maximum number of subnets}; 2^{(\text{number unmarked bits} \vee \text{mask subnets})} - 2 = \text{maximum number hosts} \vee$$

subnets.

marked , while bits with a value of zero *are considered unmarked* . Figure 1.8 shows an example of applying these formulas.

Thus, if the number of marked bits is 3, up to six subnets can be created according to the formulas given . 5 bits in the third byte and 8 bits in the fourth byte remain for host addressing. With 13-bit addresses, up to $2^{(13)} - 2 = 8190$ hosts can be connected to a subnet .

When reverting to using the full byte of the host address as the subnet address (mask 255.255.255.0), the possible number of hosts in each subnet will be reduced. Without discharge subnets address class IN Maybe have 65 534 different values that are allowed to be used as host addresses.

If the subnet address occupies a full byte of the host address, the remaining only one byte For addresses hosts, T. e. $\vee$ subnets Can place to 254 hosts. When $\vee$ some subnets will be required increase This number,

arise difficulties. For them permissions it is necessary to either shorten The subnet address field in the mask can be expanded, thereby increasing the host address length, or a secondary IP address can be added to the router interface, which will also increase the number of hosts in the subnet. However, this solution will also reduce the number of subnets created.

tasks Using Windows Calculator to Solve Network Problems

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

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

With help power functions determine number nodes, which can be assigned addresses based on the available number of bits.

Step 1: inclusion calculator Windows And definition its operating mode

A. IN menu "Start" select " **All programs > Standard** ", and then – “ **Calculator** ” Fig. 1.9.



Drawing 1.9 - External type of calculator

Alternative method launch applications "Calculator" - Open the **Start menu**, select Run, and enter **calc** and press the "**Enter**" key. Try both methods.

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

Determine which mode [Normal | 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 in this mode? (Eight)

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

Step 2: transition between systems numeration

a. Go to **Engineering mode** . Note the available options. 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 in decimal mode.

G. Install switch **Bin** (binary). Which numbers on the numeric keypad are currently active? (0 and 1)

d. Why other numbers unavailable?

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

and. Make sure, What symbols 0 - 9, A Also A, B, C, D, E And F on The numeric keypad is currently active. The hexadecimal number system (base 16) uses 16 digits.

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

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

By switching modes, numbers are converted from one number system to another. V another. Again go to V **Dec** mode . Number V window will return to decimal form. Select **Hex mode** .

l. Which hexadecimal number (0 - 9 or A - F) corresponds to the decimal number 15?

m. Clean up window from numbers 15. Again go to V **Dec** mode . For you can enter numbers use Not just a mouse, but also The numeric keypad and number keys. Using the numeric keypad located to the right of the **Enter key** , enter the number **22** .

If the number is not appears in the calculator field, press the key « **Num Lock** " to enable the numeric keypad. Once the numbers 22 V text field calculator With help keys Using the numbers at the top of the keyboard, add **0** to the number 22 (the field should then display 220). Set the **Bin radio button** .

n. Which binary number corresponds decimal the number 220?

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

enter following binary number: **11001100** . Install switch

Dec .

p. Determine, which decimal number corresponds binary number 11011100?

r. Transform next decimal numbers V binary. Make sure the results you get match the numbers below.

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

With . Transform next binary numbers V decimal. Check the result obtained.

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. Ethernet. For facilities users IP address usually seems to be as 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 converted to 8 binary digits. Remember that a computer only understands binary digits. If all 4 octets were converted to binary, how many digits would there be? (An IP address is 32-bit, 4x8.)

b. IP addresses usually introduce themselves V view four decimal numbers that take values between 0 and 255 and are separated by a period.

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 to only four digits, and 2 is converted to two digits. Since any number from 0 to 255 can be specified in each position of an IP address, eight digits are typically used to represent each such number. In the previous example, eight digits were required to represent the numbers 192 and 168 in binary form, but 10 and 2 do not require that many digits. Typically, zeros (0) are appended to the left of each binary-converted IP address number to produce eight binary numbers. Number 10 should be presented V view 00001010. Four zeros are added before the four significant binary digits.

G. IN text field calculator V binary mode enter numbers

00001010 And install switch **Dec** .

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

Do leading zeros affect the number?

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

Step 4: transformation masks 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 of four 8-bit octets, each represented as a decimal number. With the exception of the decimal number 0 (all 8 binary digits are zeros) and the decimal number 255 (all 8 binary digits are ones), each octet will have some ones on the left and some zeros on the right. Convert the 8 possible decimal values of the subnet mask octets to binary form.

Decimal number	Binary numeric
0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

b. Transform four component masks subnets 255.255.255.0 to binary form.

Decimal number	Binary number
----------------	---------------

255	11111111
255	11111111
255	11111111
0	0 (8 zeros)

Step 5: transformation broadcast addresses

- a. Networked computers and devices use broadcast addresses to send messages to entire groups nodes. Transform next broadcast addresses.

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 by two digits, 0 and 1. When calculating the number of possible nodes in a subnet, powers of 2 are used due to binary representation. As an example, consider a subnet mask that leaves six digits in the node portion of the IP address. In this case, the number of nodes in the network is 2 to the 6th power minus 2 (since one number is required to represent the network, and another to reach all nodes in the network, i.e., for the broadcast address). The number 2 is always used because we are working in binary. The number 6 determines the number of digits corresponding to nodes.

b. IN field calculator V mode **Dec** enter number **2** . Click the button " x^y ", which corresponds to raising a number to a certain power. Enter number **6** . Click button « = », A then - key "**Enter**" or "=" on the keyboard are equivalent ways to get the final result. The result will be 64. To subtract two, press the key with

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

This means, What Maybe be used 62 knots.

V. WITH help described higher process determine number nodes, if the following number of digits are used to represent nodes.

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

G. WITH help mastered method determine, what equals 10 to the 4th power.

d. Close calculator Windows.

Step 7: definition numbers 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 of bits remaining for the nodes, calculate how many nodes can be created.

b. Start by converting the 4 octets of the decimal IP address to binary, then convert the decimal subnet mask to binary. When converting to binary, remember to add leading zeros to get 8 digits 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 bits of the IP address that correspond to the ones-numbered bits in the subnet mask represent the network number. What is the binary and decimal network number for this IP address? First, determine the binary address (include all 32 bits), then convert it to decimal.

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

Network address in decimal form: 172.16.200.0

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

_____21

d. How many discharges left For creation nodes?

_____11

e. How many nodes Can create With remaining number discharges?

$$2^{11} = 2048 - 2 = 2046$$

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 172.16.0.0 network, it is necessary to allocate subnets so that up to 600 hosts can be connected to each subnet. What is the subnet mask? follows choose, to allow height numbers subnets V future?

2. Network 172.16.0.0 contains 8 subnets. You need to connect To subnets maximum possible number hosts. Which one? What subnet mask should I choose?

3. IN networks 192.168.55.0 necessary highlight maximum the number of subnets is so, to To each subnets Can it was necessary to connect 25 hosts. Which subnet mask should I choose?

4. Yours net class A contains 60 subnets. IN next two In the next year, you need to organize 40 more subnets, each of which can accommodate the maximum number of hosts. Which subnet mask should you choose?

5. U you there is net class WITH With address 192.168.19.0, containing four subnets. You need to set the maximum possible number of hosts on the segment. Which subnet mask should you choose?

6. U you There is net class IN, divided on 30 subnets. You You want to add 25 new subnets in the next two years. You'll need to connect up to 600 hosts to each segment. What subnet mask should you choose?

7. Network 192.168.1.0 needs to be divided into 9 subnets. In this case, it is necessary connect To to everyone segment maximum possible number of hosts. Which subnet mask should I choose?

8. U you there is net class WITH With three subnets. To you We need to add two new subnets in the next two years. Each network should contain 25 hosts. Which subnet mask should we choose?

9. In your existing class C network address 192.168.88.0 you need highlight maximum possible number subnets, V each of which should be up to 12 hosts. Which one? mask subnets should be selected?

10. You chose mask subnets 255.255.255.248. How many subnets and will you get hosts?

11. U you There is IP address 172.16.13.5 And mask subnets 255.255.255.128. Specify the address class, subnet address, and broadcast address.

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

13. Transformation IP- And MAC addresses of the node

- a. Click the **Start button** , select **Run** , and type **cmd** and press the **Enter key** . At the command prompt, type **ipconfig / all** .
- b. Mark IP address And physical address (Also famous How MAC address).

IP address:

MAC address:

V. WITH help calculator transform four numbers IP addresses to binary form.

Десятичное число	Двоичное число
------------------	----------------

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

A MAC address, or physical address, is typically represented by 12 hexadecimal digits grouped in pairs and separated by dashes (-). Physical addresses on Windows computers are typically displayed in the format xx-xx-xx-xx-xx-xx , where x is a digit from 0 to 9 or a Latin letter from A to F. Each hexadecimal digit in the address can be converted to a 4-bit binary number that the computer can understand. If all 12 hexadecimal digits were converted to binary, how many digits would there be? (A MAC address is 48 bits, 12x4.)

d. Convert each hexadecimal pair to binary form. For example, if the group of numbers CC-12-DE-4A-BD-88-34 corresponds to a physical address, convert the hexadecimal number to binary form (11001100). Then transform To binary view hexadecimal number

12 (00010010) and so on. Make sure to add the required number of leading zeros to get 8 binary digits for each pair of 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

You need to solve the problems according to your version, and in problems 1-12 write down the solution results in binary, decimal and hexadecimal number systems.

Content report And his form:

The report should be formatted according to the format of a simple abstract. The title page should include: the title of the course, the title of the lab work, the last name and initials of the submitting student, the group number, and the last name and initials of the receiving instructor. part of the work must 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; d)
- conclusions on the work done.

The task must be completed in accordance with the examples given.

Protection work

Protection work consists of:

1) V execution tasks And design report V in accordance with the sub-clause “Contents of the 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 purpose 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 lesson 5

Modeling networks With using topological structures general tire and the star

Target And content:

Target

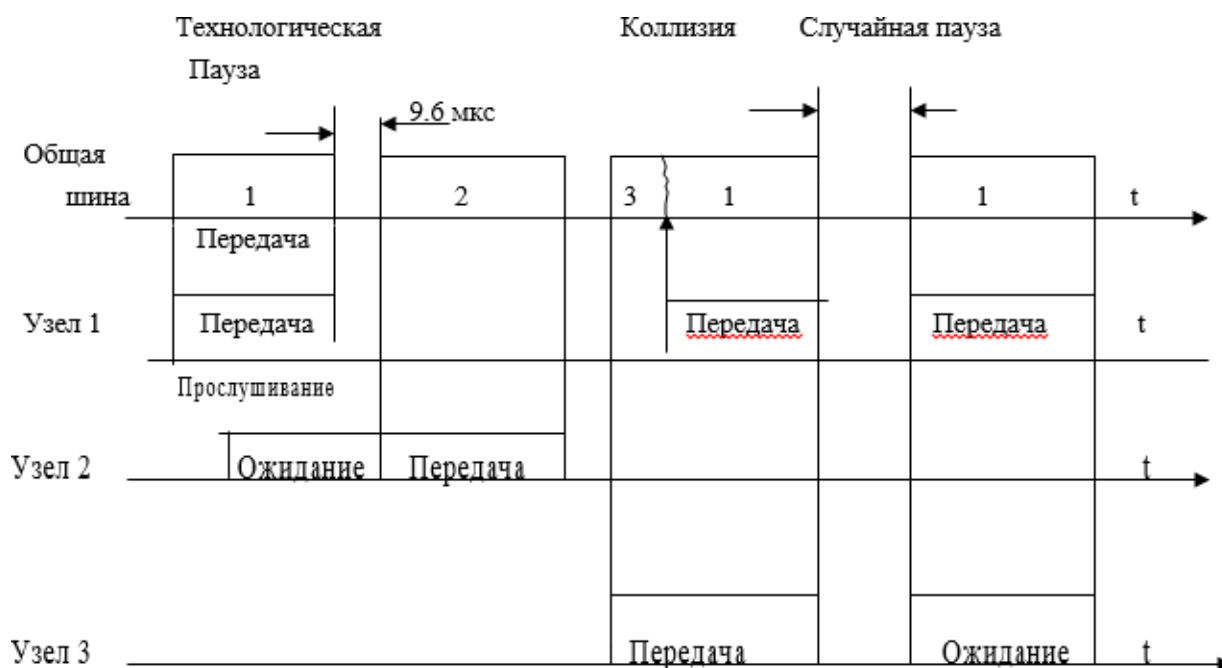
1. Construction local computing networks With using common bus topology.
2. Construction With local computing networks using topology star.
3. Removal statistical characteristics, received projects local computing networks And their study.

Theoretical Part

Method random CSMA/CD access

IN Ethernet networks use the access method by Wednesday data transfer, called carrier sense multiple access with collision detection (CSMA/CD).

This method is used exclusively in networks with a logical common bus (to which relate And radio networks, gave birth to this method). All computers such networks have direct access to the common bus, That's why she Maybe be used to transmit data between any two network nodes. All computers on the network have the ability to do so simultaneously. immediately (With taking into account delays distribution signal By physical environment) to receive data, which any from computers started transmit on general tire (rice. 3) Simplicity schemes connections - This one from factors, determined success standard Ethernet . They say, What cable, To to whom connected All stations, works V mode collective access.



Stages access To environment

All data, transmitted By networks, fit V frames certain structures and are supplied with a unique destination station address.

To be able to transmit a frame, a station must ensure that the shared Wednesday free. This achieved listening basic harmonics signal, which is also called the carrier frequency. A sign that the medium is unoccupied is the absence on her load-bearing frequencies, which at Manchester method coding equals 5-10 MHz, depending on the sequence of ones and zeros being transmitted at the moment.

If Wednesday free, That knot has right begin transmission frame. This frame is shown in Fig. 3 first. Node 1 has detected that the medium is clear and has begun transmitting its frame. In a classic Ethernet network on a coaxial cable, the signals from node 1's transmitter propagate in both directions, so that all nodes in the network receive them. The data frame is always accompanied by *preamble*, which consists of out of 7 A byte consisting of the values 10101010 and an 8th byte equal to 10101011 (the initial frame delimiter). The preamble is needed to ensure that the receiver is in bit- and byte-synchronized with the transmitter.

All stations connected to the cable can recognize the fact that a frame has been transmitted, and the station, which finds out own address V headlines frame, writes down his content in your own 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 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 2 is forced to wait until node 1 stops transmitting the frame.

After endings transmissions frame All nodes networks obliged endure a technological pause of 9.6 μ s. This pause, called the interframe interval, is needed to reset the network adapters to their initial state and also to prevent exclusive capture Wednesday one station. After endings technological pauses nodes have the right to begin transmitting its frame, since the medium is clear. Due to signal propagation delays By not all nodes on the cable simultaneously record the fact that the node has finished transmitting the frame 1 .

IN given example node 2 waited endings transmissions frame node 1, paused in 9.6 μ s and started the transmission your frame.

Origin collisions

the described approach, a situation is possible when two stations simultaneously try hand over frame data By general environment. Mechanism auditions Wednesday And pause between frames does not guarantee that a situation will not arise when two or more stations are simultaneously decide, What Wednesday free, And they are starting transmit their frames. This is called a **collision**, as the contents of both frames collide on the shared cable, causing information distortion. methods coding, used in Ethernet , no allow highlight signals each stations from general signal.

Collision - This normal situation V work networks E thernet . IN example, In the figure shown in Fig. 3, the collision was caused by the simultaneous transmission of data by nodes 3 and 1. For a collision to occur, it is not necessary for several stations to begin transmitting at exactly the same time; such a situation is unlikely. It is much more likely that the collision occurs due to that one node starts transmitting earlier another, but to the second node signals first Just Not they have time get there To to that time, When second knot decides start the transmission of your frame. That there are collisions - This investigation distributed character networks.

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

collisions all stations networks, station, which detected a collision, interrupts the transmission of its frame (at an arbitrary point, possibly not on a byte boundary) and intensifies the collision situation by sending a special 32-bit sequence, called **a jam sequence, into the network**.

After this, the transmitting station that detects a collision is required to cease transmission and pause for a short, random interval. It may then attempt to acquire the medium and transmit a frame again. The random pause is selected according to the following algorithm:

$\text{Pause} = L * (\text{delay interval}),$

where the backoff interval is equal to 512 bit intervals (in Ethernet technology it is accepted All intervals measure V bit intervals; bit interval is designated How t and corresponds time between appearance two sequential bit data on cable; for a speed of 10 Mbit/s, the bit interval is 0.1 μ s or 100 ns);

L is an integer chosen with equal probability from the range $[0, 2^N]$, where N is the number of retransmission attempts for a given 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 consecutive attempts to transmit a frame result in a collision, the transmitter must stop trying and discard the frame.

From the description of the access method, it is clear that it is probabilistic in nature, and the probability of successfully accessing a shared medium depends on the network load, that is, on the intensity of frame transmission needs at the stations. When this method was developed in the late 1970s, it was assumed that a data transfer rate of 10 Mbps was very high compared to computer needs. in mutual exchange data, That's why loading networks will Always small. This assumption remains sometimes true to this day, but applications have already appeared that work in real time with multimedia information, which Very are loading segments Ethernet . At this collisions arise much more often. With significant intensity collisions useful pass ability networks Ethernet falls sharply , because the network is almost constantly busy with repeated attempts to transmit frames. To reduce the intensity of collisions, you need to either reduce traffic by cutting down, For example, number of nodes V segment or replacing applications, or increase speed protocol, For example, go to on Fast Ethernet . It follows note, What method CSMA/CD access does not guarantee that a station will ever be able to access the medium. With a light network load, the probability of such an event is low, but with a coefficient network usage approaching 1, such an event becomes very likely. This disadvantage of the random access method is the price to pay for its extreme simplicity, which did technology Ethernet the most inexpensive. Other methods access - token access networks Token Ring And FDDI, method Demand Priority networks 100VG-AnyLAN free from this shortage.

Time double turnover And recognition collisions

Clear recognition of collisions by all network stations is a prerequisite correct operation of the Ethernet network . If any transmitting station does not recognize the collision and decides that it has transmitted the data frame correctly, then this data frame will be lost. Due to overlays signals at collisions information frame will be distorted, And He will rejected by the host station (Maybe, because of discrepancies control amounts). Quicker in total, the distorted information will be repeated transferred any protocol top level, for example, transport or application, working with connection establishment. But repeated broadcast messages protocols top levels will happen through significantly more long interval time (Sometimes even through some seconds) By comparison with microseconds intervals, which operates protocol Ethernet . That's why If collisions

Not will be reliable be recognized knots networks Ethernet , That This will come To noticeable reduction in the useful bandwidth of this network.

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

Where $T_{\min}$ — the transmission time of a frame of minimum length, and PDU, is the time during which the signal collisions manages to spread to himself distant node networks. So How V In the worst case, the signal must travel twice between the most distant stations in the network (an undistorted signal travels in one direction, and a signal distorted by a collision travels back), this time is called the double-turnaround time.

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

It is obvious that the fulfillment of this condition depends, on the one hand, on the length of the minimum frame And pass capabilities networks, A With another sides, from lengths network cable system and the speed of signal propagation in the cable (this speed is slightly different for different types of cable).

All parameters protocol Ethernet selected like this in this way, to at During normal operation of network nodes, collisions are always clearly identified. When selecting parameters, the above relationship between the minimum frame length and the maximum distance between stations in a network segment is also taken into account.

Ethernet standard **specifies that the minimum length of the frame data field is 46 bytes** (which, together with the service fields, gives a minimum frame length of 64 bytes, and together with the preamble, 72 bytes or 576 bits). This can be used to determine the distance limit between stations.

In 10-megabit Ethernet, the transmission time for a minimum frame length is 575 bit intervals, meaning the round-trip 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 the signal must travel along the line twice during this time, the distance between two nodes should not be be more 6 635 m. IN standard magnitude this distances chosen significantly less, taking into account other, more stringent restrictions.

One of these limitations is related to the maximum permissible signal attenuation. To ensure the required signal strength when passing between the most distant stations in a cable segment, the maximum length continuous segment of thick coaxial cable, taking into account the noise it introduces attenuation, selected at 500 m. On a 500 m cable, the collision detection conditions will be met with a large margin for frames of any standard length, including 72 bytes (round trip time By cable 500 m makes up total 43.3 bit interval). That's why The minimum frame length could have been set even shorter. However, the technology's developers chose not to reduce the minimum frame length, keeping in mind multi-segment networks built from several segments connected by repeaters.

Repeaters increase power transmitted With segment on segment signals, in result attenuation signals decreases And Can use net much longer, consisting of several segments. In coaxial Ethernet implementations , developers limited the maximum number of segments in the network to five, which in turn limits the total network length to 2,500 meters. Even in such a multi-segment network, the collision detection condition is still met with a large margin (compare the distance of 2,500 m obtained from the permissible attenuation condition with the maximum possible distance of 6,635 m calculated above based on the signal propagation time). However, in reality, the time margin is significantly smaller, since in multi-segment networks the repeaters themselves introduce into the propagation

signal an additional delay of several tens of bit intervals. A small reserve was also made to compensate for deviations in cable and repeater parameters.

By taking all these and other factors into account, a carefully chosen ratio was established between the minimum frame length and the maximum possible distance between network stations, ensuring reliable collision detection. This distance is also known as the maximum network diameter.

With the increase in frame transmission speed, which occurs in new standards, the maximum distance between network stations decreases proportionally to the increase in transmission speed. In the Fast standard Ethernet it is about 210 m, in the Gigabit standard Ethernet would have been limited to 25 meters if the developers of the standard had not taken some measures to increase the minimum packet size.

Table 1 shows the values of the main parameters of the frame transmission procedure of the standard 802.3, which do not depend from implementation physical environment. Important note, that each variant of the physical medium of Ethernet technology adds to these limitations its own, often more stringent, limitations that must also be met.

Table 1. Parameters level MAC Ethernet

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

Methodology And order execution Work

Methodology

1. Construction local computing networks With using topology common bus.

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 item New.
3. IN device browser find paragraph « GenericLANs ».

4. Move required devices V working region, following following instructions:
 - a. Select Thin Ethernet Segment in the image subwindow and move it to the working area.
 - b. Change dimensions images devices V working areas By at your discretion.
 - c. Enlarge size font signatures To device, having chosen from context menu item "Properties".
 5. Add four workers stations in window work area.
 - a. Find paragraph LAN workstations », then Workstations And select folder Generic Devices».
 - c. Pull out Ethernet Workstation.
- You'll get the following (Figure 2.1):

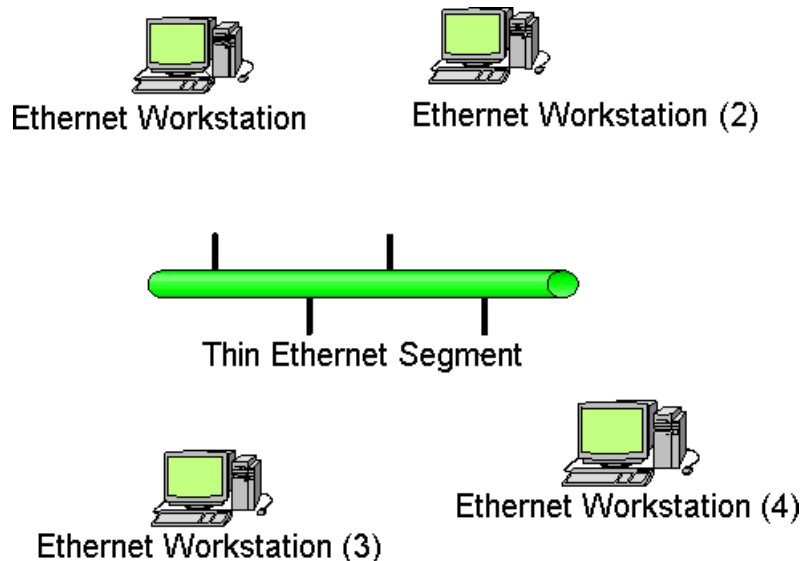
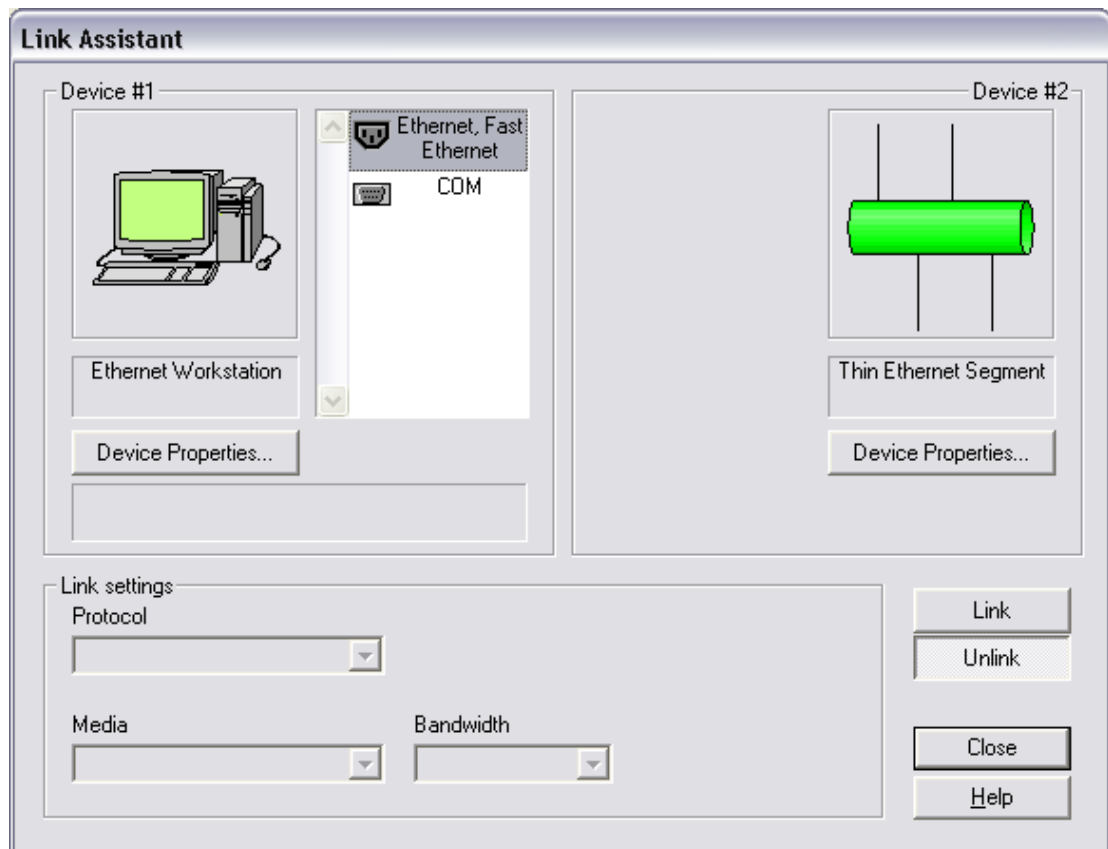


Figure 2.1 – External appearance of workstations

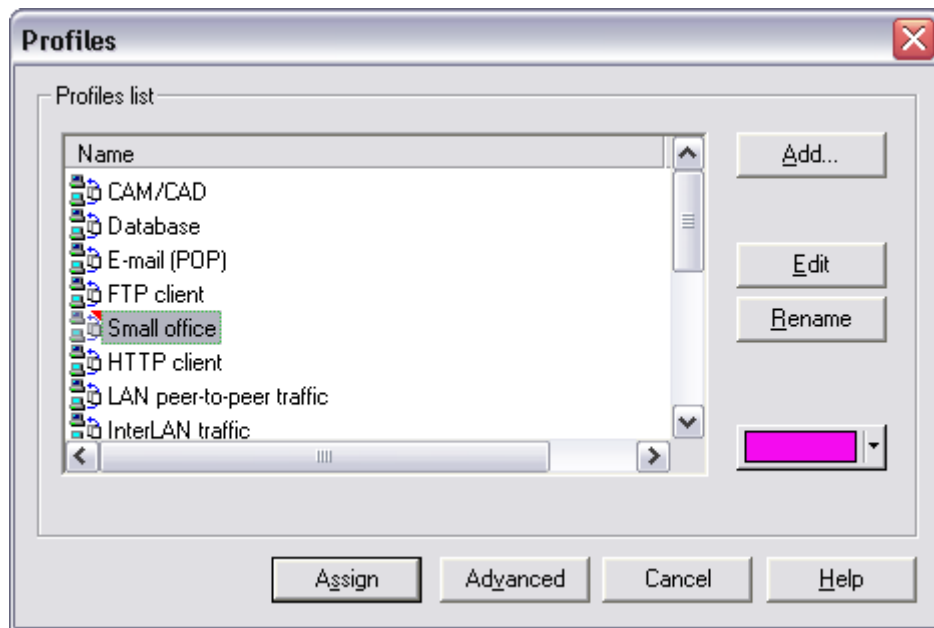
Method definitions compatible devices:

1. Click mouse on the device.
 2. Select the Find Compatible option (Find Compatible) from the Objects menu .
 7. Compound tires And workstations .
 - a. IN panels modes click button .
 - b. Left click on Ethernet first Workstation , and then on Thin Ethernet Segment .
- The following dialog will appear (Figure 2.2):



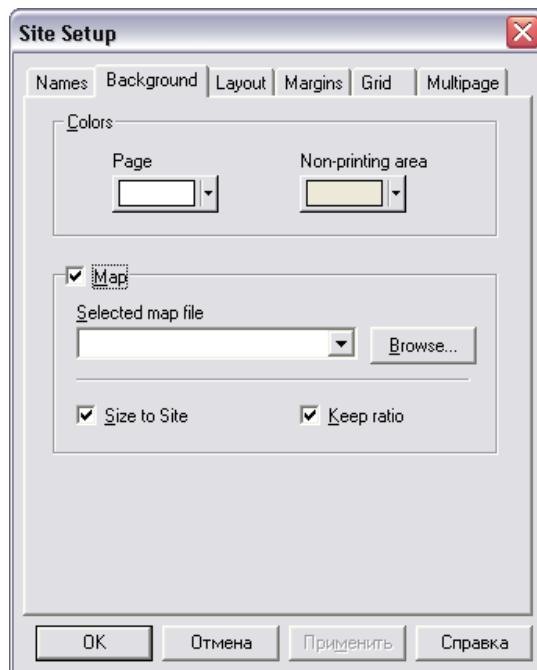
Drawing 2.2 - External view panels Link Assistant

- c. Click buttons " Link ", then " Close ", to install connection And close wind
 - ow. d. For fast installations connections hold on key Shift, click mouse on 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 Ethernet Workstation
- (4). The following dialog will appear (Figure 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 on Ethernet first Workstation (4), and then to Ethernet Workstation .
 - f. Repeat steps 9b-e For Ethernet Workstation (2) And Ethernet Workstation (3).
 10. To test the functionality of the created network project, click the "Start" button on the control panel. Packets will flow between workstations through the segment .
 11. Regulation intensity interactions informational exchange.
 - a. Click button Animation Setup »  , And V appeared In the dialog, move the slider " Packet" intensity ».
 - b. Click button OK. Through some seconds intensity traffic must change.
 12. Change speed movements packages.
 - a. Click button Animation Setup »  , And V appeared In the dialog, move the slider " Packet" speed ».
 - b. Click the OK button. After a few seconds, the packet speed should change.
 13. Change sizes images packages.
 - a. Click button Animation Setup »  , And V appeared In the dialog, move the slider " Packet" size ».
 - b. Click button OK. Size images packages must change.
 14. Take a look on used You devices And select bookmark Recently used » - "Used" in the window sill images.
 15. Location cards How background worker windows.
 - a. From contextual menu worker windows select « Site Setup » - "Settings window
 - ws." b. On bookmark Background put tick " Map ". Use the " Browse " button to select the map file.
- To understand, O how speech, take a look on this one panel (drawing 2.4):



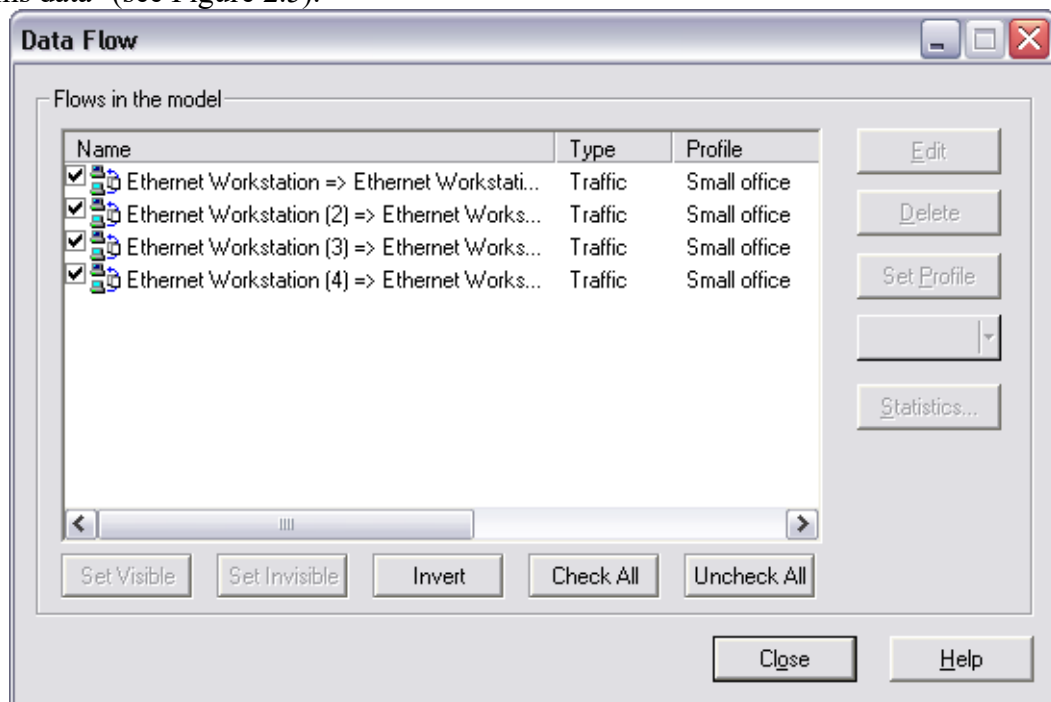
Drawing 2.4 - External view panels Site Setup

16. Coloring background. From contextual menu worker windows select « Site Setup » - "Settings windows."

- a. On bookmark Background take off tick " Map ".
- b. IN list "Page" select color to taste.
- c. IN Non- printing list select another color.
- d. Click OK.

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

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



Drawing 2.5 - External view panels Data Flow

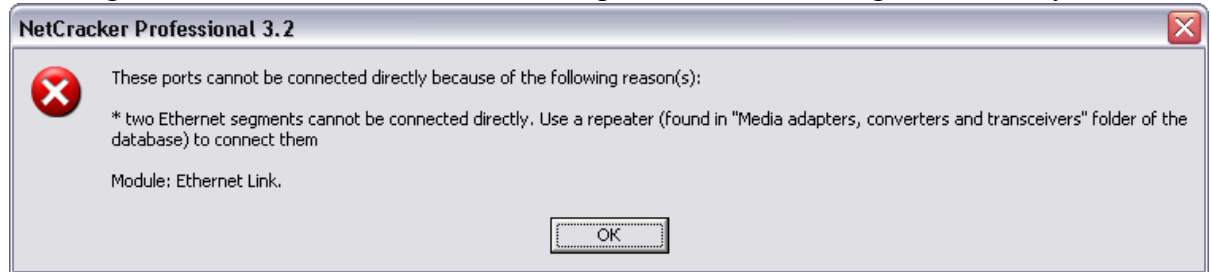
IN appeared dialogue will be displayed profiles already selected You types traffic.

18. expansion .

a. Add another Thin segment to the working window Ethernet Segment and a few other Ethernet workstations Workstation . Connect them to the network by repeating steps 9b-e for the new workstations.

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

Drawing 2.6 - External view windows at attempt connections two segments directly for



connections of two segments in one net to you must be placed between them adapter.

c. Select standard cursor button Standard V mode panels .

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

e. IN under the window images select Ethernet Media Converter », move to a free space in the working 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.

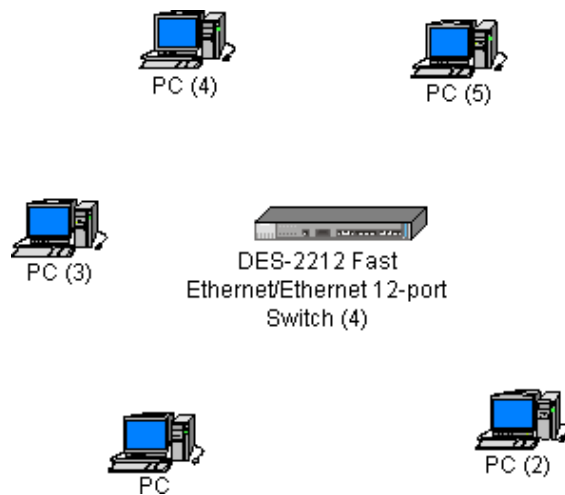
a) Move to the working area DES-2212 Fast Ethernet / Ethernet 12-port Switch by selecting it in the images subwindow.

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 using Fast Ethernet adapters.

3) Add some workstations V window work area.

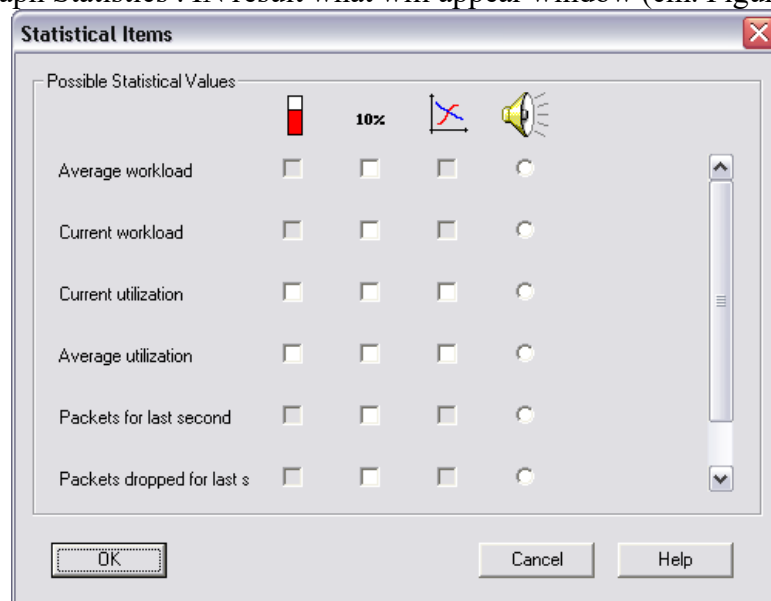
a. Find the "LAN workstations " item, then " PCs " and select the " Generic" folder. Devices ».

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



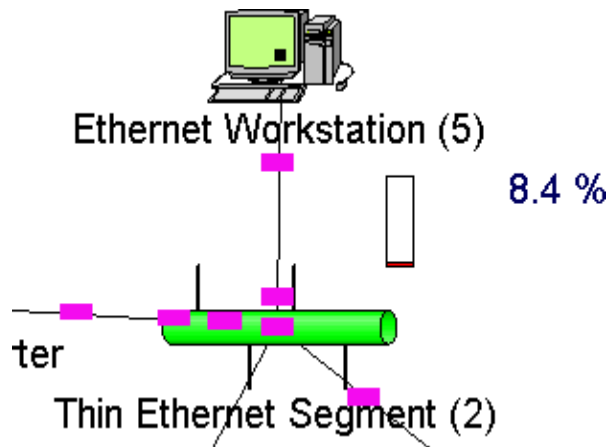
Drawing 2.7 - External view workstations

- 4) Add network adapters V workstations .
 - a. Collect paragraph LAN workstation ».
 - b. Find LAN adapters», Ethernet, « Generic Devices».
 - c. Add By alone Ethernet adapter V workers stations PC, PC(2), PC(3). AND one by one Fast Ethernet adapter in PC(4), PC(5).
 - d. Create compound between switch And stations. At When connecting, pay attention to the compatibility between different ports and network cards.
 - e. Assign traffic between workers stations How This was described in question 1, item 9.
 - 5) Add V working region more alone switch. Choose DES-5024 Fast Ethernet/Ethernet 24-port Modular Switch from "Switches", Workgroup, Ethernet, D-Link Systems.
 - a) Transfer a few more workstations, add adapters to them and assign traffic by repeating steps 3 and 4.
- Received net will have topology star consisting from two segments.
3. Removal of statistical characteristics of the obtained local area network projects and their study.
 - a. Right-click on any of the connection lines and in the context menu menu select paragraph Statistics . IN result what will appear window (cm. Figure 2.8)



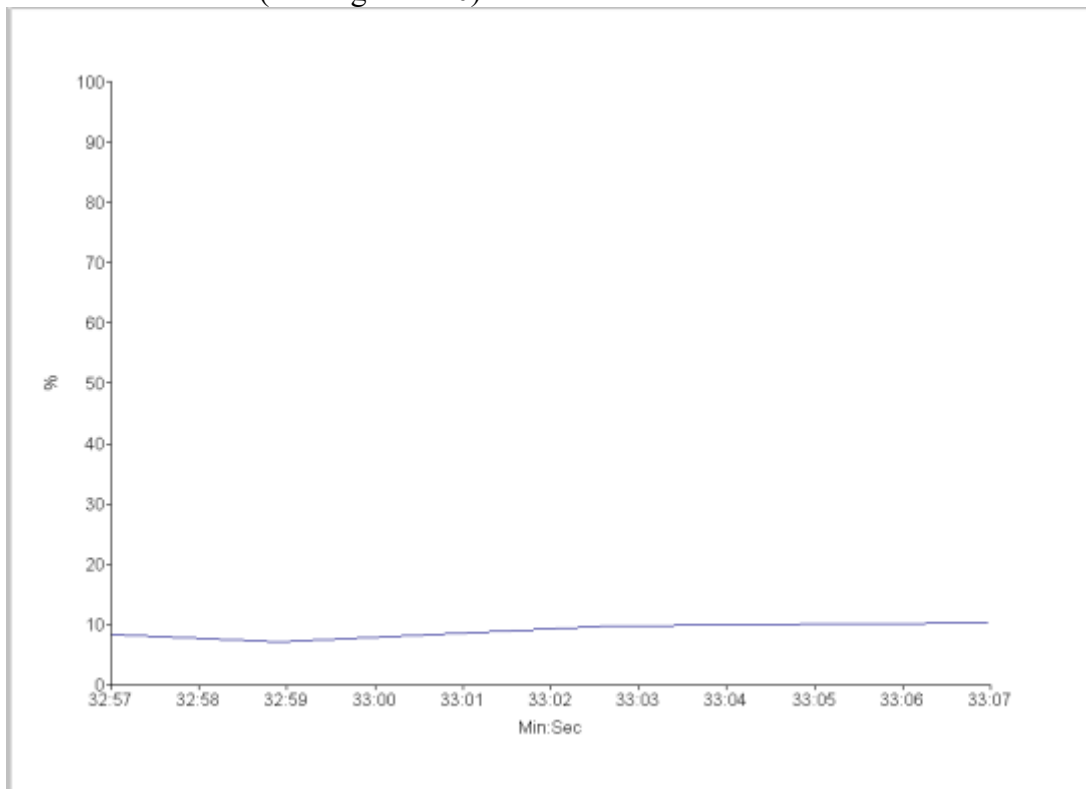
Drawing 2.8 - External view statistics windows

- b. Put it check marks, For example, against Current utilization V first column and opposite Average utilization in the 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, what will happen. IN NetCracker Also Maybe creating graphs.
- a. Right mouse click
click on any from lines connections And V contextual menu select Statistics item .
- b. Put it tick, For example, against Average utilization V third column. Click OK.
- c. On screen schedule reflecting
work selected lines (cm. Figure 2.10).



Drawing 2.10 - Statistics graph

- a. From menu File select team Save.
- b. By default Name file will Net1.net. You you can change his on Whatever you deem necessary. The .NET extension will be added automatically.

- c. Close project, preliminary stopping him.
- d. Build single-level network project according to Yours option tasks, guided by the rules set out above.

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 of work:

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

Control questions:

- 1. IN what kind topological structures is used method access To environment CSMA/CD data transmission?
- 2. Name it stages access method CSMA/CD To environment transmissions data.
- 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 lesson 9

Study communication equipment Switch 2960 Purpose and

content:

Target

Learn the basic principles of configuring Switch 2960 communications equipment .

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. Configuration ports

Theoretical justification:

A switch is a network device that filters, distributes, and creates a frame stream based on the analysis of the recipient's address. It operates at the data link layer of the OSI model.

Methodology And order execution of work:

Methodology

Registration on Switch

When you log in to a Switch 2960 device, you see an interpreter prompt. Exec V user mode, appears information about the device and control 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 – This item allows you to select step-by-step configuration . Selecting the [M] key displays an additional 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 look at the second item of the control menu, "Command Line." It allows you to configure the device using control commands. list which it's not difficult get. For beginning necessary choose key [K] After the operation is completed, the Exec interpreter prompt will appear indicating that you are in 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, perform the following operation:
>?

Exec commands : Transcript each from teams presented V table 2.1.

Table 2.1 - Teams user mode

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

At this stage, it is possible to perform operations that are not of a global scale, as characterized by Table 2.1.

For Togo to produce global configuration necessary execute the command " enable " and enter privileged mode (privileged) mode).

>

enable

#

Just like in user mode, to get a list of valid commands and any help information, you need to enter "?".

#?

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 Switch command #SH
CLOCK

11:35:49.985 word ?? ??? 20 2011

Installation passwords

For installations passwords on manager console And entrance V privileged the regime must be carried out as follows:

#config t

Enter configuration commands, one per line. End with CNTL/Z.

(config)#enable password level 1 km1p

(config)#enable password level 15 mk1p

(config)#^Z

%SYS-5-CONFIG_I: Configured from console by console

#

For installations password permitted secret necessary execute next commands: (config)# enable secret mk1p9

(config)#^Z

%SYS-5-CONFIG_I: Configured from console by console

#disable

> en

Enter password :*

**** #

Change name V device Switch 2960

For changes name devices are required execute V 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 device are saved automatically.

Installation IP addresses

For IP address settings And gateway V mode configurations we are performing the following 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 show running-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\$H7PDx17VYMqaD3id4jJVK/

!

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

To configure ports, execute the following commands. In configuration mode, enter the command " interface " , followed by the interface name and number .

```
#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 0/1
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 its defaults
port Perform switch port configuration
shutdown Shutdown the selected interface
spanntree 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 its defaults
port Perform switch port configuration
shutdown Shutdown the selected interface
spanntree Spanning tree subsystem
vlan -membership VLAN membership
configuration My_switch (config- if)#
```

Configuration descriptions interfaces

When installing descriptions, you need to set the installation to configuration mode, select the port and run the " description " command and the description itself.

```

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_vlan
My_switch(config-if)#int f0/26
My_switch(config-if)#description trunk_to_Building_4
My_switch(config-if)#
    Information about interface Can get With help next command.
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 100000 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!
!
interface Ethernet 0/1
description 'finance_vlan'
!
interface FastEthernet 0/26
description 'trunk_to_Building_4'
!
interface FastEthernet 0/27
line console
end

```

Применение команды «duplex»

For configurations duplex applies duplex command .

```

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

```

Table 2.2 - Parameters teams 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 of work:

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

Tasks

First it is necessary clear all information from Switch And execute the operations listed below .

Set the IP address and gateway for the device, change the Switch name , enable console passwords, enable privileged mode, and enable secrets. Set Ethernet ports 0/1, 0/2 , and 0/3 to half-duplex mode, and FastEthernet. 0/26 V full-duplex mode, FastEthernet 0/27 V full-duplex mode on

100 Mbps, and all other Ethernet ports in automatic mode. Check the implementation established parameters. View information O Switch . Browse through all the device menu sub-items.

Once you are sure that all actions have been completed correctly, you need to call the teacher and present the completed assignment for review.

Content report And his form:

The report should be formatted according to the format of a simple abstract. The title page should include: the course title, the lab title, the last name and initials of the submitting student, the group number, and the last name and initials of the receiving instructor. The main body of the lab should contain:

a) answers to the control questions proposed in the laboratory work; b) detailed consideration proposed examples laboratory work c) description of each stage of the task;

G) conclusions By work done .

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

Control questions And protection Works: Test

questions.

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

Protection work

Protection the 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; in answers to additional questions

Practical lesson #2. Introduction V inter-network Cisco's IOS operating system.

Theoretical Part

At first at the entrance V network device user sees command line user mode view:

```
Switch >
```

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

To access the full set of commands, you must first activate privileged mode.

Press ENTER to start.

```
Switch>
```

```
Switch> enable
```

```
Switch#
```

```
Switch# disable
```

```
Switch>
```

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

The transition to this mode will be indicated by the appearance in the command line prompt in the form of the # **sign**. From the privileged level you can get information about system settings and access the global configuration mode And others special modes configuration, including interface, subinterface , line, network device, route map, etc. configuration modes. To exit the IOS system, type the exit command on the keyboard .

```
Switch> exit
```

Regardless of how the network device is accessed: through the console of a terminal program connected via a null modem to the COM port of the network device, or V framework session protocol Telnet , device Can translate in one from modes. We are interested in the following modes.

Custom mode — This mode viewing, V which user Maybe only browse certain information O network device, but not Maybe Nothing change. IN this mode invitation has view type Switch >.

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

Global Configuration Mode - Implements powerful one-liners teams, which decide tasks configuration. IN this mode the invitation has view type Switch (config) # .

IOS recognizes commands in any mode by the first unique characters. When pressed tabulations IOS itself will complement the team to the full name.

When entering any mode in the command line the command name and a question mark (?) Comments about the command are displayed on the screen. Entering a single character will result in a list of all commands in the mode. Multiple screens of lines may be displayed on the screen, so a hint (More) will sometimes appear at the bottom of the screen. To continue, press Enter or Space.

Global configuration mode commands define the overall behavior of the system. Additionally, global configuration mode commands include commands for switching to other configuration modes, which are used to create configurations that require multi-line commands. To enter global configuration mode, use the privileged mode command `configure` . When entering this command, specify the source of the configuration commands: `terminal` , `memory` (non-volatile memory or file), `network` (server tftp (Trivial ftp - simplified ftp (online)). By default, commands are entered from the console terminal. For example

```
Switch# configure terminal
Switch(config)#(commands)
Switch(config)# exit
Switch#
```

Commands for activating a specific type of configuration must be preceded by global configuration commands. Thus, to configure an interface, the possibility of which is indicated by the Switch (config -if)# prompt, a global command is first entered to determine the interface type and its port numbers:

```
Switch# conf t
Switch(config)# interface type port
Switch( config -if)# (commands)
Switch( config-if)# exit
Switch(config)# exit
```

For restrictions access To system are used passwords. 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 via Telnet protocol:

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

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

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

Team **enable password** limits access To privileged regime :

Switch#conf t

Switch(config)# enable password пароль

Далее

Ctrl-Z

Switch#ex

...

Press RETURN to get started

Switch>en

Password: **пароль**

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

Command no shut (abbreviation no shutdown) is used to keep an interface active (without this command, the interface could be temporarily disabled). The opposite command, shut , will disable the interface.

It is important to be able to monitor the correct functioning and condition of a network device at any time. moment in time. The following commands are used for this:

Team	Description
show version	Displays information about the system hardware configuration, version software, 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 to exchange basic configuration information. CDP will work without any protocol configuration. By default, CDP included on everyone interfaces. CDP works on second (channel)

level models OSI. That's why CDP Not is routable protocol And works only with directly connected devices. The CDP protocol binds the physical Wednesday transmissions data more low level With protocols higher network layer. Therefore, devices supporting different Layer 3 protocols can recognize each other.

When starting the device The CDP protocol starts automatically. After this, it can automatically detect neighboring devices that are also running the CDP protocol. Among the discovered devices there will be not only those who work with the protocol IP.

CDP allows administrators to access data about another network device to which they have a direct connection.

For conclusion information O neighboring devices, discovered By CDP protocol, the **show command family is used cdp** . It displays the following data for each port and each device connected to it: Device IDs, Address List, Port ID, Feature List, Hardware device platform.

Teams ping And traceroute

For diagnostics possibilities establishments connections V networks Request-response or echo packet protocols are used. The results of such protocols can help assess the reliability of the path to another device, as well as the overall delay values and those between intermediate devices. In order for this to happen team worked, necessary, to Not only local network device knew how to get to the destination, but also for the device at the destination to know how to get to the source.

ping command sends ICMP(Internet Control Message Protocol) echo packets for verification connection. In the example below, the transit time of one echo packet exceeded the specified one, as indicated by the dot (.) in the output, and four packets were successful, as indicated by the exclamation mark (!).

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 destination 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

tracert command shows the addresses of intermediate interfaces (hops) along the packet path. to the destination.

Switch > **tracert 172.16.101.1**

The extended version of the ping command is only supported in privileged mode. To enter extended mode, enter Extended in the prompt. commands enter letter "y" (Yes)

Team V mode dialogue interrogates values parameters. Important It should be noted that this command allows you to check the connection between network devices while on one device. 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]:

Команда telnet

telnet virtual terminal protocol , part of the TCP/IP protocols, allows you to establish a connection between telnet network device client And telnet network device server, which allows for operation in virtual terminal mode. Telnet is used for remote management of a network device or to check the connection at the application level. A successful Telnet connection allows you to control the remote device as if you were sitting at its console. Network devices Cisco devices are capable of supporting up to five simultaneous Telnet incoming sessions .

Practical Part

With connection With network Cisco device

Create in Packet Tracer the topology shown in the figure using the default router model, Generic . Name the devices as you see in Figure 1: Router1, Router2, and Router4.

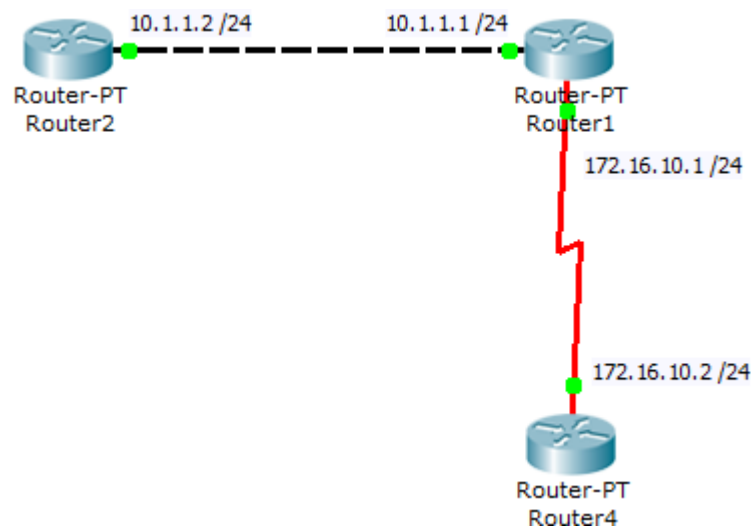


Fig. 1

The black line indicates an Ethernet connection. The red line indicates a serial connection. To create a serial connection, select point-to-point serial connection (serial cable). Select the second device. We determine which router will act as the DCE device. This device sets the clock. In the simulator, we'll need to determine its clock frequency.

Save topology.

Introduction With network device Cisco.

1. For choice network Router1 devices click in work area programs Click on the image of the desired device. The network device settings window will open. Here, select the CLI tab to manage the device.

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

see Continue with configuration dialog ? [yes / no]:

Enter: " no " And click key <Enter> You will

see

Router >

You are now connected to network device and you are in command line mode user . Here " Router " - This Name Network devices, A ">" means, What You are in user mode.

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

Router #

4. To return in mode user, Just print disable . From user mode введите logout or exit to leave the 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. Enter the command used to view all available commands:

```
Router > ?
```

Key Enter press No need.

3. Now log in V privileged Router mode > enable

```
Router #
```

4. Browse list available teams V privileged Router # mode ?

5. Let's move on V mode

configurations Router#config terminal

```
Router(config)#
```

6. *The hostname* of a network device is used for local identification. When you log into a network device, you see *The hostname* before the mode symbol (">" or "#"). This name can be used to identify the location. Set "Router1" as the name of your network device.

```
Router(config)# hostname Router1
```

```
Router1(config)#
```

7. The access password allows you to control access to privileged mode. This is a very important password because in privileged mode You can make configuration changes in this mode. Set the access password to " password ."

```
Router1( config ) #enable password password
```

8. Let's test this password. Log out of the network device and try logging into the privileged account. mode.

```
Router 1> en Password
```

```
:***** Router1#
```

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

Main Show commands.

Enter user mode with the disable command. Enter the show command to view all available commands.

Router 1> **show ?**

1. The show command version is used to get the network device platform type, operating system version, operating system image file name, system uptime, memory size, number of interfaces, and configuration register.

2. Can see Router 1 clock

> **show clock**

3. In The Cisco IOS operating system image file is stored in the network device's flash memory. Unlike RAM, flash memory in real devices retains the image file even during a power failure.

Router 1> **show flash**

4. commands by default.

Router 1> **show history**

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

6. Two commands will allow you to move to the next command saved in the buffer. Press the down arrow or < ctrl > N

7. Can see list hosts And IP Addresses everyone their Router 1
interfaces> **show hosts**

8. Next team will lead out detailed information O each interface Route1 r> **show interfaces**

9. Router 1> **show command sessions**

will lead out information O each telnet sessions.

10. Router 1> **show command terminal**

shows configuration parameters terminal.

11. Can see list everyone users connected To device along terminal lines

Router 1> **show users**

12. Router 1> **show command controllers**

shows state controllers interfaces.

13. Let's move on V privileged mode. Router
1> **en**

14. Enter team For viewing everyone available show commands.

Router1# **show ?**

Privileged mode includes V myself All show teams user

regime And a number of new ones.

15. Let's look at the active configuration in the network device's memory. Privileged mode is required. The active configuration is automatically **is not** saved and will be lost in the event of a power failure.

Router1# **show running- config**

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

16. The following command will allow you to see the current state of layer 3 protocols.

Router# **show protocols**

Introduction V configuration interfaces.

We'll try understand, How include (to lift) interfaces network devices and what is needed to put the interface into the UP state.

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

configurations# **conf t**

Router 1(config)#

2. Now we we want tune Ethernet interface. For this We should come in into interface configuration mode.

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

Router 1(config - if)#

3. Let's see All accessible V this mode Router 1

commands(config -if)# ?

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

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

We used abbreviated Name interface.

4. For each command, we can perform the opposite command by preceding it with the word **no** . So the command

Router 1(config -if)# **no shutdown**

includes this interface.

5. Let's add To interface description

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

To see description this interface, go V privileged mode and run the command show interface .

Router 1(config -if)#

end Router1#show

interface

6. Now join us To network **Router** device **2** And change Name his host on **Router2**

Router# **conf t**

Router(config)# **hostname Router2**

Let's go in on interface FastEthernet 0.

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

Router 2(config -if)# **no shutdown**

Now that the interfaces at both ends of our Ethernet connection are enabled, a message will appear on the screen indicating that the interface status has changed to active.

7. Let's move on to configuring the serial interfaces. Let's go to Router1. Let's check which device Our router acts as a serial line end device (DTE) terminal equipment) or communication device DCE (data circuit)

Router1# **show controllers S2/0**

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

Router1#conf t

Router1(config)#int s2/0 Router

1(config -if)#clock rate ? Let's choose frequency 64000

Router 1(config -if)#clock rate 64000 and we raise interface

Router 1(config -if)#no shut

8. Let's move on To router4 And we'll give of the same name Name. Let's raise it on it has a serial2/0 interface.

Now, When interfaces on two ends ours sequential connections are enabled, a message will appear on the screen about changing the interface status to active.

9. Let's check on each device, What configured us interfaces are in UP state.

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 all interfaces on which CDP operates.

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've verified that a network device is sending and receiving CDP updates, we can use CDP to obtain information about directly connected devices. Enter the command

```
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 did everything correctly. We see that our router, router1, is connected to the interface. Fas 0/0 (**Port ID**) of router (**Capability**) router2 (**Device ID**) of 1000 series (**Platform**) via interface Fas 0/0 (**Local**) **Intrfce**) and with the router's Ser 2/0 interface router4 1000 series via Ser 2/0 interface .

3. On router1, enter team For more detailed information O neighbors router1#

```
show cdp neighbors detail
```

This command displays one device at a time. It's used to display network layer address information. Currently, this layer isn't configured, so the Entry field address (es) is empty. The command also displays the IOS version information.

10. On router1, enter team, to to know information about device " router4 " router1# **show cdp entry Router4**

This command gives the same information as show cdp neighbor detail , but for one specific device. Remember that hostnames are case-sensitive.

11. On device router1 enter team, to see, How often router1 sends CDP updates to neighbors and how long neighbors should keep them.

```
router1#show cdp
```

```

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

```

To save bandwidth on low-speed devices, CDP can be disabled .

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

And again turn on For total router1

```
devices ( config )# cdp run
```

12. Sometimes it is necessary to disable CDP for a specific interface, for example, if its bandwidth is low or for security reasons. On router1, disable CDP on interface FastEthernet 0/0.

```

router1 (config)# interface fa0/0
router1 ( config -if)# no cdp enable
router1 (config)# Ctrl-Z router1#
show cdp interface

```

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

Setting up IP interface addresses

1. Let's connect To device **Router1** And let's install IP address Ethernet interface

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

```
Router 1( config -if)# ip address 10.1.1.1 255.255.255.0
```

2. Now we will assign the IP address 172.16.10.1 255.255.255.0 to the S0/0 interface without leaving the interface configuration

```
Router 1( config -if)# in s0
```

```
Router 1( config -if)# ip ad 172.16.10.1 255.255.255.0
```

Note that a point-to-point serial connection always allocates an entire subnet.

3. Let's switch to device **Router2** and assign the FastEthernet 0/0 interface the IP address 10.1.1.2 255.255.255.0

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

```
Router 2( 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 Serial 2/0 interface .

```
Router 4( config -if)# ip address 172.16.10.2 255.255.255.0
```

5. On each look at the device yours active configuration and make sure that assigned IP addresses appeared there.

```

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

```

6. View detailed IP information for each interface and ensure that the configured interfaces are in the UP state.

```

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

```

7. Brief information Can get team show IP interface brief, 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 the device **Router1**. You should be able to successfully ping the directly connected FastEthernet 0/0 interface on 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 Router4 Router1# **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. Back on Router2, you should be able to successfully ping the 10.1.1.1 address of the directly connected FastEthernet 0/0 interface on Router1. Back on Router4, you should be able to successfully ping the 172.16.10.1 address of the directly connected interface. Serial 2/0 on Router1. Let's try to ping the FastEthernet 0/0 interface on the Router1 device.

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 on the Router2 device. Failed.

10. Let's come back on Router2. Let's try ping address 172.16.10.1 interface

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

We encountered failures because we did not configure routing on the routers.

11. Come in on Router1 device . Determine paths passages packages on Router2

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 172.16.10.2 Router1#

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 telnet support .

1. Log in to Router1. We need this network device to accept Telnet sessions and be password protected. Each so-called line in a network device potentially represents an active telnet session that the device Maybe support. Our network devices support to 5 lines assigned to virtual terminals vty . We use all 5 lines

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

Router 1(config - line)#

2. Now we will inform you network device, What us will be needed password entrance into the system.

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

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

3. Log in on device Router2 And let's install telnet connection With Router1. For this, we use the IP address of its FastEthernet 0/0 interface.

Router2# **telnet 10.1.1.1**

4. We we'll see request enter password. Enter password password And click < enter >. Notice that the network device name has changed to "Router1 " because we established a telnet connection to Router1. The command

Router 1> **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 Router 2 .

Now on a second click simultaneously keys control-shift-6, Then let go and immediately press the **x** key. Notice that the network device name has changed back to "Router2." You are now back on the Router2 device.

Router1><Control> + <Shift> + <6> потом <x>

Router2#

6. Enter the show command sessions . This will allow you to see all active telnet sessions. To resume telnet session, specify the session number you want to resume (V ours case There is only one With number 1) And enter team 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 the x key to go back to Router2.

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

Router2#

8. Close session

Router2#disconnect 1

Closing connection to 10.1.1.1 [confirm]

Save project V in general And configuration each router V separateness (to a text 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 log in V modes global configurations, activate private configuration view and exit these modes?
5. How navigate V previously introduced teams And repeat their?
6. What such CDP, for what He serves and How should I use it?
7. Which one? information returns team ping ?
8. to ping all devices on the network in pairs while on one device ?
9. For what serves team traceroute ?
10. For what serves team protocol telnet ?
11. How set a name host?
12. Which one? information Can look teams show V user mode?
13. Which one? information Can look teams show V privileged mode, but can't be viewed in user mode?
14. What the device can perform router For serial communication line?

15. On what device at sequential connection frequency? is possible set sync
16. How raise interface And define his 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 close telnet compound?

Order execution And surrender work

1. 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 the variant and run it in PacketTracer assignment for independent work
5. Submit the results of the assignment to your teacher for independent work. Demonstrate their files With configurations routers. Show him that the computers are pinged 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 in Select the appropriate devices in the designer and create the topology shown in Figure 2. Assign names to the devices yourself. Enable the interfaces used on each device. Check their status. On each device, use the CDP show commands. cdp neighbors , get information about neighboring devices. Save screenshots of CDP commands.

2. Assign addresses to the interfaces according to option (v=1-16) from Table 3. All masks are equal to 255.255.255.0. For example, for option 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.

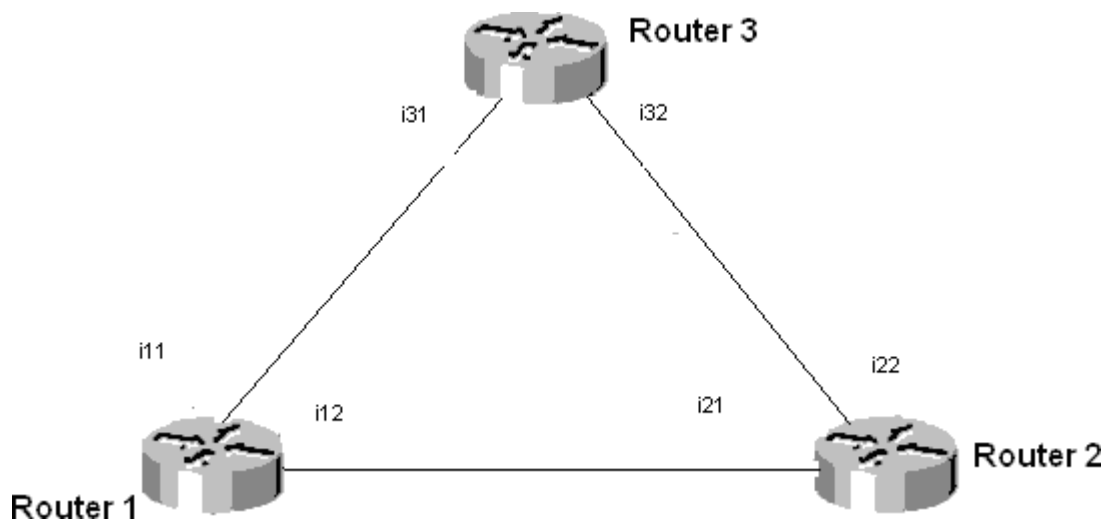


Fig. 2.

3. Check that the addresses are assigned. On each device, run the show command IP interface Brief . Save the screenshots.

4. If made All Right You you can ping from any computer certain (but not all) interface addresses of other computers.

From\To	I11	I12	I21	I22	I31	I32
---------	-----	-----	-----	-----	-----	-----

Router1	Yes	Yes	Yes *	Net	Yes *	Net
Router2	Net	Yes	Yes	Yes	Net	Yes *
Router3	Yes	Net	Net	Yes	Yes	Yes

Table 6.

Do this. Save screenshots for the pings of the connections marked in Table 4 with the * sign.

5. ping on Router1 . Save three screenshots for 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 of the Router2 console.

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 completion of the practical part.
- 3 Screenshot topology from drawing 2
4. All screenshots, specified V **Task For independent work**
5. Configurations three routers from .txt files.

Practical lesson No. 3. Static Routing Theoretical part

ARP (Address Resolution Protocol)

Once the sender has determined the receiver's IP address, it looks in its ARP table to find out the receiver's MAC address. If the source detects that the MAC and The receiver's IP addresses are present in the ARP table, It establishes a correspondence between them and uses it during encapsulation of IP packets into data link layer frames. The MAC addresses of data link layer frames are taken from ARP tables. After this, the frame is sent from the sender to the recipient via the physical channel.

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 a broadcast ARP request over the network with the following content: provide the MAC address of the network interface with the IP address of the ADR. All network devices on the network segment receive the request, and only the device with the IP address of the ADR responds to it, sending the MAC address information back to the sender. his own network interface With IP address ADR. Sender writes down couple

<MAS address, IP address ADR > V my ARP table.

Routing

Routing protocols are the rules by which information about packet transmission paths is exchanged between routers. Protocols are characterized by convergence time, loss, and scalability. Several routing protocols are currently in use, each with its own strengths and weaknesses.

One of the main tasks of a router is to determine the best path to a given destination. The router determines paths (routes) to destinations either from a static configuration entered by the administrator, or dynamically based on routing information received from other routers. Routers exchange routing information using routing protocols. A router maintains routing tables in RAM. A routing table is a list of the best known available routes. A router uses this table. For acceptance solutions Where guide plastic bag. For viewing tables routes should use the command show IP route . Even if no routing commands have been configured on a router X, it still builds a route table for the networks directly connected to it, 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

Routes to directly connected networks are mapped to the router interface they are attached to. Here, /24 denotes a mask of 255.255.255.0, and /16 denotes 255.255.0.0.

The route table maps network prefixes (network addresses) to output interfaces. When X receives a packet destined for 192.168.4.46, it looks for the prefix 192.168.4.0/24 in its routing table. According to the table, the packet will be routed to the Ethernet0 interface. If X receives a packet destined for 10.3.21.5, it will route it to Serial0.

This table shows four routes for directly connected networks. They are labeled C. Router X discards all packets destined for networks not listed in the routing table. To route packets to other destinations, additional routes must be included in the table. New routes can be added using two methods:

Static routing – the administrator manually defines routes to destination networks.

Dynamic Routing – routers follow rules, defined by routing protocols for exchanging route information and selecting the best path.

Static routes are not changed by the router itself. Dynamic routes are changed automatically by the router itself when it receives route change information from neighboring routers. Static routing consumes few computing resources and is useful in networks that do not have multiple paths to the destination. If there is only one path from router to router, static routing is often used.

To configure static routing in Cisco routers, two versions of the ip command are used.

First version

IP route DestinationNetworkAddress MaskNetworkPurpose Interface

The command tells the router that all packets destined for DestinationNetworkAddress-DestinationNetworkMask should be forwarded to its interface Interface . If the interface Interface - type Ethernet , then the physical (MAC) addresses of outgoing packets will be broadcast (why?).

Second version

IP route DestinationNetworkAddress MaskNetworkPurpose Address

The command tells the router that all packets destined for DestinationNetworkAddress-DestinationNetworkMask should be forwarded to that interface from which the IP address is reachable . Typically, Address is the address of the next hop on the path to the DestinationNetworkAddress . The output interface and physical addresses of outgoing packets are determined by the router using its ARP tables based on the IP 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 router's local interface. Serial1. Next example displays network prefix 10.7.0.0/16 on IP address 10.4.0.2 of the next hop on the way to 10.7.0.0/16. Both of these commands will add static routes to the routing table (label S):

S 10.6.0.0 via Serial1

S 10.7.0.0 [1/0] via 10.4.0.2

When an interface goes down, all static routes mapped to that interface are removed from the routing table. If the router can no longer find the next hop address along the path to address specified in the static route, the route is excluded from the table.

Note that for networks of the type Ethernet it is recommended to always use form (2) of the ip command route . The Ethernet interface on the router is usually connected to several Ethernet interfaces of other devices on the network. Specifying in the ip command route IP addresses will allow the router to correctly form the physical address of the output packet according to its ARP tables.

Routing By default.

It is not necessary for each router to maintain routes to every possible destination network. Instead, a router maintains a default route or gateway of last resort (last resort). Default routes are used when a router cannot match a destination network with a route table entry. The router must use a default route to forward packets to another router. The next router will have a route to that destination network or have its own default route to a third router, and so on. Ultimately, the packet will be routed to a router that has a route to the destination network.

The default route can be statically entered by the administrator or dynamically obtained from the routing protocol.

Since all IP addresses belong to the 0.0.0.0 network with a mask of 0.0.0.0, in the simplest case you need to use the command

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

Manually assigning a default route to each router is suitable for simple networks. In complex networks, dynamic default route exchange is necessary.

Interface loop

On Network devices can create network interfaces that are not associated with actual data transmission channels and assign IP addresses with masks to them. Such interfaces are called loops (loopback). Loops useful for phased design

networks. If a subnet is subsequently connected to a real network interface of a router, a loopback interface is first created on the router, configured to interact with the rest of the network, and only then replaced with a real interface. The loopback interface appears after the interface command. loopbackN or int for short IN, where N is a non-negative integer – the loop number. For example

```
Router(conf)>int lo 1.1.1.1 255.0.0.0
```

Команда trace

trace command is an ideal way to find out where data is being sent in networks. This command uses the same The ICMP protocol technology is similar to the ping command, but instead of checking end-to-end communication between the sender and receiver, it checks each step along the way. The trace command takes advantage of routers' ability to generate error messages when a packet exceeds its Time to Live (TTL). This command sends multiple packets and displays the round-trip time for each one. The advantage of the trace command is that it displays the next router reached. on paths To point appointments. This Very powerful means For Localizing failures along the path from sender to recipient. Trace utility response options

Symbol	Meaning
!H	Probing plastic bag was accepted router, But Not redirected, which usually happens because of the access list
P	The protocol is inaccessible
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 Router1 table# **show**

arp

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

It contains only one line about the MAC address of its Ethernet interface with IP address 10.1.1.1.

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

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

3. Ping Ethernet interface router Router1 Router2#ping 10.1.1.1

4. Look at your ARP table again. It now contains two lines. An entry has appeared about MAC address of the Ethernet interface Router1 with IP address 10.1.1.1.

```
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
```

5. Connect to router1 and view its ARP table. It already contains 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
```

A post appeared about MAC address of the Ethernet interface of Router2 with IP address 10.1.1.2. Why, since we didn't send any IP packets from Router1? Because, what Router1 needed to know to respond to a ping from Router2 MAC address of the Ethernet interface of Router2 with IP address 10.1.1.2, and it generated an ARP packet for him receipt.

Static routes

ping some interfaces from Router2 and Router4 due to a lack of routing. We'll fix that.

1. Join us To router router2. We Not could ping Addresses 172.16.10.1 and 172.16.10.2. See the route table.

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 connected ones networks. There is no route to the 172.16.10.0/24 network. Let's add a route to the 172.16.10.0/24 network via the address 10.1.1.1 nearest hop on the way to this network:

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

From here on, 172.16.10.0/24 is an abbreviated notation defining the subnet 172.16.10.0 with a mask of 255.255.255.0. The mask 255.255.255.0 contains 24 units, which is denoted by /24.

2. Successfully let's ping serial interface Router1

Router2# **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
S    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 packages pings Not know, How them return back from Router4, since there are no routes defined on Router4.

4. Join us To router router4. Take a look table Router4# **show routes IP route**

```

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

```

No route To networks 10.1.1.0/24. Let's add route To networks 10.1.1.0/24 through address 172.16.10.1 of the nearest hop on the way to this network:

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 on the network can be pinged from each network device. Check this.

Routing By default.

Network devices Router2 and Router4 have only one output to the outside world: via interfaces with addresses 10.1.1.1 and 172.16.10.1, accordingly. Therefore, You don't have to specify which subnets we route packets to and use default routing.

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 we'll assign default routes. 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 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 Router1
loops(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 Router2 loop# **ping 1.1.1.1**

Save project V in general And configuration each router V separate file.

Control questions

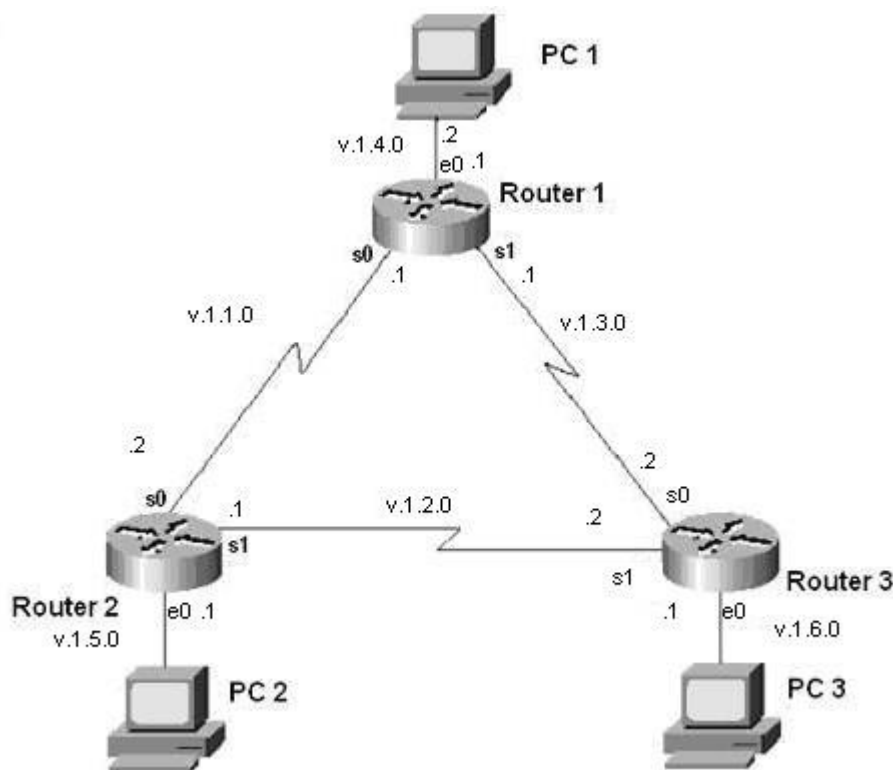
1. How the sender finds out MAC recipient's address ?
2. How look ARP table?
3. When V ARP table appear new lines?
4. What such route table ?
5. If administrator Not tuned none routes, That What she will contain?
6. How static routing is different from dynamic?
7. Which two forms tasks static routing You do you know?
8. How V team routing is determined net destination?
9. Why For networks type Ethernet recommended Always use form (2) routing commands?
10. Explain values fields V teams routing.
11. Why V quality fields **Address** recommend use address next hop on the way to the destination network.
12. When is used routing By default?
13. When use interface loop?
14. How works team traces ?

Order execution And surrender work

1. 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 independent work.
5. Show me to the teacher result execution points 8 And 9 tasks 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. Use the required routers.



Drawing 1

IN ours networks six subnets. You you see, What every router connected To three subnets.

2. On each router raise used interfaces And view neighbors with the show command `cdp neighbors` . Take screenshots.

3. Assign interfaces networks addresses according to drawing 1 And table 1 V which v – this is the option number. All masks are 255.255.255.0. Don't forget to assign default gateways to 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	S 0:v. 1.1.1		S 1:v. 1.3.1	E 0:v. 1.4.1		
Router2	S 0:v. 1.1.2	S 1:v. 1.2.1			E 0:v. 1.5.1	
Router3		S 0:v. 1.2.2	S 1: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 show command router running-config and show IP interface brief . For computers, use the ipconfig command .

5. Check that the addresses are assigned correctly by running this on each router. teams ping To direct to neighbors. For example, on on Router1, run

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 tie up between by yourself computers PC1, PC2 And PC3. To do this, we will configure static routing on the routers. In each router let's write it down routes on remote Ethernet networks. For To solve the problem of routing packets to remote serial connection networks, there is no need.

U each router There is By two on deleted Ethernet networks. Total You need to register six static routes.

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

This the team will do

router1(config) #ip route 1.1.5.0 255.255.255.0

1.1.1.2 Specify the remaining five routing commands.

7. On each router look table routing team show IP route . Take screenshots.

8. On each router do it screenshots extended pings a) on router1 from PC2 to PC3

b) on router router2 from PC1 To PC3 c) on

router router3 from PC1 To PC2

For example, result extended ping on router router1 from PC2 To PC3 for option 1 (v=1) has the form

```

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 others computers. Total six screenshots. For example, tracing from PC1 on PC2 for option 1 (v=1)

```
PC1:#tracert 1.1.5.2
```

```

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

 0 1.1.4.1 0 msec 16 msec 0 msec
 1 1.1.1.2 20 msec 16 msec 16 msec
 2 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 part .
2. Configurations three routers from .txt files, created at completion of the practical part.
3. Screenshot topology from drawing 1 With addresses his own options
4. Table 2 With addresses your own version
5. Configurations three routers from .txt files, created at completing an assignment for independent work.
6. All screenshots, specified V task For independent work

Laboratory Job No. 4. Dynamic routing

Theoretical Part

Static routing is unsuitable for large, complex networks because they typically include redundant links, multiple protocols, and mixed topologies. Routers in complex networks must quickly adapt to topology changes and select the best route from multiple candidates.

IP networks have a hierarchical structure. From a routing perspective, the network is viewed as a collection of autonomous systems. In autonomous subsystems of larger networks widely used for routing to other autonomous systems default routes.

Dynamic routing can be accomplished using one or more protocols. These protocols are often grouped according to where they are used. Protocols for operation within autonomous systems are called interior gateway protocols (interior gateway protocols (IGP)), and protocols for working between autonomous systems are called external gateway protocols (exterior gateway IGP protocols include RIP, RIP v2, IGRP, EIGRP, OSPF, and IS-IS. EGP3 and BGP4 are EGP protocols. All these protocols can be divided into two classes: distance vector protocols and link-state protocols .

Routers use metrics for route assessments or measurements. When from router To networks there is an appointment many routes, And All They use the same routing protocol, then the route with the lowest metric is considered the best. If If different routing protocols are used, then administrative distances assigned to routes by the router's operating system are used to select the route.

RIP uses V quality metrics quantity transitions (hops). EIGRP uses a complex combination of factors including channel bandwidth and channel reliability.

The results of the routing protocols are entered into the route table, which constantly changes at change situations V networks. Let's consider typical line in the 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 means RIP, O means OSPF, etc. The notation [120/3] means, this route has administrative distance 120 And metric

3. The router uses these numbers to select a route. The 00:00:06 element defines the time when this line was updated. Serial0 is the local interface through which the router will route packets to network 192.168.14.0/24 via address 10.3.0.1.

In order for dynamic routing protocols to exchange information about static routes, additional configuration must be performed.

Distance vector routing

This routing is based on the Bellman -Ford algorithm. At certain points in time, the router transmits to neighboring routers all my routing table. Simple protocols such as RIP and IGRP simply broadcast routing table information through all router interfaces without specifying the exact address. a specific neighboring router.

A neighboring router, upon receiving a broadcast, compares the information with its current routing table. Routes to new networks or routes are added to it. To famous networks With the best metric. Deletion occurs non-existent routes. The router adds its own values to the metrics of the received routes. The new routing table is again propagated to neighboring routers (see Fig. 1).

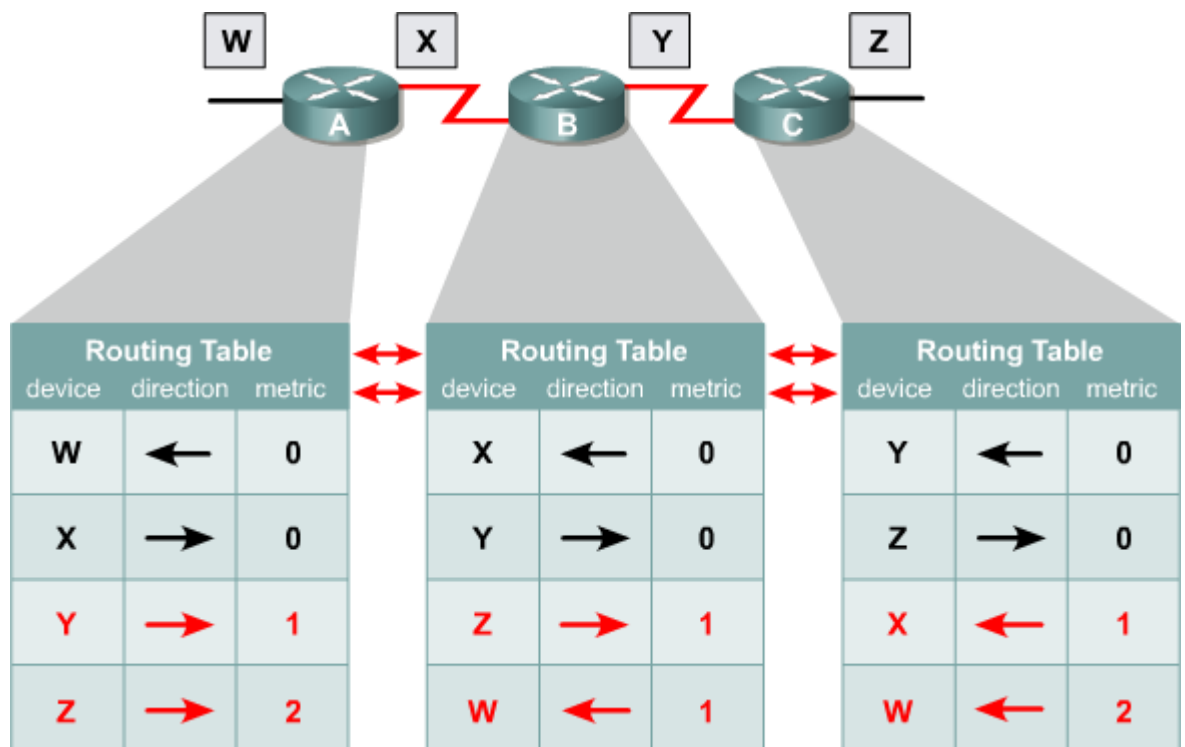


Fig. 1. Distance vector routing.

Protocols states connections

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

The router considers the link state of the interfaces of other routers in the network. The router builds a complete database of all link states. V his own areas, That There is has enough information For creation his own

mapping . Each router then independently runs the SPF algorithm on its own network mapping or link state database to determine the best path, which is entered into the routing table. These paths to other networks form a tree with the local router as the vertex.

Routers advertise the state of their links to all routers in the area. This announcement is called an LSA. (link-state advertisements).

Unlike distance vector routers, link-state routers can form special relationships with their neighbors.

Has place elementary influx LSA packages for constructions bases data link states. Further routing updates are performed only when the link state changes or if the state has not changed for a certain period of time. If the link state changes, a partial update is sent immediately. This update contains only the link states that have changed, not the entire routing table.

An administrator concerned with link utilization finds these partial and infrequent updates an effective alternative to distance vector routing, which broadcasts the entire route table at regular intervals .

Link state protocols have faster convergence and better bandwidth utilization compared to Distance vector protocols. They are superior to distance vector protocols for networks of any size, but have two major drawbacks: increased demands on router computing power and complex administration.

Convergence.

This process is both collaborative and individual. Routers share information among themselves, but independently recalculate their routing tables. In order for individual routing tables to be accurate, all routers must have the same idea of the topology networks. If routers agree on a network topology, they converge. Rapid convergence means rapid recovery from link failures and other network changes. Routing protocols and the quality of network design are judged primarily by convergence.

When routers are converging, the network is susceptible to routing problems. If some routers determine that a particular link is missing, others will mistakenly assume it is present. If this happens, the individual routing table will become inconsistent, potentially leading to dropped packets and routing loops.

It is impossible for all routers The network simultaneously detected topology changes. Depending on the protocol used, it may take a long time for all routing processes in the network to converge. This is influenced by the following factors:

Distance V hops to points topology changes .

Number routers, using dynamic Protocols. Bandwidth and communication channel loading.

Loading routers .

Effect some factors Maybe be reduced at thorough design

netw
orks.

Configuration dynamic routing

There are two main commands used to configure dynamic routing: router and network . The router command initiates the routing process and has the form:

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

Where Protocol - 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 network added to the routing process, keyword - additional parameters. network - number allows the routing process to determine the interfaces that will participate in sending and receiving packets updating route information.

To view information about routing protocols, use the show command. IP protocol , which displays the values of routing process timers and network information related to routing. This information can be used to identify a router suspected of providing bad routing information.

The contents of the IP routing table are displayed by the show command. IP route . It contains records about All famous network router And subnets and indicates on the way to obtain this information.

Protocol RIP

Key characteristics protocol RIP:

routing on basis vectors distances;

metrics at choice paths V view quantities transitions (hops); the

maximum permissible number of hops is 15;

By default, routing information update packets are sent in broadcast mode every 30 seconds.

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

Team network assigns IP network address With to which the router has a direct connection.

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

Process routing connects interfaces With corresponding addresses and begins processing packets in the specified networks.

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

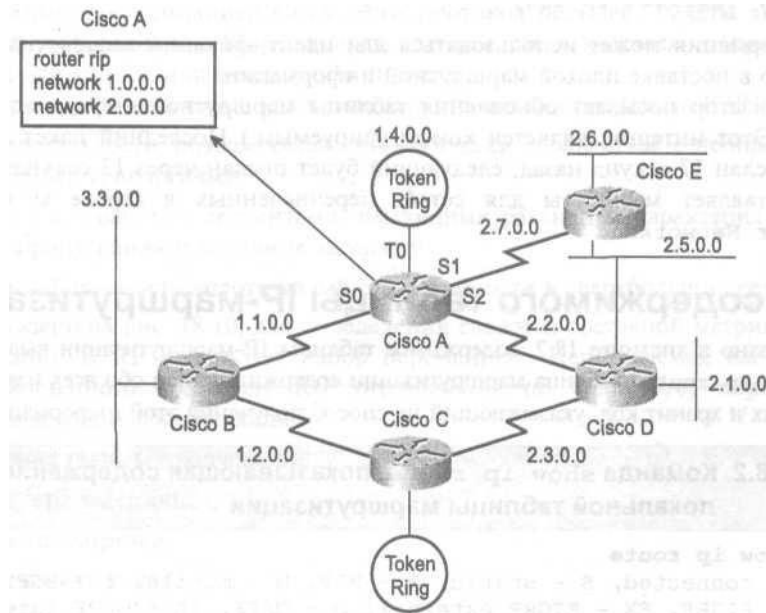


Fig.2.

debug command IP rip displays the contents of RIP routing update packets in the form in which they are data is sent and received.

Protocol IGRP

IGRP is a distance vector routing protocol developed by Cisco. This protocol sends routing update packets at 90-second intervals, containing information about networks for a specific autonomous system. This protocol is characterized by its versatility, allowing it to automatically handle complex topologies, and its flexibility in working with segments with different bandwidth and latency characteristics. The metric it uses does not have the hop limitation inherent in RIP. It includes the following components: Bandwidth; Latency; Load level; Link reliability; Maximum transmission unit size on the link.

Selecting IGRP as the routing protocol is done using the command:

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

where the Autonomous-system parameter is called the autonomous system number and identifies the IGRP routing computation process. Processes in network routers with the same autonomous-system number will share route information.

network command specifies the directly attached networks to be included in this routing process:

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

In the example shown in Fig. 3, the Cisco router A is running a routing organizing process IGRP routing V autonomous system with number 109. Networks 1.0.0.0 and 2.0.0.0.

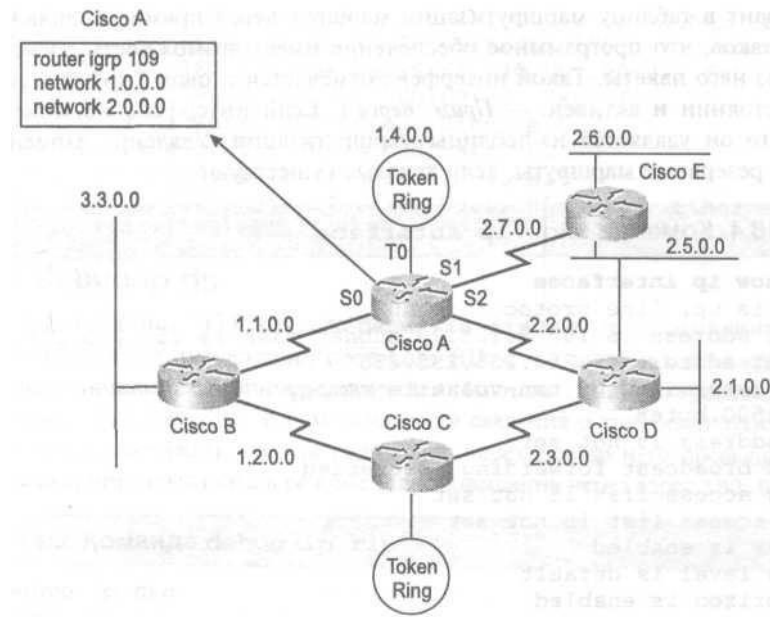


Fig.3.

debug command IP igrp transactions and debugging IP igrp events displays the contents of IGRP routing update packets in the form in which these data is sent and received

Protocol OSPF

OSPF is dynamic, hierarchical A link-state protocol used for routing within autonomous systems. It is based on open standards and was designed as a replacement for RIP. It is an evolution of earlier versions of the IS-IS routing protocol. OSPF is a robust protocol that supports least-weight routing and load balancing. The shortest path in the network is calculated using Dijkstra's algorithm . Cisco maintains its own version of the OSPF standard.

Once a router is configured to run OSPF, it begins the process exploring its surroundings, going through several initialization phases. Initially, the router uses the Hello phase to discover its neighbors and establish relationships for exchanging routing updates with them. Then, the router begins the ExStart phase. initial exchange between bases routes. Next is a phase exchange, V

In which the designated router sends routing information and receives acknowledgments from our new router. During the boot phase, the new router compiles its routing table. Once the calculations are complete, the router enters the full state, in which it is an active member of the network.

For launch OSPF routing serves Router command (config)# **router ospf N**,

where N is the OSPF computing process number. Unlike IGRP, it can be different for different routers in an autonomous system. An OSPF Area is organized team

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

And defines autonomous system.

In OSPF, the network-number has a special format. For a network included in the routing process, the inverse mask is used . So, network 212.34.0.0 255.255.0.0 should be placed in OSPF routing area 7, the command should be given

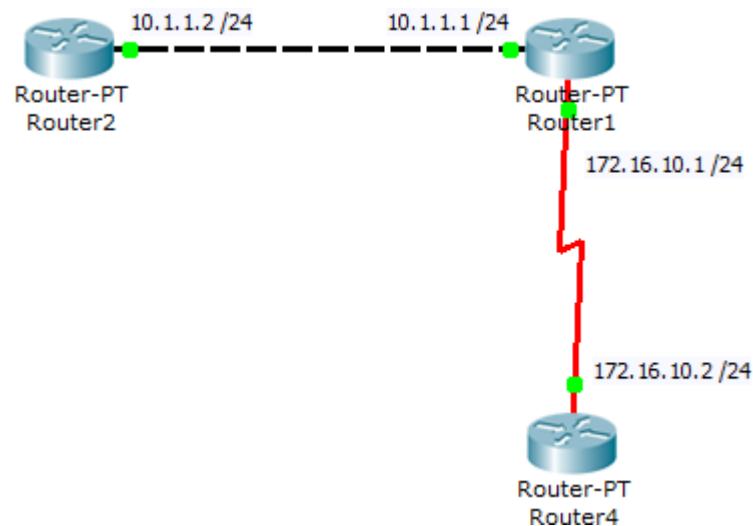
Router(config- router)# **network 212.34.0.0 0.0.255.255 area 7**

The show command IP ospf interface for each interface displays all OSPF information: IP address, area, process number, identifier router, cost, priority, network type, timer intervals.

The show command IP ospf neighbor displays important information regarding the status of neighbors.

Practical Part

1. Load the topology and configuration used in the practical part of Lab 2 into the simulator.
2. If everything is done correctly, you will be able to ping the addresses of directly connected interfaces of other routers from any router. On each device, use the CDP show commands. cdp neighbors detail , get the IP addresses of neighboring devices and ping them.
3. In Lab #2, we were unable to ping long-range interfaces. Network 172.16.10.0/24 was unreachable from Router2, and network 10.1.1.0/24 was unreachable from Router4. In Lab #3, we solved the problem using static routing. In this lab, we'll use various forms of dynamic routing to address the issue.



Drawing 4.

4. Let's see tables Router2# **sh**

routes IP route

There is no route to network 172.16.10.0/24.

Therefore V this one net from Router2 Not they

are coming pings . Router4# **sh IP route**

No route on network 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 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, use the show command. running-config Let's see how the routers interpreted our commands. We see that the 10.1.1.0/24 network was perceived as 10.0.0.0/8, and the 172.16.10.0/24 network was perceived as 172.16.0.0/16. This is due to IP address classes.

3. Show command IP Let 's look at the parameters the RIP protocol works with. 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 Router2# **sh**

routes 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 net 172.16.10.0/24 through Ethernet interface on address 10.1.1.1. Pings to this network from Router2 will work. Check.

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Let's move on on another 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 net 10.1.1.0/24 through Serial interface on address 172.16.10.1. Pings to this network from Router4 will work. Check.

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

5. debug command IP rip Let's look at how routers exchange routing information. For example, for Router1, we have messages that repeat every 30 seconds.

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

Disable Router1 tracing# **no**

debug IP rip

Save configuration.

EIGRP

Let's stop on everyone routers RIP with the command 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, use the show command running-config Let's see how the routers interpreted our commands. We see that the 10.1.1.0/24 network was perceived as 10.0.0.0/8, and the 172.16.10.0/24 network was perceived as 172.16.0.0/16. This is due to IP address classes.

3. Show command IP Let's look at the protocol parameters that the EIGRP protocol works with. 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 Router2# **sh**

routes 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

```

Eat route on net 172.16.10.0/24 through Ethernet interface on address 10.1.1.1. Pings to this network from Router2 will work. Check.

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Let's move on on another 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 net 10.1.1.0/24 through Serial interface on address 172.16.10.1. Pings to this network from Router4 will work. Check.

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

7. Teams debug IP eigrp transactions and debugging IP eigrp events See how routers exchange routing information.

Save configuration.

OSPF

Let's stop on everyone routers EIGRP with the command Router (config)# **no router eigrp 100**

1. Enable OSPF on all routers. Give the OSPF process number 100. Create OSPF area 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 our commands in the same form as we asked them.

3. Show team IP Let 's look at the parameters the OSPF protocol works with. 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 Router2# **sh**

routes 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 net 172.16.10.0/24 through Ethernet interface on address 10.1.1.1. Pings to this network from Router2 will work. Check.

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 net 10.1.1.0/24 through Serial interface on address 172.16.10.1. Pings to this network from Router4 will work. Check.

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 neighbor will show you all the information about the OSPF protocol parameters.
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 And link state protocols?
8. What such convergence protocols routing?
9. Which parameters influence on speed convergence?
10. How on router launch And tune protocol routing RIP?
11. How on router launch And tune protocol routing EIGRP?
12. How on router launch And tune protocol routing OSPF?
13. How look content packages updating route RIP protocol information?
14. How look content packages updating route EIGRP protocol information?
15. Please clarify, What V EIGRP understood under autonomous system?
16. IN how difference in format teams router For EIGRP and OSPF?
17. IN how difference in format teams network for RIP, EIGRP And OSPF?

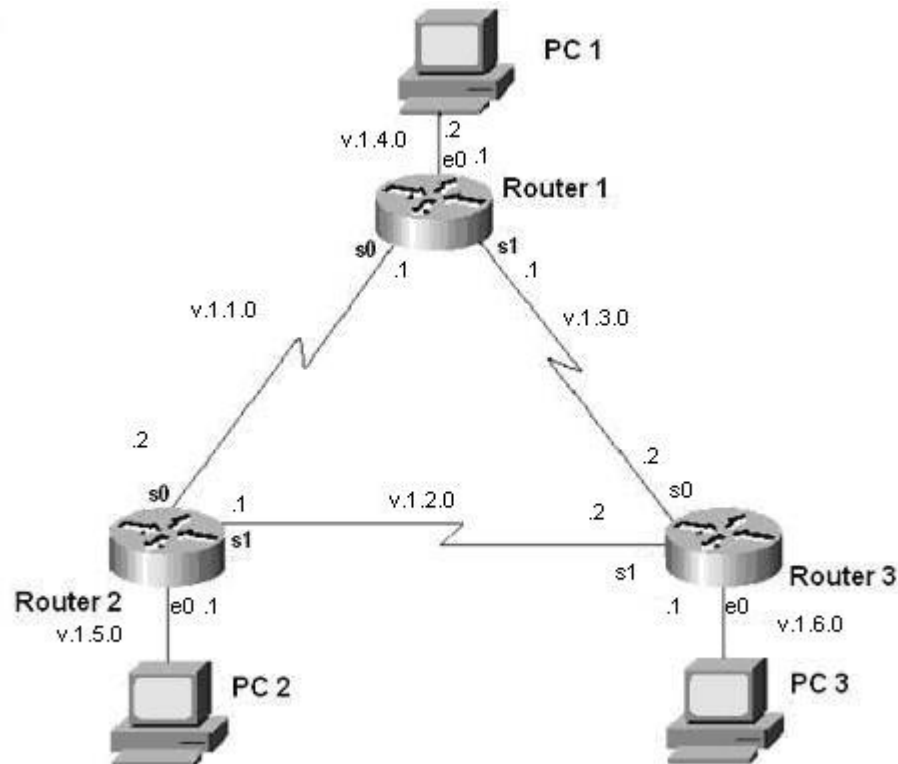
Order execution And surrender work

1. 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 option from previous laboratory work, complete V Boson assignment for independent work.
5. Submit to your teacher the results of completing points 7, 10, 14 and 18 of the independent work assignment.
6. Make out report. Content report Look below.

7. Protect report.

Exercise For independent work

1. Use topology his own options from previous laboratory work presented in Figure 5.



Drawing 5.

Our network has six subnets. You can see that each router is connected to three subnets.

2. Manually edit the saved configuration from the previous successfully completed lab: remove static routing commands from the routers' rtr files.

3. Download edited configuration V simulator.

4. On each router, check that the configuration is loaded correctly using show commands. cdp neighbors and show IP interface brief .

If the serial interface does not come up, check with the **show command. running - config** , what's on the DCE side interface serial communication **clock** command is given **rate** ! If not set, set it.

5. Configure dynamic routing using RIP on each router.

6. View the routing table on each router. 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, run tracert commands against the other computers. Take screenshots. Six screenshots in total. For example, tracert from PC1 to PC2 for option 1 (v=1) has the form

```
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 *

```

We see that the path for packets from PC1 to PC2 (1.1.5.2) goes sequentially through Router1 (Ethernet 1.1.4.1) and then via Router2 (serial0 1.1.1.2)

8. Let's turn it off on router router1 consistent interface serial 0 Router1(config)#
interface serial 0

```
Router1( config- if)# shutdown
```

9. After a couple of minutes, when the routing information has been updated in the network, look at the routing table on each router 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      1.1.3.0/24 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

```

We see that the table has changed: the 1.1.1.0/24 network has disappeared and all packets are now routed to address 1.1.3.2 via the Serial1 interface.

10. On each computer, run tracert commands against the other computers. Take screenshots. Six screenshots in total. For example, tracert from PC1 to PC2 for option 1 (v=1) has the form

```
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 via Router3 (serial0 1.1.3.2) and then via Router2 (serial1 1.1.2.1).

11. Save configuration.
12. Disable RIP and configure dynamic routing using IGRP on each router.
13. View the routing table on each router. 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
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

```

14. Verify that you've done everything correctly. On each computer, run tracert commands against the other computers.
15. Save configuration.
16. Disable IGRP and configure dynamic routing using OSPF on each router.
17. View the routing table on each router. 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
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

```

18. Verify that you've done everything correctly. On each computer, run tracert commands against the other 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 part.
2. Configurations of three routers from .txt files created during the practical part for each routing protocol. A total of nine (9) files.
3. Screenshot topology from drawing 5 With addresses his own options
4. Table 2 previous laboratory work With addresses his own options
5. Configurations of three routers from .txt files created during the independent work assignment for each routing protocol. A total of nine (9) files.
6. All screenshots, specified V task For independent work

Laboratory Job No. 5. Classless addressing CIDR And variable length masks (VLSM)

Theoretical Part

A scalable network requires an addressing scheme that allows for growth. However, uncontrolled network growth can lead to a number of unforeseen consequences. measure adding nodes and subnets the enterprise network can A shortage of available addresses may arise, requiring changes to the existing address scheme. This can be avoided through careful planning of a scalable addressing system for the enterprise network.

Unfortunately, the architects TCP/IP could not predict the exponential growth of the Internet, and address allocation is currently a pressing issue.

When TCP/IP was introduced in the 1980s, it was based on a two-level addressing scheme. The high-order portion of the 32-bit IP address defined the network number (address), while the low-order portion defined the host number. The network address is necessary for interoperability between networks. Routers use the network portion of the address to organize communication between hosts on different networks.

For human readability, IP addresses are written as four decimal numbers separated by periods. The 32-bit address is divided into four groups of eight bits, called octets. Each octet is written in decimal notation and separated by periods. For example:

10101100000111101000000000010001 <-> 10101100 00011110 10000000 00010001 <->
172 30 128 17 <-> 172.30.128.17

The question arises: how can we distinguish the network address and host address from any IP address? In the early days of TCP/IP, a classful addressing system was used to solve this problem. IP addresses were divided into five disjoint classes. The division was based on the values of the first few bits in the first octet.

If first bit V first octet is equal to zero, That This address class A. Addresses class B addresses start with binary 10. Class C addresses start with binary 110.

In class A addresses, the network address is located in the first octet. In class B, the first and second octets are used for network addressing. In class C, the first, second, and third octets are used for network addressing. The use of classes D and E is specific. and is not considered here.

In modern networks, classes are often ignored and a classless IP scheme based on subnet masks is used.

From here on, we'll use masks as a sequence of binary ones followed by a sequence of binary zeros, with a total length of 32 bits. Masks are typically written in decimal notation, similar to IP addresses.

11111111111111110000000000000000 <-> 11111111 11111111 00000000 00000000 <->
255 255 0 0 <-> 255.255.0.0

Mask subnets is necessary addition to IP address. If bit V IP address corresponds to a single bit in the mask, then this bit in the IP address represents the network number, If a bit in an IP address corresponds to a zero bit in the mask, then that bit in the IP address represents the host number. So, for a mask of 255.255.0.0 and an address of 172.24.100.45, the network number will be 172.24.0.0, and for a mask of 255.255.255.0, the network number will be 172.24.100.0.

Another form of writing the mask is /N, where N is the number of ones in the mask. This form is only used in conjunction with an IP address. For example, for a mask of 255.255.0.0 and an address of 172.24.100.45, you would write 172.24.100.45/16.

All addresses class A have mask 255.0.0.0, addresses class IN have mask 255.255.0.0, and class C addresses have a mask of 255. 255. 255.0. The converse is not true, since the first bits in the first octet of the address are used to determine the class.

If an organization has a Class B network (mask 255.255.0.0), it can subnet this network using the mask 255.255.255.0. For example, if the address 172.24.100.45 belongs to the organization, the Class B network number would be 172.24.0.0, and the internal corporate subnet number would be 172.24.100.0. Note that the resulting subnets will not be Class C networks.

If the number of zeros in the mask is M, then the number of available host addresses in the subnet is $2^M - 2$. This means that using two addresses in a subnet is not recommended. One of these addresses, with the last M bits set to zero, is called the subnet address, and the second address, with the last M bits set to one, is called the broadcast address. Thus, for the address 172.24.100.45/24, the subnet address is 172.24.100.0, and the broadcast address is 172.24.100.255. The number of addresses in the subnet is $2^8 - 2 = 254$.

Class A and B addresses make up about 75 percent of the address space. The number of class A networks A and B are approximately equal to 17,000. Acquiring a Class B network, let alone a Class A network, is currently quite problematic. Class C addresses make up about 12.5 percent of the address space. The number of Class networks C is approximately 2.1 million. Unfortunately, the Class C network is limited to 254 addresses that do not meet the needs of large organizations that cannot acquire Class A or B addresses.

Classful IP addressing, even with subnetting, cannot meet the scalability requirements of the Internet community.

By the early 1990s, almost all Class B networks were already allocated. The addition of new Class C networks to the Internet led to significant growth in routing tables and router overload. The use of classless addressing has significantly alleviated these problems.

CIDR

Modern routers use a form of IP addressing called classless. cross-domain routing (Classless Interdomain Routing (CIDR)),

which ignores classes. In class-based systems, the router determines the class of the address and then splits the address into Network octets and host octets are based on this class. In CIDR, the router uses mask bits to determine the network portion and host number in an address. The address boundary can be located in the middle of an octet.

CIDR significantly improves IP scalability and efficiency in the following ways:

- flexibility;
- economical usage addresses V highlighted range;
- improved aggregation routes;
- Supernetting is the combination of contiguous network addresses into a new supernet address defined by a mask.

CIDR allows routers to aggregate or summarize routing information. They do this by using a mask instead of address classes to define the network portion of an IP address. This reduces the size of routing tables by using only one address and mask to represent routes to many. subnets.

Without CIDR and route aggregation, a router must contain individual information for all 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	The third octet	The 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 of the address for each of these eight subnets are unique, a classful router sees eight unique networks and must create a route table entry for each of these subnets.

However, these eight subnet addresses have a common part: the first 13 bits are the same. A CIDR-compliant router can summarize routes to these eight subnets using a common 13-bit prefix in the addresses: 00101100 00011. To represent this prefix in decimal form, we pad it with zeros on the right.

10101100 00011000 00000000 00000000 = 172.24.0.0.

13-bit mask subnets has the form

11111111 11111000 00000000 00000000 = 255.248.0.0.

Therefore, one address and one mask defines a classless prefix that summarizes routes to eight subnets: 172.24.0.0/13.

Supernetting

Supernetting is practice of use bit mask For grouping several class networks into one network address. Supernetting and route aggregation are different names for the same process. However, the term supernetting is more commonly used when the networks being aggregated are under common administrative control. Supernetting takes bits from the network portion of the mask, while subnetting takes bits from the host portion of the mask. Supernetting and route aggregation are the inverse concepts of subnetting .

Since Class A and B networks are almost exhausted, organizations are forced to request multiple Class C networks from providers. If a company receives a block of contiguous addresses in Class C networks, supernetting can be used. and all addresses in the company will be located in one larger network or supernet .

Let's consider a company called ABC, which requires addresses for 400 hosts. class addressing, the company must request a class B network from the central Internet service InterNIC. If the company receives such a network, then tens of thousands of addresses in it will not will be be used. Alternative is receiving two networks class WITH, What yields $254 * 2 = 504$ host addresses. The disadvantage of this approach is the need to support routing for two networks.

With a classless addressing system, supernetting allows Company ABC to obtain the necessary address space with a minimum number of unused addresses and without increasing the size of its routing tables. Using CIDR, ABC requests a block of addresses from its ISP , not from the central Internet service (InterNIC). The ISP determines ABC's needs and allocates address space from its own address space. The ISP assumes management of the address space in its internal classless system. All external Internet routers contain only summary routes to the ISP's network. The ISP itself maintains routes more specific to its customers. including ABC. This approach significantly reduces the size of route tables for all routers on the 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 tables are visible, what are the addresses have common 23-bit prefix 11001111 00010101 0011011. By padding the prefix on the right with zeros 11001111 00010101 00110110 00000000, we get a supernet with a 23-bit mask, 207.21.54.0/23.

The provider provides the ABC company network to the outside world as a network 207.21.54.0/23.

CIDR allows providers distribute effectively And Sum contiguous IP address spaces.

VLSM

Variable-Length Mask Subnet Mask (VLSM)) allows an organization to use more than one subnet mask within the same network address space. The VLSM implementation is often referred to as "subnets within subnets."

Let's consider the subnets created by borrowing the first three bits in the host portion of the Class C address 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 received eight subnets, each of which can contain no more than 30 hosts.

Each connection via a serial interface requires two addresses. and a separate subnet. Using any of the /27 subnets for this will result in a loss of addresses. A 30-bit subnet is best suited for creating a two-address subnet. Mask. This is exactly what's needed for a serial connection. Let's split one of the subnets 207.21.24.192/27 into eight subnets using a 30-bit mask.

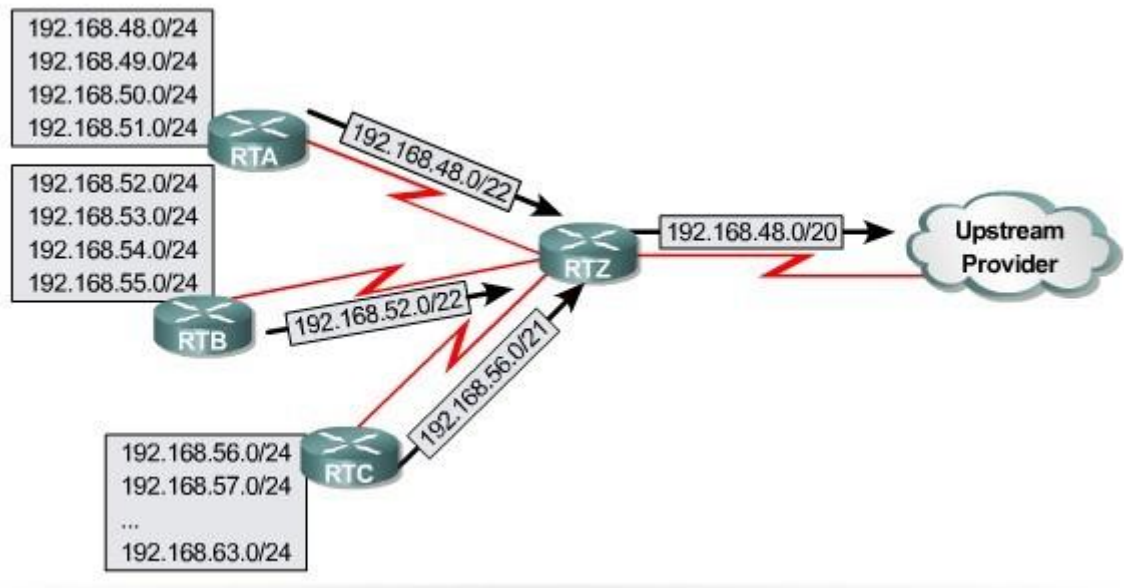
0	207.21.24.192/30
1	207.21.24.196/30
2	207.21.24.200/30
3	207.21.24.204/30
4	207.21.24.208/30
5	207.21.24.212/30
6	207.21.24.220/30
7	207.21.24.224/30

Таблица 4.

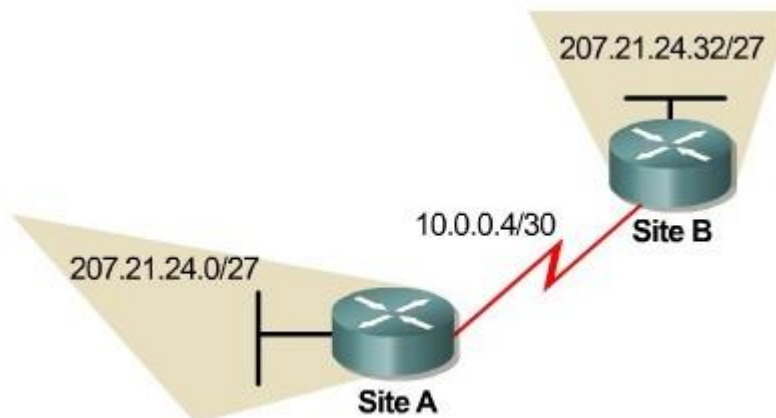
That there is every from the remaining seven subnets /27 Can use for Host addressing on seven local area networks. These local area networks can be linked into a global network using no more than eight consecutive connections from our eight networks.

For proper routing in VLSM networks, routers must exchange information about subnet masks.

Using CIDR and VLSM not only prevents address waste but also facilitates route aggregation, or summarization. Without route summarization, the Internet would have ceased to develop by the late 1990s. The figure illustrates how summarization reduces the load on routers.



Rice. 1



Rice. 2

This complex network hierarchy And subnets summed up V various points like this, What the whole network looks like from the outside 192.168.48.0/20. For route summarization to work correctly, address assignment must be done carefully: the addresses being summarized must have the same prefixes.

Torn subnets

Discontinuous subnets are networks from the same main network separated by a network in a completely different address range. Classful routing protocols RIP version 1 and IGRP do not support discontinuous networks, since routers do not exchange subnet masks. If the site in Figure 1 A and the site B work on RIP version 1, then the site A will receive routing information updates from site B on the network 207.21.24.0/24, not in the 207.21.24.32/27 network.

RIP v2 and EIGRP summarize addresses at class boundaries by default. This summarization is generally desirable. However, it is not recommended for discontinuous subnets. You can cancel class autosummary with the `no auto-summary` command.

Practical Part

We configure VLSM and test its functionality on two routing protocols: RIP version 1 and RIP version 2.

Let's consider a class C network 192.168.1.0/24. It is necessary to allocate a minimum of 25 addresses for each of the two local networks and reserve the maximum number of addresses for further development.

To support 25 hosts in each subnet, a minimum of five bits in the eight-bit host portion of the address is required. Five bits will yield a maximum of 30 possible host addresses ($2^5 = 32 - 2$). If five bits are to be used for hosts, the other three bits in the last octet of the address can be added to the 24-bit mask of our Class C network. Therefore, a 27-bit mask can be used to create the following eight 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.

For further maximization address spaces subnet 192.168.1.0 /27 is again divided into 8 subnets using a 30-bit mask:

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 point-to-point serial connections and minimize address wastage since each subnet contains only two addresses.

Let's build and configure the network shown in Figure 3. For the router For Vista we'll use the 2501 model, and for the other two, the 805 model. We'll use the 2950 switch.

1. Raise it up interfaces And check net team **show cdp neighbors** .
2. Assign addresses according to the figure. Check the assignment with the **show command. IP interface brief** .

3. For the computer HostA, there is ambiguity in the default route assignment: either to the address 192.168.1.33 of the Ethernet interface of the router SanJose1, or to the address 192.168.1.34 of the Ethernet interface of the router SanJose2 . Choose any one, for example

```
hostA# ipconfig / dg 192.168.1.33
```

4. We'll configure RIP routing on all three routers with address autosummary disabled . This will allow subnet information to flow through.

```
Router ( config )# router rip
```

```
Router(config-router)# version 2
```

```
Router(config-router)# no auto-summary
```

```
Router(config-router)# network 192.168.1.0
```

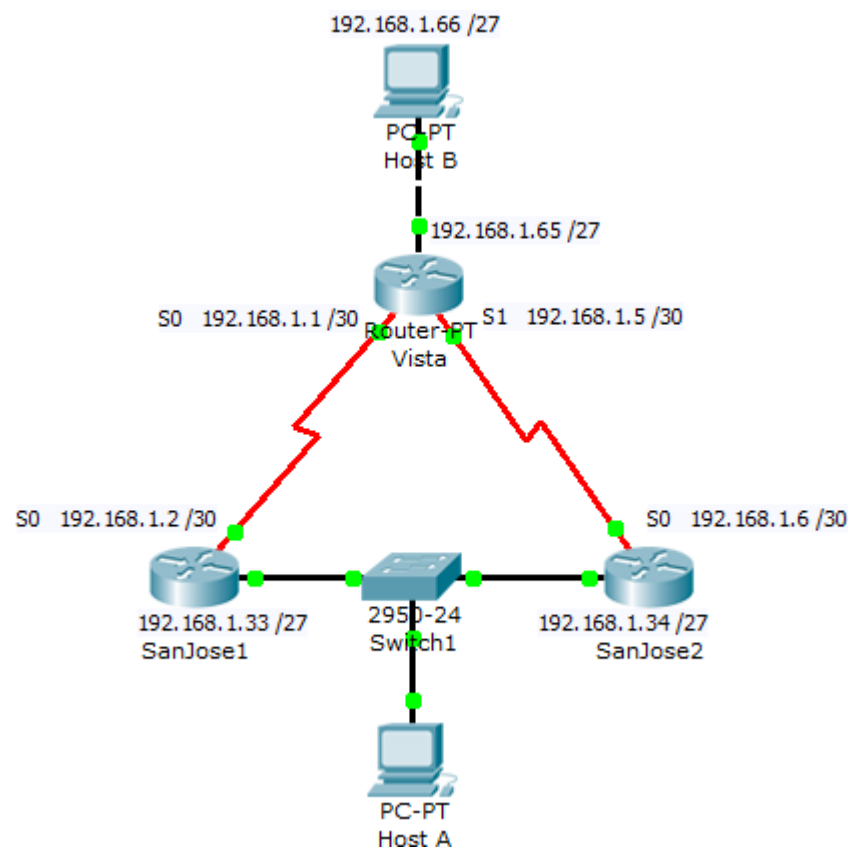


Fig. 3

5. Must see, that the Vista router has a route to the local network 192.168.1.32/27, where the computer hostA is located .

```
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 that the table shows only one route to the network 192.168.1.32/27 – to the address 192.168.1.2 through interface Serial0, Although there are more one route on net 192.168.1.32/27 –

via interface address 192.168.1.6 Serial1. In a real router, we would see both of these routes. The simulator displays one route, but exchanges routing information over both 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's on the router? SanJose1 has a route to the local network 192.168.1.64/27, where the computer hostB is located .

```
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 on local network 192.168.1.64/27, where the hostB computer is located .

```
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 computer hostA from computer hostB And vice versa. Do it 2 screenshot.

Note, What simulator implemented So, What given example works And without entering commands version 2 and no auto-summary .

Control questions

1. For what do you need a mask?

2. What is CIDR?
3. What is VLSM?
4. How are host and subnet addresses separated into IP address classes?
5. How are IP address classes separated into IP address classes? Highlight the host address and the subnet address?
6. What is the number of available addresses in subnets?
7. Based on the number of hosts in the subnet specified by the teacher, determine the minimum mask.
8. Which forms record masks do you know?
9. Why consistent compound highlight V separate subnet?
10. What mask is recommended for a serial network and why?
11. How do CIDR and VLSM contribute to the efficient use of address space?
12. What is Supernetting?
13. What is route aggregation and how does it help reduce the size of router route tables?
14. What are torn subnets, and which protocols routing them don't support?
15. Which peculiarities work simulator at implementation RIP protocol?

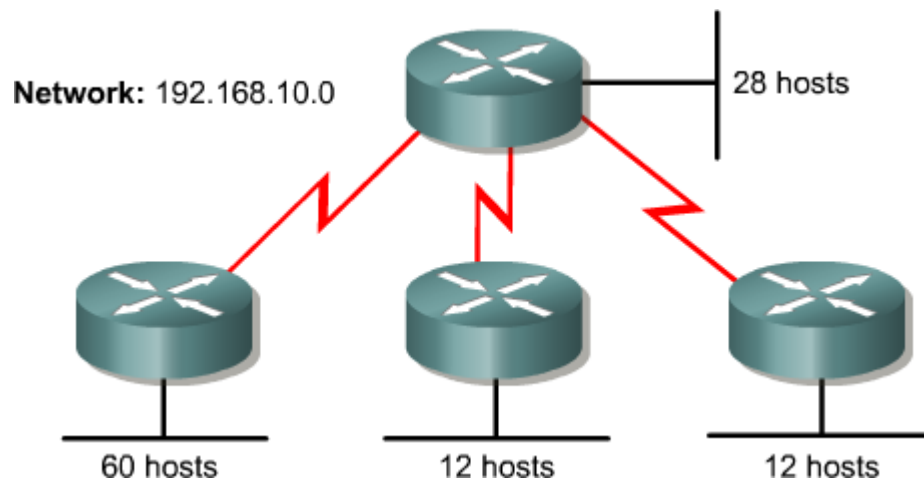
Order execution And surrender work

1. 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 for independent work.
6. Make out report. Content report Look below.
7. Protect report.

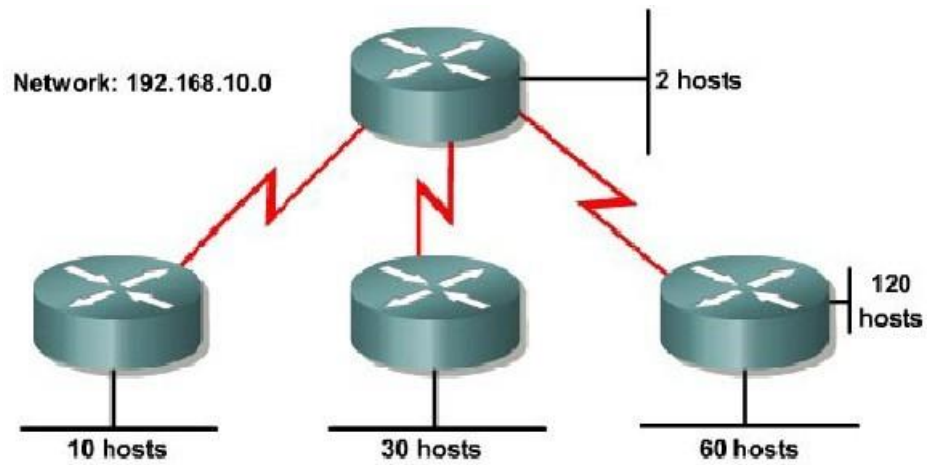
Exercise For independent work

Design the following four networks according to the resulting variant. See Figs. 4, 5, 6, and

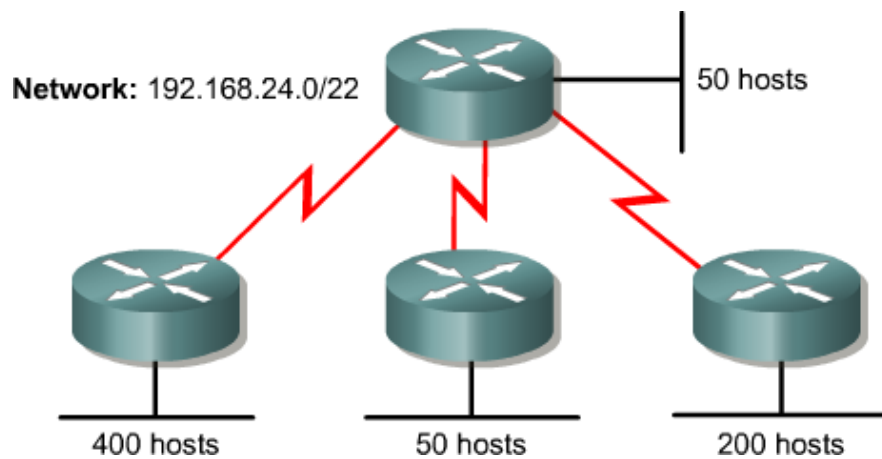
7.



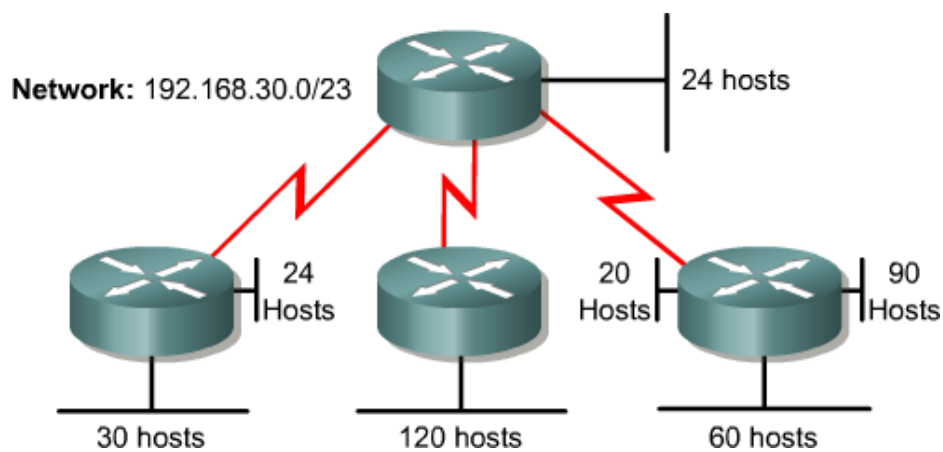
Rice 4. Option 1.



Rice 5. Option 2



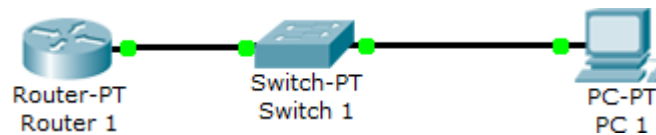
Rice 6. Option 3.



Rice 6. Option 4.

Order solutions options

1. In the designer, select the correct routers with the required number and type of interfaces. Use multi-slot devices with a scalable number of interfaces. In the simulator, they have addresses like Ethernet 2/0, which means interface 0 in slot 2.
2. Create a topology. Local network  ,  is presented as a switch with one computer



3. . Do it screenshot topology.
4. Assign each subnets correct mask With minimal number zeros. Remember that the mask for a serial connection is /30.
5. Make up your mind, which addresses You you will be assign on network interfaces routers and computers.
6. Apply V graphic editor on yours topology appointed addresses and masks.
7. IN simulator appoint addresses on network interfaces routers and computers.
8. Check it out right appointments addresses teams **show IP interface brief** (router) or **ipconfig** (computer).
9. Configure dynamic routing using RIP version 2 on each router .
10. On each router withdraw table routing And do it screenshot.
11. You should ping from any computer any another computer.
12. Optionally, you can use loopback interfaces in routers for modeling local area networks with their subsequent replacement with an Ethernet interface connecting the router to one computer via a switch.

Content report.

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

1. Screenshot topology, created at execution practical part.
2. Configurations of all routers from .txt files created during the practical part.
2. Screenshot topology yours options With addresses and masks.
4. Configurations of all routers from .txt files created during the independent work assignment.
5. All screenshots, specified V task For independent work

Laboratory Job No. 6. Lists management ACL access

Theoretical Part.

Access control list (access control list ACL) is a sequential list of rules, which are used for permissions or flow ban Packets within the network are permitted based on the information contained within the list. Without an access list, all packets within the network are permitted without restrictions to all parts of the network. An access list can be used to control the distribution and receipt of information about route table changes and, most importantly, to ensure **security** . Security policy, in particular, includes protection from external attacks, access restrictions between organizational departments, and network load balancing.

An access list allows a router to be used as a firewall to block or restrict access to an internal network from an external network, such as the internet. A firewall is typically placed at the connection points between two networks.

Standard ACL

When using standard ACL, the only criterion for determining whether that the package is allowed or prohibited, is IP address source of this package. Format element list access next

Router(config)#access-list No permit | deny source-address source-mask,

where No. is An integer is the access list number; source-address denotes the packet's source address; source-mask is the inverse mask applied to the address; permit allows the packet to pass; deny denies the packet to pass. The number # determines whether the access list element belongs to a specific access list with the same number. First access-list command defines the first element access list, the second command defines the second element of the access list, and so on. The router processes each access list defined in it, element by element, from top to bottom. That is, if the address If a packet's source address, taking into account the mask, satisfies the condition of a list element, the router does not process further list elements. Therefore, to avoid unnecessary processing, elements defining more general conditions should be placed at the beginning of the list. Multiple access lists can be defined within a router. The standard list number must be in the range 1–99. The mask in an access list is specified in inverse form; for example, a mask of 255.255.0.0 becomes 0.0.255.255.

Cisco routers assume that all addresses not explicitly mentioned in the access list are denied. This means there is an invisible element at the end of the access list.

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 other traffic, it is enough to place one element in the access list

```
Router(config)# access-list 77 permit 1.1.1.1 0.0.0.0.
```

Here supposed, What We organized list access With number 77.

Let's consider the possibility of using standard access lists for a range of addresses. Let's take the range 10.3.16.0 – 10.3.31.255 as an example . To obtain the inverse mask, you can subtract the lower address from the higher address, resulting in 0.0.15.255. Then An example of a list element can be specified with the command

```
Router ( config )# access-list 100 permit 10.3.16.0 0.0.15.255
```

For to ensure that the access list started to do its job it must be applied to the interface using the command

```
Router(config- if)# ip access group access list number in either out
```

list can be applied either as an input (in) or as an output (out) access list. When you apply an access list as an input access list, the router receives the input packet and compares its input address with the list elements. The router allows the packet to be routed to the destination interface if the packet satisfies the permit elements of the list, or discards the packet if it matches the deny elements of the list. If you apply an access list as an output access list, the router receives the input packet, routes it to the destination interface, and only then processes the packet's input address according to the elements. list access this interface. Next router or permits пакету покинуть интерфейс либо отбрасывает его согласно разрешающим и запрещающим элементам списка соответственно. Так, созданный ранее список с номером 77 applied to the router's Ethernet 0 interface as an input list by commands

```
Router(config)# int Ethernet 0
```

```
Router(config- if)# ip access group 77 in
```

The same list is applied to the router's Ethernet 0 interface as an output list using the commands

```
Router(config- if)# ip access group 77 out
```

Canceled list on interface With help **no** commands

```
Router(config- if)# no IP access group 77 out
```

Let's get started To creation more complex lists access. Let's consider network in the picture 1. Allow all packets coming from network 10.1.1.0 /25 (10.1.1.0 255.255.255.128), but deny all packets originating from network 10.1.1.128 /25 (10.1.1.128 255.255.255.128). We also want to deny all packets originating from the 15.1.1.0/24 network (15.1.1.0 255.255.255.0), with the exception of packets from a single host with the address 15.1.1.5. We allow all other packets. We'll give the list number 2. The sequence of commands to accomplish this task will be as follows.

```
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 is performed by the last element of **access-list 2 permit 0.0.0.0 255.255.255.255**.

Let's make sure, What We completed delivered task.

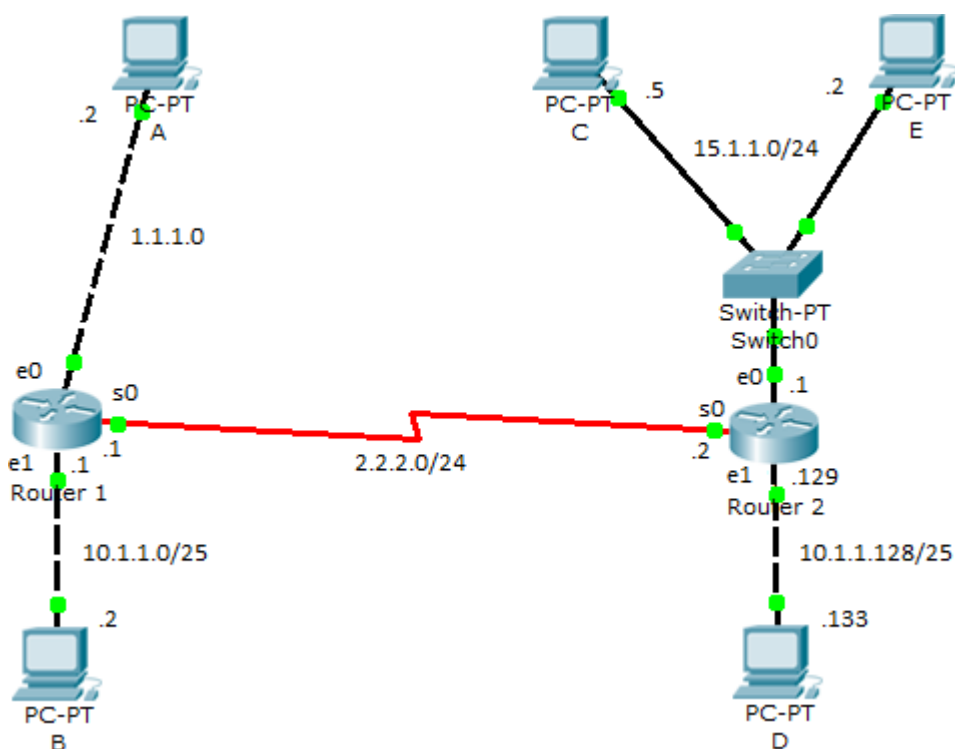
1. Allow All outgoing packets from networks 10.1.1.0 255.255.255.128.

The last line in the access list satisfies this criterion. There is no need to explicitly permit this network in our access list, since there are no lines in the list that match this network except for the last permit 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 meets this criterion. It's important to note the inverse mask 0.0.0.127 for this network. This mask indicates that we shouldn't consider the last seven bits of the fourth octet of the address, which are assigned to addressing on this subnet. The mask for this network 255.255.255.128, which says that the last seven bits of the fourth octet define the addressing on this network.

3. Deny all packets originating from the network 15.1.1.0 255.255.255.0, except packets from the single host with the address 15.1.1.5



Drawing 1.

This requirement is satisfied by the second and third lines of our access list. It's important to note that the access list implements this requirement in a different order than it does in the previous section. defined. Necessarily it should be remembered, What access list is processed from top to bottom, and upon the first match, packet processing stops. We first request that all packets originating from the 15.1.1.0 255.255.255.0 network be denied, and only then are the packets allowed. With address 15.1.1.5. If V teams, defining list access We,

If we swap the second and third teams, then the entire network 15.1.1.0 will be denied until host permission is granted 15.1.1.5. That is, the address 15.1.1.5 immediately. At the beginning it will be prohibited by a more general 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 three teams.

Like this in this way, we have next subsequence actions For access list implementations.

1. Define criteria And restrictions For access.

2. Implement them using the access-list commands , creating an access list with a specific number.

3. Apply list To certain interface or How incoming, or as outgoing.

Let's focus on the last point. In general, the standard access list should be placed as close to the destination as possible, rather than the source of the packets. There may be exceptions, though. Since the standard access list only works with source addresses, detailed configuration isn't always possible. Efforts are required to avoid this. unwanted access configurations. If the list is placed near the packet source, it is highly likely that access to devices on which no access configuration is implemented will be hindered.

Let's specify the security policy for the network in Figure 1. Our goal is to create a policy for computer A (address 1.1.1.2 network 1.1.1.0/24), which from all the devices of the local network 15.1.1.0/24, which includes computer C (15.1.1.5), will allow access to computer A only to computer C itself. We also want to create a policy that prohibits remote access To computer A from any devices local networks

10.1.1.128/25 of computer D (10.1.1.133). We allow all other traffic. In Figure 1, computer PC5 (15.1.1.5) plays the role of an arbitrary representative of the local network 15.1.1.0/24, different from computer C.

List placement is critical to enforcing this policy. Let's take the previously created list number 2. If we make this list an output on the serial interface of Router 2, the task for computer A will be completed, but traffic between other local networks will be restricted. A similar situation occurs if we make this list an input on the serial interface of Router 1. If we place this list as an output on the Ethernet A interface of Router 1, the task will be completed without any side effects.

Extended ACL

With a standard ACL, you can only specify the source address, and the mask is optional. With extended ACLs, you must specify both the destination and source addresses. With masks. You can add additional protocol information For

source and destination. For example, for TCP and UDP, you can specify the port number, and for ICMP, you can specify the message type. As with standard ACLs, you can log using the log option .

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), neq (not equal), gt (greater than), lt (less than), range (two ports are specified to define the range).

As with standard ACLs, an extended ACL must be bound to an interface. or for traffic incoming to the interface

Router(config- if)# IP access group №ACL in

or For coming out from traffic interface

Router(config- if)# IP access group №ACL about ut

the ACL number - number list.

Examples elements extended ACL Allow

SMTP from anywhere to 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 set up rights access.

Named ACL

Named ACLs are referenced by name rather than by number, which provides clarity and ease of reference. To create a named ACL, use the command

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 .

The name of a named list is case-sensitive. The commands for creating an unnamed list are similar to the commands for creating numbered list items, but the creation process itself is different. You must use the keyword IP before the main one ACL operator and thus enter configuration mode specifically for this named list. In this mode, you start with keywords permit or deny and do not have to enter access-list at the beginning of each line.

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 at the top of the list. As soon as a packet being processed by the list satisfies an element of the list, processing of that packet stops. Standard ACLs should be placed closer to the destination where the traffic should be filtered. Outbound (out) extended ACLs should be placed as close as possible to the source of the packets being filtered, and ingress should be placed closer to the destination where traffic must be filtered.

Named ACLs allow you to edit them. To do this, you need to run the command that was used to create them.

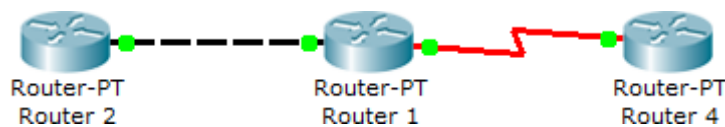
Router(config)# IP access list extended ACL_name

Use the vertical arrow keys to find the list row you want to change. Edit it using the horizontal arrow keys. Press Enter. The new row will be added to the end of the list. The old row will not be deleted. To delete it, enter no. at the beginning of the line.

To edit numeric ACLs should be destroyed and recreated, or the list should be modified offline and loaded into the device using.

Practical Part.

1. Let's load it V simulator topology, depicted on drawing 2.



Drawing 2.

Let's assign addresses to the interfaces (mask 255.255.255.240) according to the table. Not forget to set the clock on the DCE serial device.

	Router2	Router1	Router4
Ethernet	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

Ha Router2

Router2(config)#router rip

Router1(config-router)#version 2

```
Router2(config-router)#network 24.0.0.0
```

и на 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 can ping the Ethernet0 interface (24.17.2.2) of Router 2 from 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 on router 2 commands

```
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
```

Applicable list To interface Ethernet router 2 Router2(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 working configuration

```
Router2# show running- config
```

We Also Can see, What list applied To interface, using show command IP interface ”.

Find the line “ Innbound ” in the output. 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 attempting to ping the Ethernet0 interface (24.17.2.2) of router 2 from router 4

```
Router4# ping 24.17.2.2
```

Type escape sequence to abort.

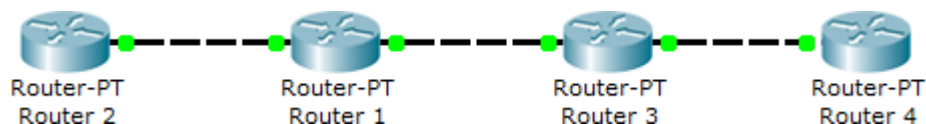
Sending 5, 100-byte ICMP Echos to 24.17.2.2, timeout is 2 seconds:

```
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 works correctly.

2. Let's create And let's load V simulator topology on drawing 2,



Drawing 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
```

Для Router2

```
Router2(config)#router ospf 1
```

```
Router2(config- router)#network 160.10.1.0 0.0.0.255 area 0
```

```
end
```

Для 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
```

Для Router4

```
Router4( config ) # router ospf 1
```

```
Router4(config- router)# network 180.10.1.0 0.0.0.255 area 0
```

For checks ping extreme router2#ping

```
180.10.1.2
```

```
router4#ping 160.10.1.2
```

Let's create a standard access list to filter traffic coming to the interface. ethernet0 1st router router1 And permits traffic from subnets 175.10.1.0 (router3) and blocks traffic from other devices.

```
router1(config)# access-list 1 permit 175.10.1.0 0.0.0.255
```

Check it out, What He

```
router1# show access-list
```

created

```
Standard IP access list 1
```

```
permit 175.10.1.0 0.0.0.255
```

Attach list How input To interface Ethernet 1 router1(config)# **interface**

FastEthernet1/0

```
router1(config- if) #ip access group 1 in
```

Check accession with the router1# **show**

running-config command

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 to be, and between 4 And 2 - No.

Let's change it list access And let's resolve traffic from subnets 180.10.1.0 (router4) and block traffic from other 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 router1# show

access-list changed

```
Standard IP access list 1
    permit 180.10.1.0 0.0.0.255
```

Attach list How input To interface Ethernet 1 router1(config)# **interface FastEthernet1/0**

```
router1(config- if) #ip access group 1 in
```

Check accession with the router1# show

running-config command

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 to be, and between 3 And 2 - No.

3. Make it happen And check configuration IP For networks on drawing 1 And Use OSPF to implement dynamic routing.

For router router 1 router1(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 router 2 Router2(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 the network's functionality: you should be able to ping any interface from any device. Or, more simply, all computers A, B, C, D, and PC5 should be able to ping each other in pairs .

Let's create list access from theoretical parts

3.1 On router router 1 let's create 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 output

```
router1(config)# interface FastEthernet0/0
```

```
router1(config- if)# ip access-group 2 out
```

Create screenshot result execution router1# **show access-list commands**

Let's ping A, B, C, PC5, D in pairs . The result should be as follows access 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 interface e0 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**

Let's ping A, B, C, PC5, D in pairs . The result should be as follows access matrix

From\To	A	B	C	E	D
A	+	+	+	-	-
B	+	+	+	-	-
C	+	+	+	+	+
E	-	-	+	+	+
D	-	-	+	+	+

Table 2

We see that traffic between networks 10.1.1.0/25 and 10.1.1.128/25 is now blocked. Traffic between network 10.1.1.0/25 and network 15.1.1.0/24 is also blocked, with the exception of computer C with address 15.1.1.5.

4. We use topology And configuration point 1 this laboratory Let 's cancel the access configuration made in point 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**

Applicable 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 Allow only telnet from the serial connection subnet 24.17.2.16/240 to enter 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 list access.

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 installation 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 router1(conf

)#interface **Serial2** /0 packets

router1(conf-if)# **ip access-group 101 in**

router1(conf-if)# **interface fa0/0**

router1(conf-if)# **ip access-group 102 in**

For checks, What EACL are present on interfaces, use router1# **show running-config command**

or

router1# **show IP interface**

Let's check functioning EACL. Let's join to router4 And L e t ' s

t r y to ping the Serial2/0 interface on router1 without success.

router4# **ping 24.17.2.17**

EACL number 101 blocked ping. But must allow telnet router4#

telnet 24.17.2.17

Success. Enter the password for router1. The prompt for router4# has changed to router1>.

Press ctrl-shift-6 and then 6 to return to router4. The log will indicate that EACL 101 was triggered on router1.

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 connection router4#

show sess

router4# **disconnect 1**

Let's join to router2 And We'll see, Can whether We ping Serial0 interface on router4.

Router2# **ping 24.17.2.18**

Why unsuccessfully? Plastic bag starts V Router2, is coming through Router1 (O The log will tell us when EACL 102 is triggered on router1

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 reorganized and sent back to Router1. When Router4 reorganizes the packet, the source address becomes the destination address, and the destination address becomes the source address. When the packet arrives at the Serial0 interface on Router1, it is rejected because its source address is equal to the IP address of the Serial0 interface on Router4 (24.17.2.17), and only tcp is allowed here .

Let's join to router2 And We'll see, Can whether We ping Ethernet0 interface on router1.

```
router2# ping 24.17.2.1
```

Successfully. Likewise And For telnet

```
router2# telnet 24.17.2.1
```

EACL they work successfully. O EACL triggering 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 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 in
```

```
router1(conf-if)# interface Ethernet0
```

```
router1(conf-if)#no ip access-group 102 in
```

и отменим на router1 EACL

```
router1(conf)#no access-list 101
```

```
router1(conf)#no access-list 102
```

Let's set the task of prohibiting only pings from the entire network router4 to router2. Access list can be arrange and on router1 And on router2. Although It is recommended to place the ACL closer to the source (to reduce traffic), in this example we will place a named list called 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
```

The first command specifies that we are creating a named extended access list called deny_ping . The second command specifies that we are denying ICMP traffic with a source address of strictly 24.17.2.18 and a destination address of strictly 24.17.2.2. The third team allows other IP traffic.

Let's check Creation list

```
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)
```

All Right, We we see V first line Just another form deny command representations 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 router2 Router2(conf)#

```
interface Ethernet0
```

```
Router2(conf- if)# ip access-group deny_ping in Let's
```

join To router4 And let's ping router 2 router4# ping

```
24.17.2.2
```

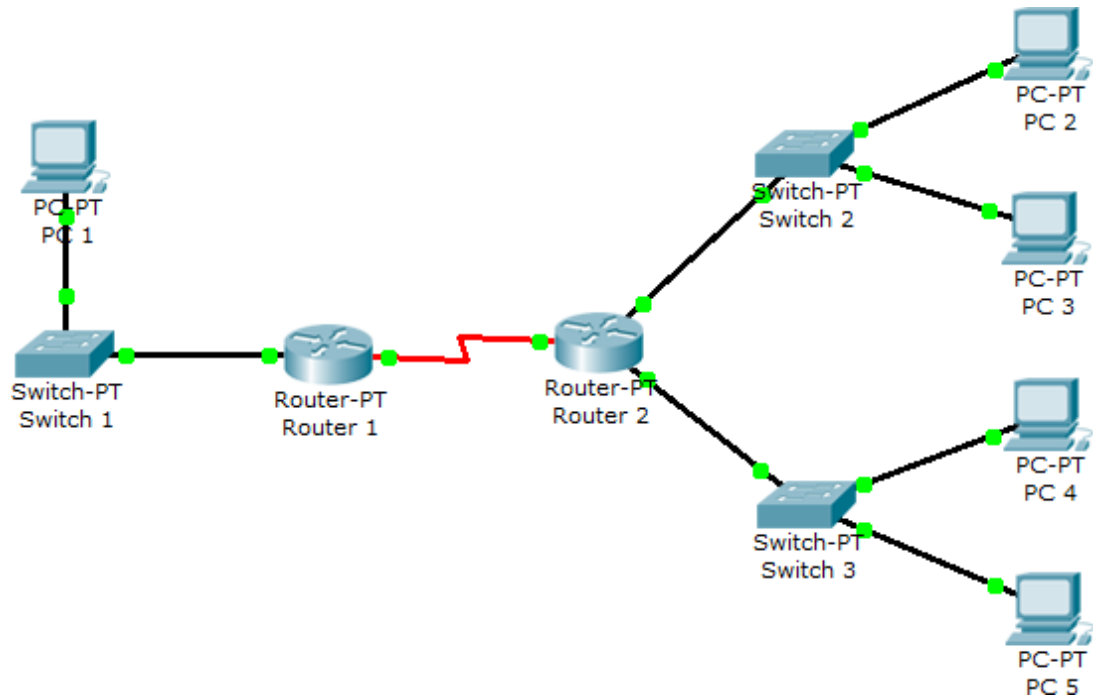
Failure. Let's join To router1 And let's ping router2 Router1# **ping**

24.17.2.2

Success. Let's join To router2 And We'll see on two separate Log messages: the first one is about disabling ping from router4 and the second one is about allowing 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 complex questions extended lists access. Let's create a topology



Drawing 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 PC4 and PC5 to the local network of PC1 and denies traffic from the local network of PC2 and PC3 to the local network of PC1. Since the traffic comes from router2 to router 1, we should place an access list on the serial2/0 interface of router1 for incoming 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 command directly solves the task at hand, and the second one enables broadcasting of RIP protocols. Let's check the 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
```

To test the access list, try pinging PC1 from PC2, PC3, PC4 and PC5.

PC# Ping 1.1.3.2

Pings won't work for PC2 and PC3 . Pings will work for PC4 and PC5 . The access list is working. Check the 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 creating

```
Router2# show access
```

```
list
```

```
Extended IP access list 101
  deny ip host 1.1.1.130 host 1.1.1.3
  permit ip any any
```

Let's apply list access To fast Ethernet interface router2 Router2(conf)# interface

```
FastEthernet0/0
```

```
Router2(conf- if)# ip access group 101 in
```

Join us To PC2 And check, What You Not you can kick PC5 PC2# 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 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 the local network of computers. PC2 and PC3. Since we're blocking all traffic, we'll use the 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 log

Router2(conf)#access-list 102 permit ip any any

Let's check creating

Router2# **show access**

list

```
Extended IP access list 102
  deny ip 1.1.1.128 0.0.0.127 host 1.1.3.2
  permit ip any any
```

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 provide a log on the Router2 console. But you can see the effect like this.

```
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 see that after each unsuccessful ping the number of traced (matched) packets increases.

Control questions

1. What such ACL?
2. Which address is criterion For permissions/prohibitions package?
3. Where Are ACLs applied ?
4. How ask element ACL And What such inverse mask?

5. How router processes elements ACL?
6. Which element Always implicitly present V 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 To interface.
11. What filter extended ACL?
12. Which one? additional functionality have extended ACL compared to standard ones?
13. Can whether, using advanced ACL, impose restrictions on traffic to a specific 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. What is the difference in the command formats for entering numeric and named ACL elements?

Order execution And surrender work

1. 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 to table 1, and then table 2.
4. Show to the teacher, What net satisfies matrix access from Table 1.
5. Show to the teacher, What net satisfies matrix access from Table 2.
6. Do it V Packet Tracer exercise For independent work.
7. Construct your own access matrix according to the option and show the teacher that the network satisfies this matrix.
8. Make out report. Content report Look below.
9. Protect report.

Exercise For independent work

1. Apply access list 2, created in paragraph 3 of the practical part, according to the option

Va riant	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 commands

router1# **show access-list**

And

router1# **show running- config**

3. Build matrix access.

4. Do it three subparagraph point 6 practical parts For topology in Figure 4 and its version v configuration given in the 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 point 6 practical part.

Content report.

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

1. Screenshots topologies, created at execution practical part.
2. All screenshots, created at execution practical parts.
3. Configurations everyone routers from .txt files configurations, created when completing the practical part.
4. Configuration routers from .txt files, created at execution point 1 of the assignment for independent work.
5. Matrix access, specified V point 3 tasks For independent work.
6. Configuration routers from .txt files, created at execution point 4 of the assignment for independent work.
7. All screenshots, specified V task For independent work.

Laboratory Job No. 7. Transformation network addresses NAT

Theoretical Part

Network address Network Address Translation (NAT) is designed to simplify and conceal IP addressing. NAT allows the external world to perceive a company's internal IP addressing structure differently than it actually appears. This allows an organization to connect to the Internet without having a globally unique IP address within itself. This provides Internet access for corporate internal IP networks. With internal IP addresses (intranet), which are not globally unique and therefore cannot be routed on the Internet. NAT is also used to connect geographically distributed divisions of an organization over the Internet.

address ranges have been allocated by the global community for Intranet addressing:

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 an internal IP address from the internal address space to an IP address in the external address space. When NAT receives a packet from the intranet , it modifies the source address, recalculates the checksum, and sends it to the Internet.

NAT translates and maps addresses from one domain to another. This ensures transparent routing from host to host. NAT uses several address translation methods, each used in a specific situation.

Cisco uses specific terminology for NAT for hosts on the intranet and the Internet both before and after address translation:

Interior (inside) address. Address, used V organizations. Different Organizations may have the same internal addresses.

External address (outside). Address, defined somewhere outside the given organization. The external address of another organization may coincide with the internal address of this organization.

Global address. This is a registered and legal IP address that can pass through Internet.

Local address. An IP address used internally on an intranet . These addresses do not overlap with Internet addresses and are therefore considered local.

Internal local address (inside local). An address used within an organization that does not cross Internet addresses.

Internal global address (inside global). An address used within an organization that is an Internet address.

External local address (outside local). Address, defined somewhere outside of this organization, which is not an Internet address.

External global address (outside global). Address, defined somewhere outside the given organization, which is an Internet address.

Simulator always shows that External local address (Outside Local) is always equal external global address (outside global).

When sending packets from an internal host interface, NAT replaces the source address with a global address. When receiving a response packet, NAT replaces the global destination address (the address of the local router's external interface) with the address of the internal host interface. For this replacement, the router maintains special address translation tables that are constantly updated. There are three address translation methods: static, dynamic, and overload . With static NAT, internal_address - global_address pairs are explicitly specified using IOS commands . With dynamic translation, global addresses are taken from a defined pool of external addresses. With overload, all internal addresses subject to translation are replaced with a single global address on the router's external interface.

For configuration NAT should be defined on the router as internal and external networks using **ip commands nat inside | outside** . This command is defined at the interface level, that is, in the context of **the interface command** . Additional commands depend on the NAT type used. This can include setting static NAT, defining a pool of external addresses , or specifying a command for overloading. Typically, an ACL should also be specified to define the internal traffic to be translated. The ACL itself does not perform any NAT translation.

Let us also dwell on overloading, which is usually called PAT (Port Address Translation). PAT allows multiple internal hosts to share a single global address. One implementation option PAT is based on use sequences free TCP And UDP ports and is as follows.

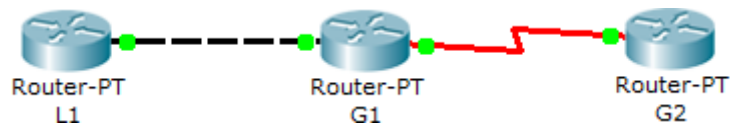
The NAT service is located on router M with internal global address X. Let there be a packet P from internal local address Yi and port Pi To external address G and port p. The packet passes through router M. NAT replaces the source address Yi and source port Pi of the internal host with a unique pair X:Pinew , where Pinew is the next available port number. The line (Yi:Pi , X: Pinnew , G:p) is entered to the NAT table router M. The response packet will contain X in the destination address field, and Pinew in the destination port field . The address: source port field will contain G:p . Router M values X, Pinev , G, p finds V his own NAT table line (Yi:Pi , X: Pinev , G:p) and replaces the receiver address X in the packet with Yi , and the destination port Pinew with Pi . The response The packet will arrive at the correct address Yi with the correct destination port Pi . The Pinew port is returned to the list of free ports.

NAT process transparent to internal addresses. So host With internal address Yi sent plastic bag in external world And received answer "Not guesses", What plastic bag

passed NAT translation on the router is performed on both sending and receiving data. The internal host appears to have direct access to the outside 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 on G1 G1(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**

Ha L1

L1 (config)#**router ospf 1**

L1 (config- router)#**network 10.10.1.0 0.0.0.255 area 0**

Для G2

G2 (config)#**router ospf 1**

G2(config- router)#**network 175.10.1.0 0.0.0.255 area 0**

On G2 solvable entrance by telnet with password

G2 G2 (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 - connection from L1 (10.10.1.2) to G2

L1# **telnet 175.10.1.2**

Password: **G 2** 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 using the disconnect command on L1 and G2.

You need to configure NAT/PAT on router G1. Three forms need to be configured translation addresses: statistical translation network addresses, dynamic translation and overload (translation addresses ports). We assume, What net Ethernet 10.10.1.0/24 This

internal intranet network , which connects to the outside world via G1, namely via the 175.10.1.0/24 serial interface network.

1.1 On router G1, we will configure NAT for static translation of the internal local L1 Router Ethernet Addresses 10.10.1.2 V new internal global address 169.10.1.2, held by the organization:

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 serial2/0 interface How external

G1(config-if)# interface s2/0

G1(config-if)#ip nat outside

For conclusion tables translations addresses enter team on router G1# **show ip nat**

translations

Pro	Inside global	Inside local	Outside local	Outside global
---	169.10.1.2	10.10.1.2	---	---

Check it out translation, created Telnet connection from L1 To G2. Entering By Telnet on G2 enter the show command users . You should see the translated IP address 169.10.1.2.

L1# telnet 175.10.1.2

Password: **G 2**

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 Serial2/0 G1 interface 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 remove router G1 previous NAT command statistical translation

G1(config)# **no IP nat inside source static 10.10.1.2 175.10.1.1**

and configure NAT to dynamically translate the L1 router's Ethernet address. We'll use an address range of 169.10.1.50 - 169.10.1.100. Let's define the address pool **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 transformed

G1(config)# **access-list 1 permit 10.10.1.0 0.0.0.255**

^Z

G1# **Show access- list**

Required using the show command running-config check that router G1 has picked up the commands entered. The output should include

```
!
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. Telnet into G2 enter the show command users . You should see the translated IP address 169.10.1.50.

L1# **telnet 175.10.1.2**

Password: **G 2**

G2> **show users**

	Line	User	Host(s)	Idle Location
★	0 con 0		idle	00:00:00
★	1 vty 1		idle	169.10.1.50

That There is NAT took from pool addresses first free address 169.10.1.50.

To display the address translation table, enter the show command. IP nat translations 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, remove the previous dynamic translation NAT commands and configure forwarding (port address translation) of the L1 router's Ethernet address (10.10.1.2) to the serial2/0 interface address (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**

Required using the show command running-config check that router G1 has picked up the commands entered. The output should include

```

!
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. From router G2, enter the show command users . You should see the translated IP address 175.10.1.1.

L1# **telnet 175.10.1.2**

Password: **G 2**

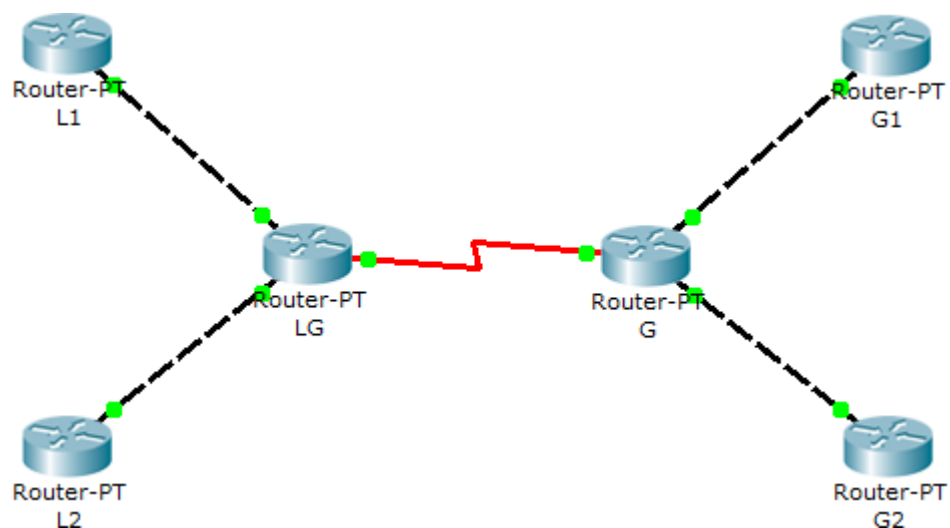
G2> **show users**

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:34	
* 67 vty 0		idle	00:00:00	175.10.1.1

Take it out list 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 a topology. Router models L1, L2, G1 and G2 are 805, and LG and G are 1605.



Drawing 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		

Configurable routing OSPF 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 solvable 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 the functionality: telnet from L1 to G1, from L1 to G2, from L2 to G1, from L2 to G2.

Necessarily kill All telnet sessions **disconnect** command **1** . Total to you You will need 8 commands. Two for 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 network 1.1.1.0/24 as external

```
LG(config)#interface s2/0
LG(config-if)#ip nat outside
LG(config-if)#interface fa0/0
LG(config-if)#ip nat inside
LG(config-if)#interface fa1/0
LG(config-if)#ip nat inside
```

Let's create list access For addresses two internal Ethernet LG networks (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 it out functioning: come in telnet from L1 on G1 L1# **telnet**

1.1.2.2

Password: **G 1**

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.

Telnet from L1 to G2

L1# **telnet 1.1.3.2**

Password: **G 2**

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 device L2. Come in telnet from L2 on G1 L2#

telnet 1.1.2.2

Password: **G 1**

G1> **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.

Telnet from L2 to G2

L2# **telnet 1.1.2.2**

Password: **G 2**

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 see And on G1 And on G2 By two telnet sessions. All four sessions shown as sessions from one address - internal global address 1.1.1.1 of interface Serial2/0.

Let's move on on LG. Let's see four broadcasts LG# **show** addresses

IP nat tr

Pro	Inside global	Inside local	Outside local	Outside global
icmp	1.1.1.1:9392	10.1.1.2:9392	1.1.2.2:9392	1.1.2.2:9392
icmp	1.1.1.1:9393	10.1.1.2:9393	1.1.2.2:9393	1.1.2.2:9393
icmp	1.1.1.1:9394	10.1.1.2:9394	1.1.2.2:9394	1.1.2.2:9394
icmp	1.1.1.1:9395	10.1.1.2:9395	1.1.2.2:9395	1.1.2.2:9395
icmp	1.1.1.1:9396	10.1.1.2:9396	1.1.2.2:9396	1.1.2.2:9396
icmp	1.1.1.1:9392	10.1.1.2:9392	1.1.3.2:9392	1.1.3.2:9392
icmp	1.1.1.1:9393	10.1.1.2:9393	1.1.3.2:9393	1.1.3.2:9393
icmp	1.1.1.1:9394	10.1.1.2:9394	1.1.3.2:9394	1.1.3.2:9394
icmp	1.1.1.1:9395	10.1.1.2:9395	1.1.3.2:9395	1.1.3.2:9395
icmp	1.1.1.1:9396	10.1.1.2:9396	1.1.3.2:9396	1.1.3.2:9396
icmp	1.1.1.1:9392	10.1.2.2:9392	1.1.2.2:9392	1.1.2.2:9392
icmp	1.1.1.1:9393	10.1.2.2:9393	1.1.2.2:9393	1.1.2.2:9393
icmp	1.1.1.1:9394	10.1.2.2:9394	1.1.2.2:9394	1.1.2.2:9394
icmp	1.1.1.1:9395	10.1.2.2:9395	1.1.2.2:9395	1.1.2.2:9395
icmp	1.1.1.1:9396	10.1.2.2:9396	1.1.2.2:9396	1.1.2.2:9396
icmp	1.1.1.1:9392	10.1.2.2:9392	1.1.3.2:9392	1.1.3.2:9392
icmp	1.1.1.1:9393	10.1.2.2:9393	1.1.3.2:9393	1.1.3.2:9393
icmp	1.1.1.1:9394	10.1.2.2:9394	1.1.3.2:9394	1.1.3.2:9394
icmp	1.1.1.1:9395	10.1.2.2:9395	1.1.3.2:9395	1.1.3.2:9395
icmp	1.1.1.1:9396	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 command L1#

telnet 1.1.2.2

Second portion broadcasts corresponds command L1#

telnet 1.1.3.2

Third portion broadcasts corresponds team

L2# telnet 1.1.2.2

The fourth portion broadcasts corresponds command L2#

telnet 1.1.3.2

In everyone cases is used interior global address 1.1.1.1 interface Serial2/0.

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 such 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 on a network that has a connection to the outside world via NAT versus host with global address?

Order execution And surrender work

1. Study theoretical And practical part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute contract All points practical parts.
4. Create All screenshots, given V practical parts.
5. Show the teacher the result of the last command **show IP nat tr** from points 1 and 2 of the practical part.
6. Do it V Packet Tracer exercise For independent work.
7. Show the teacher the result of the last command **show IP nat tr** from points 1 and 2 of the assignment 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 your own version of v configuration given in the 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

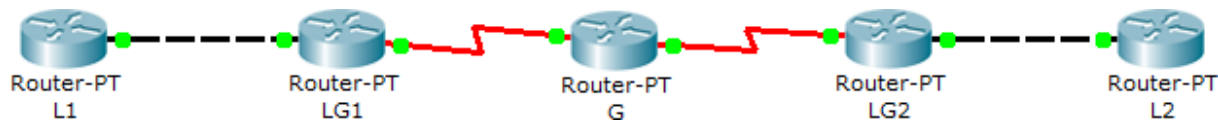
Do it those same screenshots, which made V point 1 practical part.

2. Do it point 2 practical parts For topology on drawing 2 And your own version of v configuration given in the 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 point 2 practical part.

3.1. Create topology



3.2. Let's configure the addresses according to the table . All masks are 255.255.255.0. v is the variant number.

	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. This simulates a real-world situation where L1 and L2 network devices are from two different companies. have the same local internal addresses 10. v .1.2 and are associated with the outside world (G) through routers LG1 and LG2, which have NAT.

3.3. Allow me access By telnet To router G.

3.4. Give a demonstrable answer to the question: is it possible to set up routing in the simulator like this? NAT so that router L1 (L2) can telnet to router G under the global internal address 1.v.1.2 (1.v.2.2) . Provide your answer (positive or negative) with the contents of the .rtr files and screenshots.

Content report.

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

1. Screenshots topologies, created at execution practical part.
2. All screenshots, created at execution practical parts.
3. Configurations everyone from .txt files, created at execution practical part.
6. Configuration routers from .txt files configurations, created when performing for independent work.
7. All screenshots, specified V task For independent work.

Laboratory Job No. 8. Remote access. Frame Relay Theoretical Part

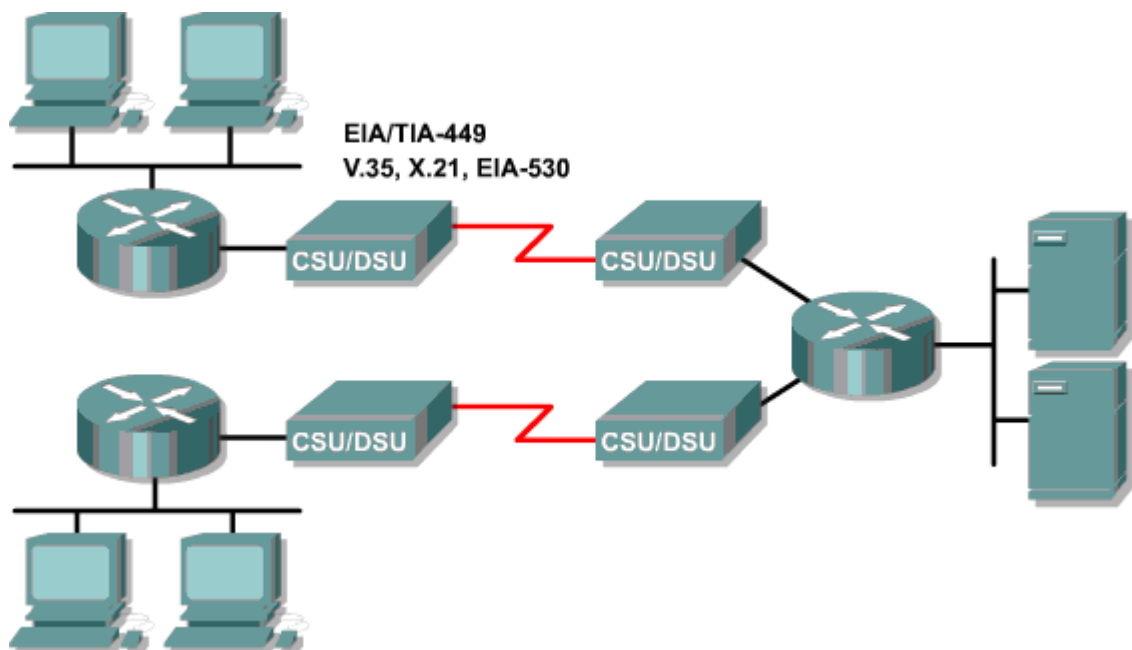
Remote access

There are three type sequential channels connections:

1. Networks With switching channels: dial-up telephone net, ISDN.
2. Dedicated or leased lines: DSL, cable modems and communication lines of the 64k, T1, T3, OS-12 type,
3. Networks With switching packages: Frame Relay , X.25 And ATM.

Data transmission can be either synchronous or asynchronous. Leased dedicated lines typically require a synchronous serial connection.

Each communication line is connected to the serial port of the router by a CSU/DSU (channel service unit / data service unit – channel servicing device/data servicing device).



Drawing 1.

Therefore, in addition to the actual cables from the communications provider, each connection requires a separate synchronous serial port on the router and a CSU/DSU device. As a result, the cost of maintenance several allocated lines sharp is increasing. That's why majority companies find building fully meshed WANs on dedicated lines too expensive.

CSU/DSU is DCE (data communications equipment – data transmission equipment) device. DCE adapts physical interface on DTE (data terminal

equipment – terminal equipment A DTE device is a device that conforms to the rules for transmitting signals in the carrier network. An example of a DTE device is a router.

The CSU/DSU provides modulation, time synchronization and is used to interact with digital transmitting equipment. It is important that The CSU/DSU is used by a router to communicate with a digital channel in much the same way that a PC uses a modem to communicate with an analog telephone channel. That is, In the PC-modem connection, the PC is a DTE device, and the modem is a DCE device.

Selected or rented channels

Typically serial connections in networks operate at the following speeds

56 kbps

64 kbps

T1 (1.544 Mbps) standard USA

E1 (2.048 Mbps) European standard E3

(34.064 Mbps) European T3 standard

(44.736 Mbps) US standard

The DTE (router) is connected to the DCE (CSU/DSU) via a synchronous serial port using one of the following standards: EIA /TIA-232 (RS-232), EIA/TIA-449, V.35, X.21, EIA-530.

EIA/TIA-232 is used to connect a DTE (router, PC) to an analog modem (DCE (CSU/DSU)). Released over 30 years ago, it has become a classic. However, It is not acceptable on leased lines for speeds greater than 120 kbps .

The V.35 standard is suitable for higher speeds (over 2 Mbps). It is used to connect a router port to a T1/E1 via a separate CSU/DSU.

Today, for many serial links such as T1, many routers have within itself, the CSU/DSU is integrated into the interface card. That is, there is no need for a separate DCE (CSU/DSU).

Networks With switching packages SKP.

Unlike leased lines and circuit-switched connections, packet switching does not rely on a dedicated, point-to-point connection over the carrier network. Instead, data packets are routed within the carrier network based on the addressing contained in the packet or frame headers, allowing the provider to support multiple customers on the same physical lines and switches.

IN In packet-switched networks, the provider configures its switching equipment to create virtual circuits (virtual circuits (VCs)) to provide end-to-end connections. Virtual chains can be constant or can be built

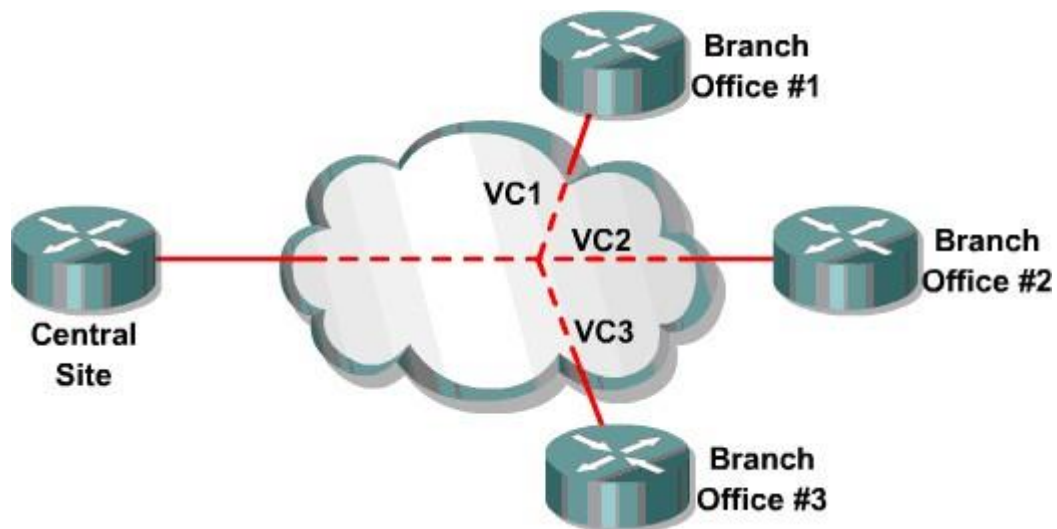
on demand. Frame Relay is a typical packet switching service in a WAN. ATM and X.25 technologies are also frequently used.

First SKP were built using the X.25 protocol. Since X.25 was designed to operate on unreliable telephone copper circuits, then it provides error detection

Investigative Committee This networks With multiple access, using special Equipment for delivering user traffic. The physical carrier of signals within the SCP is typically high-speed dedicated communication channels, most often optical. To ensure the required end-to-end connection within the SCP, switching equipment is configured.

SPCs offer the network administrator less control than point-to-point connections. However, the cost of a virtual circuit in a SPC is lower than that of a dedicated line. Access to the SPC itself is typically via a router's synchronous serial port over a single dedicated T1 or T3 line and allows connection with by many remote websites. At absence Investigative Committee will be required a separate dedicated line to each remote site.

Virtual Frame Chains Relay provides speed up to T3, making packet switching technology a high-speed, cost-effective alternative to leased lines. A single synchronous serial connection to the packet switching network can support multiple virtual circuits in point-to-multipoint (one-to-many) and point-to-point configurations (Figure 2). The process of combining multiple data transmissions on a single physical line is called multiplexing.



Drawing 2.

Multiplexing becomes possible thanks to that, What DTE (How (rule router) encapsulates data in SCP packets containing SKP addresses. ISP switches use these addresses to determine how and where to deliver individual plastic bag. IN in the Frame case Relay these addresses are called DLCI (Data Link Connection

Identifiers). Ability To multiplexing means, What one port A single router, along with a single CSU/DSU, can support dozens of virtual circuits, each leading to a separate site. Consequently, packet switching makes even a fully meshed topology affordable .

Frame Relay does not correct errors and is well suited for work on highly reliable digital transmission channels.

Frame Relay does not provide the same level of reliability, flexibility, and security as dedicated lines, which are preferred for mission-critical traffic and high-volume data exchange.

Another popular packet switching technology is ATM (Asynchronous Transfer Mode). ATM This international standard For element-by-element transmission, in which contains information of various types such as data, voice and video are placed into fixed-length cells of 53 bytes. The fixed cell length allows for their processing in hardware, which reduces latency. ATM is designed so that to take advantage of high-speed transmission media E3, T3 and SONET.

Protocols global networks

Routers before how hand over IP packages By channel connections, encapsulate them into frames of the second network layer.

Typical protocols second level global networks:

Point-to-Point Protocol (PPP) – router -to- router and router-to-host communication protocol for synchronous and asynchronous channels.

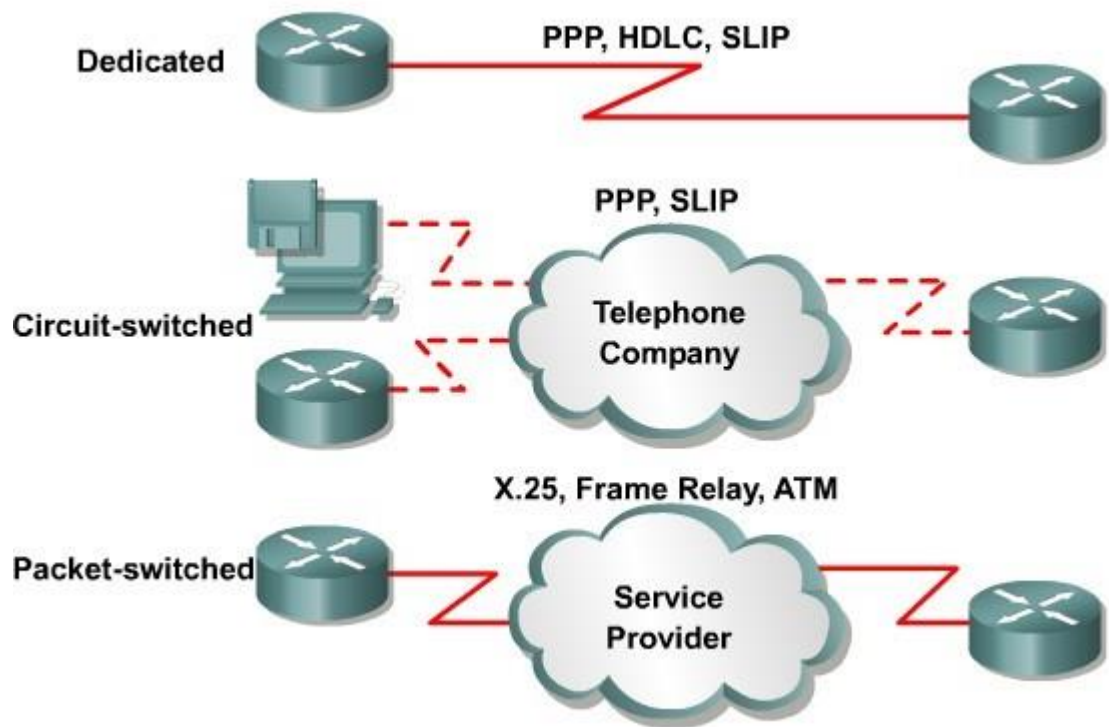
Serial Line Internet Protocol (SLIP) – a predecessor of PPP, used for point-to-point serial connections over TCP/IP.

High-Level Data Link Control (HDLC) is proprietary to Cisco and is used to connect two Cisco devices.

X.25/LAPB is a standard that defines the connection method between DTE and DCE devices. in remote terminal access and computer communications in public data networks.

Frame Relay is a high-performance protocol used on many network interfaces .

The figure shows which data communication protocols are used in each of the three types of WAN connections.



Drawing 3.

Frame Relay

Currently Frame Relay replaces X.25 as a switching technology packages. Standardized in 1990, Frame Relay simplifies data link layer functions and provides only error checking, not error correction. This low-redundancy approach to packet switching increases throughput and efficiency. Modern fiber-optic links and digital transmission services provide significantly fewer errors than their copper predecessors. For this reason, the use of X.25-style reliability mechanisms at the data link layer is now generally considered unnecessary. Error correction is handled by higher-level protocols, such as 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 determine process for transmitting data over a packet-switched network Relay is a connection-oriented data communications technology that is optimized to provide high speed and efficiency.

Modern telecommunication networks are characterized by being relatively error-free digital transmission 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 Frame error correction mechanisms Relay outperforms X.25 in terms of speed. As a result , Frame Relay acceptable For use there, Where required high

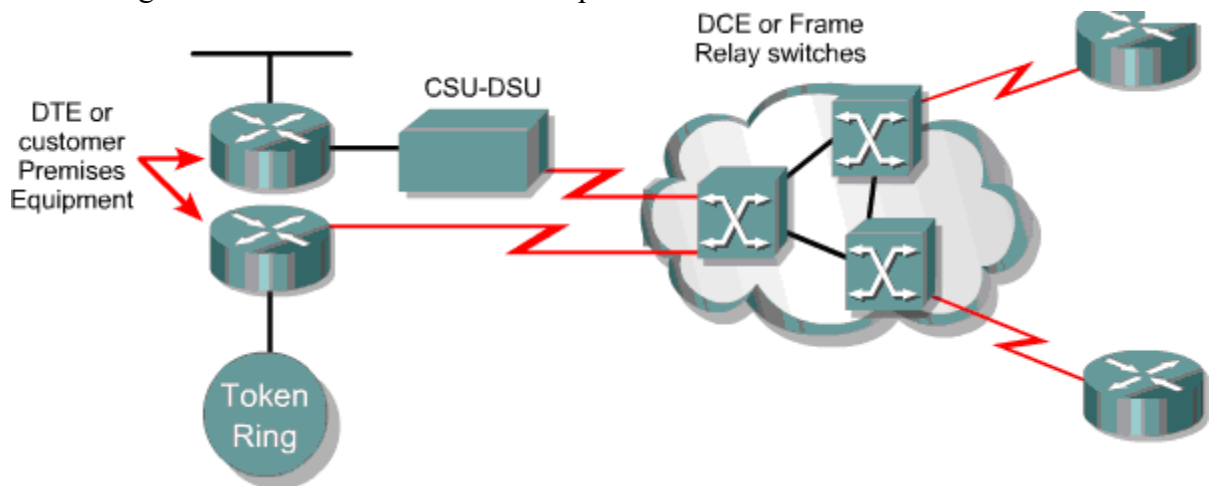
performance as in local area networks. The physical network on which the Frame Relay can be either a public or private network and have a different physical nature: fiber optics, satellite communication channels, leased lines.

Frame Relay defines the process of communication between the client's DTE, such as a router, and the provider's DCE. Once traffic reaches the switch provider, Frame Relay does not define the method by which data is transmitted within a Frame network. Relay . Therefore, the Frame provider Relay can use a variety of technologies, such as ATM or PPP, to move data from one end of its network to the other.

Devices Frame Relay

Devices connected to the global network Frame Relay can be either DTE or DCE devices. DTE devices are considered terminal equipment. and are usually located on the premises of clients - consumers of Frame services Relay . Examples DTE devices are routers And devices access FRAD (Frame Relay Access Devices). FRAD is a special device for communication between LAN and Frame Relay .

Intranet DCE devices are owned by the provider. They provide synchronization and/or packet switching services within the network and provide actual data transmission in WAN.



Drawing 4.

Frame Network Relay is built using Frame switches . Relays acting as DCEs. Within the Frame network Relay can use various data transmission technologies, such as ATM. Physical communication channels are also not regulated - this can be optics, satellite communication channels, leased lines.

Regardless of the technology inside the Frame network Relay , communication between the consumer and the provider Frame Relay is carried out using the Frame protocol. Relay .

Functioning Frame Relay

Typically, the longer the distance a leased line covers, the more expensive the service. Maintaining a fully meshed connection between remote sites using leased lines is prohibitively expensive for many organizations. On the other hand, packet-switched networks provide a way to multiplex multiple logical data transfers over a single physical link. A single connection to the provider's packet-switched network will be less dear, than individual ones highlighted lines between the consumer and each remote site. Packet-switched networks use virtual circuits to deliver packets end-to-end across a shared infrastructure.

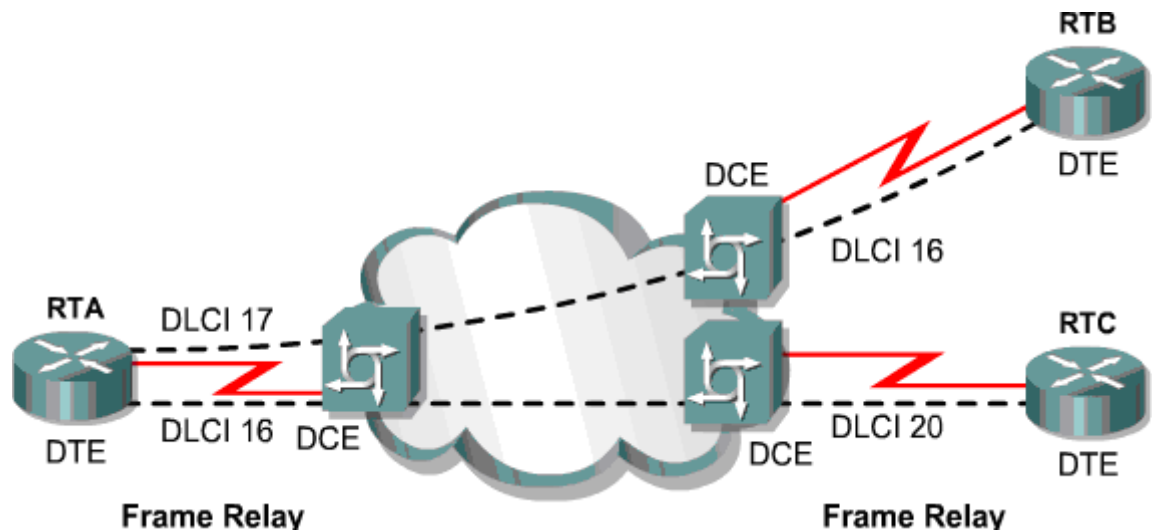
A packet switching service such as Frame Relay requires the consumer to maintain only one circuit, typically T1, to the provider's central office (CO). Frame Relay provides tremendous cost efficiency because one site can connect to many geographically dispersed sites using a single T1 line and a single DCE (CSU/DSU) device to connect to the local central office.

For communication between any two sites, the service provider must install virtual chain between these sites inside networks Frame Relay . Although The fee is for each virtual circuit, and it's small. This is what Frame does. Relay is an ideal technology for creating a fully meshed topology.

Frame Networks Relays support both permanent virtual circuits (PVCs) virtual circuits) So And switched virtual chains SVC (switched virtual circuits). PVC – most typical for Frame Relay PVCs are permanently established connections that are used when Frame networks Relay is stable traffic between specific DTE devices.

SVCs are temporary connections used when there is sporadic traffic between DTE devices. Because they are temporary, SVC connections require setup and termination for each connection. Most providers only support PVCs.

IN Frame Each end of a virtual circuit is assigned a connection identifier. The provider's switching equipment maintains a table mapping these identifiers to output ports. When a frame is received, the switch analyzes the identifier and delivers the frame to the appropriate output port.

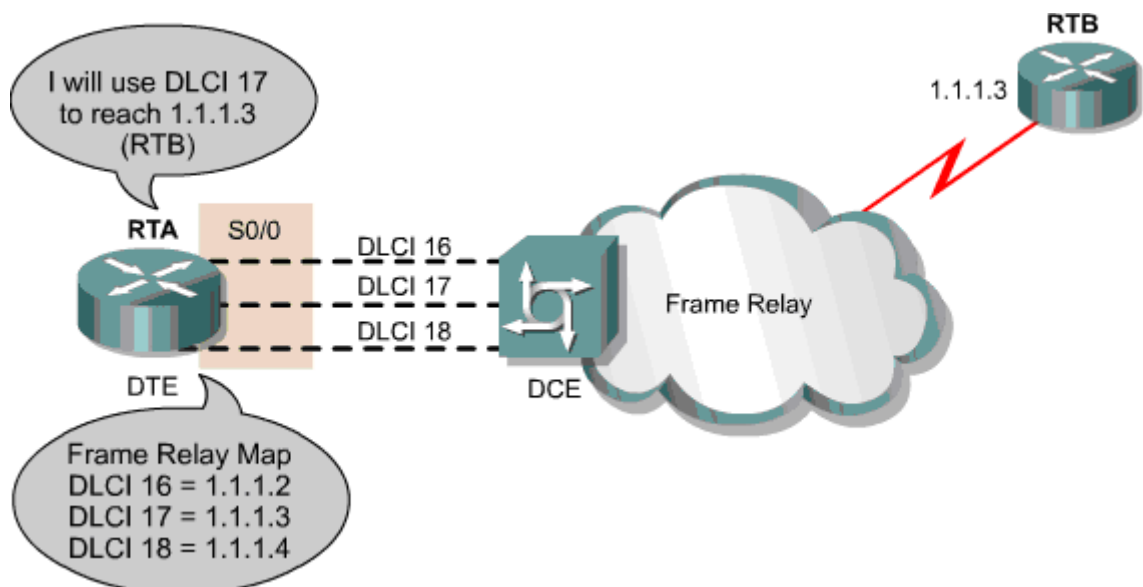


Drawing 5. Frame Relay DLCI

Frame networks Relay such identifier is called DLCI (data-link connection (ID)). They identify the virtual circuit. To create a PVC, the switch uses two DLCIs for each pair of DTE devices (routers).

Two United virtual chain devices DTE can use different DLCI values to refer to the same connection. In Figure 5, the PVC connecting routers RTA and RTB has a DLCI of 17 assigned between RTA and the directly connected switch. DLCI 16 on RTB defines the same The PVC is the connection between the RTB and the directly connected switch. Meanwhile, the RTA uses DLCI 16 to reference the PVC that connects to the RTC.

In order for the RTA router to know which PVC to use at the third network layer, IP addresses must be mapped to DLCI numbers. In the figure, the RTA router must map L3 addresses to available DLCIs.



Drawing 6.

For example, RTA maps the IP address 1.1.1.3 of the RTB router to DLCI 17. Since RTA knows which DLCI to use, it will need to reach the destination the IP packet should be encapsulated into a Frame Relay containing the corresponding DLCI number .

Routers Cisco support two type headings Frame Relay : Cisco And ietf .

First type - For equipment Cisco, second - For devices different manufacturers.

By including the DLCI number in the Frame header Relay , RTA can communicate with both RTB and RTC over a single physical circuit. With this statistical multiplexing, the bandwidth is automatically allocated for active channels. If RTA Not has packets to send to RTB, then RTA can use all available bandwidth to communicate with RTC. With TDM (Time-division multiplexing) In multiplexing, a certain bandwidth is allocated for each channel, regardless of the presence of data for transmission in the channel.

For WAN service provider organization Frame Relay assigns numbers to its clients DLCI. Typically, DLCIs 0 to 15 and 1008 to 1023 are reserved for special purposes. Clients The service provider assigns DLCI numbers in the range 16 to 1007. For broadcasting, DLCIs 1019 and 1020 can be used. The Local Management Interface (LMI) uses DLCI 1023 or 0. Some Frame service providers Relays may allow their customers to select their own DLCI numbers.

To map DLCI numbers to Layer 3 addresses, a router must first know which VCs are available. Typically, the process of determining available VCs and their DLCI numbers is carried out according to the LMI standard.

Once the router knows the DLCI numbers for the available VCs, it must determine which Layer 3 addresses to map to which DLCI numbers. Address mapping can be configured either manually or dynamically. Regardless of whether the DLCI mapping to a remote IP address is performed manually or dynamically, the DLCI used must not have the same value at both ends of the PVC.

Frame Relay LMI

LMI is a signaling standard between a DTE device (router) and a DCE device (Frame switch) Relay). The LMI is responsible for managing the connection between devices, verifying that data is being transmitted, and periodically reporting the emergence of new PVCs and the destruction of existing PVCs.

Now exists three incompatible implementation LMI Cisco , ansi And q933a.

When using Cisco IOS Release 11.2 and later, the router attempts to automatically detect the type LMI used by the provider's switch

Inverse ARP

Using appropriate configuration commands, a DLCI number can be manually mapped to a Layer 3 address. In complex networks, constructing a static mapping can be labor-intensive, and such mapping is not adaptable to Frame topology changes. Relay . Using LMI, the Frame switch Relay can notify routers about DLCI of the new virtual circuit. This notification does not contain a level 3 address. The station that received the notification will be aware of the new connection, but will not be able to address the other end. Without a new configuration or a mechanism for determining the other end's address, the new virtual circuit cannot be used.

Inverse Address Resolution Protocol (Inverse Address Resolution Protocol (Inverse ARP)) was developed For provision mechanism dynamic displays DLCI on third-level address. Inverse ARP works much like ARP in LAN. However, in ARP, the device knows the remote IP address and needs to determine the remote device's MAC address . In Inverse ARP, the router knows the Layer 2 address, which is the DLCI, but needs to determine the remote IP address.

Once the router has received information about available PVCs from the switch and their DLCI, he can send An inverse ARP request to the other end of each PVC for its Layer 3 address. At the same time, this request provides the remote system with the local system's Layer 3 address. The information received from the inverse ARP is used to construct the Frame mapping. Relay to IP.

If a Cisco router configures an interface to use Frame encapsulation Relay , then Inverse ARP is enabled automatically. If a static mapping is configured for a specific interface, then Inverse ARP is automatically disabled for that protocol and that DLCI. If the router on the other end does not support inverse ARP, then static mapping should be used.

Configuration encapsulation V Frame Relay

When configuring the router's serial interface to connect to Frame Relay Frame encapsulation must be defined Relay . There are two possible encapsulations: IETF and Cisco . Cisco devices use Cisco encapsulation by default . The Cisco method is proprietary and cannot be used if the Cisco router is connected via a Frame network. Relay with equipment from another manufacturer.

Frame configuration Relay in Cisco IOS versions older than 11.1, using inverse ARP and auto-detection of LMI type, you only need to specify the third-level address and set the encapsulation to Frame Relay

```
Router(config-if)# encapsulation frame relay {cisco | ietf }
```

If is used Cisco iOS versions 11.1 or earlier , That necessary ask type LMI Router(config-if)# **frame-relay lmi -type { ansi | cisco | q933a }**

It is important to remember that the Frame provider Service Relay creates a virtual circuit within the Frame network. Relay, which connects two remote user network devices, typically a router. Once the router and Frame switch The relay to which it is connected completes the exchange of LMI information, the network Frame Relay has everything needed to create a virtual circuit to another remote router. Frame Network Relay isn't like the Internet, where any two devices connected to it can communicate with each other. In a Frame network Relay Before two routers can exchange information, the Frame service provider Relay must establish a virtual circuit between them in advance.

Configuration mappings Frame Relay

If dynamic address mapping is used, then for each active PVC, the router's inverse ARP service requests an IP address from the next-hop router. Once the requesting router receives the inverse ARP response, it updates its Layer 3 address mapping table. DLCI numbers. For Cisco devices, dynamic address mapping is enabled by default. If the equipment Frame Since Relay supports inverse ARP and auto-detection of the LMI type, dynamic address mapping occurs automatically. Therefore, static address mapping is not required.

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 - relay command map. How only For this DLCI static is set display, on this inverse service ARP is disabled.

To configure a static mapping, 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 the encapsulation type, default is cisco.

Broadcast option - means broadcast. It is used when configuring routing protocols and allows one to consider networks with multiple access and without broadcasting (which is what Frame is). Relay) is much the same as a local area network (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 a serial interface, this encapsulation is applied to all VCs on that interface. If the interface communicates with Cisco and non-Cisco equipment, IETF encapsulation should be selectively configured.

Examination configurations interface Frame Relay

Frame configuration Relay You should check that the connections are active. This is done using several show commands :

The show command interfaces serial shows information about the encapsulation and status of the first and second layer protocols, as well as the broadcast DLCI, about all used V sequential interface rooms DLCI And O DLCI, used for LMI.

The show command frame relay PVC Shows the status of each configured connection and traffic statistics. The command shows the status of all PVCs configured on the router.

Team **show frame relay map** shows elements current displays addresses and connection information.

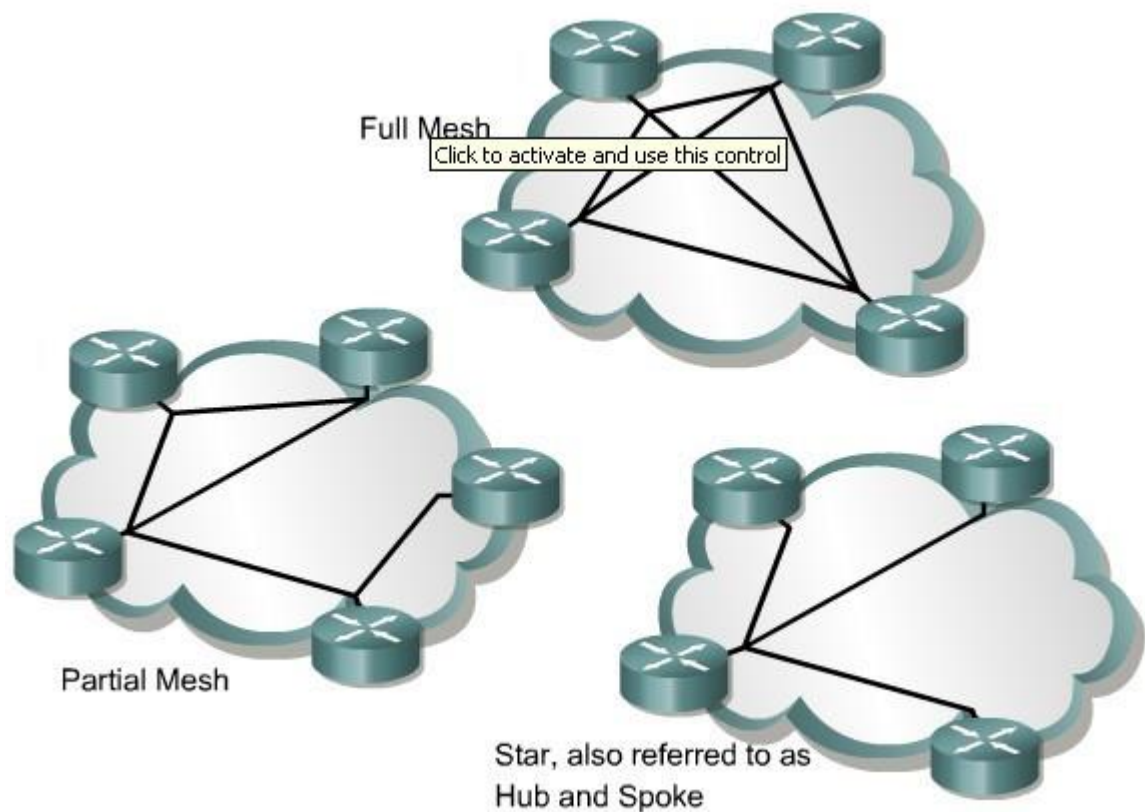
The show command frame relay lmi shows LMI traffic statistics: the number of status messages exchanged between the local router and the Frame switch Relay .

Topologies Frame Relay

Frame Relay permits interaction remote websites several ways Star, sometimes called hub and spoke

Fully connected (Full mesh)

Partially related (Partial mesh)



Drawing 7.

Topology star most popular because of his own cost Efficiency. In this topology, remote sites connect to a central site that provides services. This is the least expensive topology, requiring a minimal number of PVCs. Typically, the central router uses a single interface to connect to multiple PVCs.

In a mesh topology, all routers have PVCs to all other routers. The topology is redundant but reliable: if any link goes down, the routers can change routes. WITH growth numbers nodes the cost increases sharply.

In a partially connected topology, not all sites are directly connected. The presence of PVCs between routers is determined by traffic volume, network architecture, or other considerations.

Configuration subinterfaces For Frame Relay .

Subinterfaces are logical subdivisions of a physical interface. By configuring subinterfaces , each PVC can be configured as a point-to-point connection. This allows each subinterface to act as a leased line. This is because each point-to-point subinterface is treated as a separate physical interface.

In a point-to-point connection, a single subinterface is used to establish a PVC connection to another physical interface or subinterface on a remote computer. In this case, each pair of subinterfaces can be on its own subnet, and each subinterface has a single DLCI.

To configure subinterfaces on a physical interface, Frame encapsulation is assigned. Relay (Cisco or IETF). If the physical interface already has an IP address, it must be removed, since each subinterface has its own IP address. If the physical interface has an address, frames will not be received by 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 2 type 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 introduction these teams operating room system iOS changes the prompt to **config-subif** , meaning subinterface configuration mode .

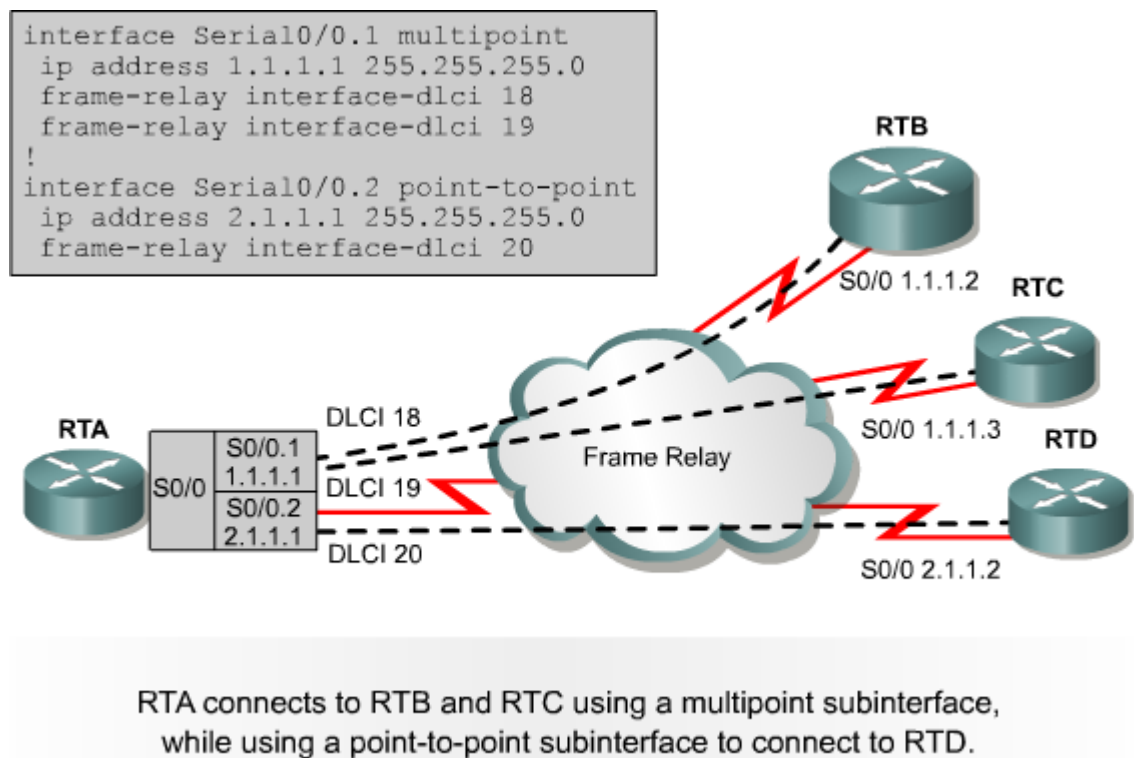
Subinterface numbers can be assigned in subinterface configuration mode . or V globally configuration mode V range from 1 to

4294967295 When configuring a point-to-point subinterface , it is common practice to number the subinterface according to the DLCI value of the PVC.

After creation subinterface follows ask IP RTA address (
config-subif)# **ip address 2.1.1.1 255.255.255.0**

Next, either a static display of Frame is configured Relay or **the frame-relay** command is used **interface-dlci** for association subinterface with DLCI. This command is required for all point-to-point subinterfaces . It is also required for subinterfaces multipoint with inverse ARP enabled. It is not required for subinterfaces. multipoint , which are configured using static route mappings.

Some Frame Switch The relay in Figure 8 uses LMI to inform RTA that three active PVCs with DLCI numbers 18, 19, and 20 are available.



Drawing 8.

When RTA learns about DLCIs 18, 19, and 20 on interface S0/0, RTA doesn't know which DLCI to use with which subinterface . This is because the LMI doesn't provide a way to notify RTA that DLCI 20 should be used by interface S0/0.2, not S0/0.1. Therefore, each subinterface must be manually associated with an acceptable DLCI number.

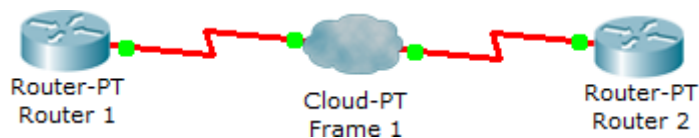
Multipoint mode is not fully supported by the simulator and will not be considered.

Practical Part

Boson designer always creates a fully connected Frame topology Relay . To create a network topology using Frame Relay , first you need to decide which routers and through what are yours? sequential interfaces will be connected to Frame Relay . Next, right-click on one of these routers, which will be connected to the Frame Relay , and select the Add context menu items connection then the desired serial interface . In the modal window that appears, select the Point-to-Multy-Point radio button. Serial Connection (Frame Relay). Click the Next button. A new modal window. Select the first router you want to connect to the Frame from the first list. Relay , in the second list select its interface, which will be connected to the Frame Relay and click the Add button . Select the second router you want to connect to the Frame from the first list. Relay , in the second list, select its interface, which will connect it to the Frame Relay and click the Add button . Repeat this for all routers. Click the Connect button. The designer will create a mesh topology, defining the PVCs and DLCIs. A window will appear with the assigned DLCIs. You can edit them. It is recommended that you accept them by clicking OK. You can change the values later. DLCI by right-clicking on the Frame cloud Relay .

Simulator Not V complete measure supports Frame Relay .

1. We create topology on 805 routers



Drawing 9.

Configuring Frame Relay

TO ROUTER						
F R O M R O U T E R		Router 1	Router 2			
	Router 1		102			
	Router 2	201				

Drawing 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 215.10.1.2 255.255.255.0
router2(config-if)# no shut

```

Let's introduce team **show interfaces serial0** on both routers . It will show whether you are connected to Frame Relay . You should see phrases ' up and line protocol is up ' and 'DTE LMI up '.

show command frame relay map On both routers. On router1, it won't show anything, since **inverse-arp is disabled** . On router2, it will show a mapping from the local DLCI to the remote IP address 201-215.10.1.1.

The show command frame relay PVC should show the PVC status 'ACTIVE' on router2 and the 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 command frame relay PVC** should show the PVC status as 'ACTIVE' on router1. Ping both routers.

1.2 Simulator version 5.3 does not support static address assignment. Simulator version 6.0 Final beta supports.

Download former topology from drawings 9 And 10.

and create a 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 routers.

1.3 Usage subinterfaces

Download former topology from drawings 9 And 10 And create new router1 configuration (config)# **interface seria0**

```

router1(config- if)# encapsulation frame- relay
router1(config-if)# no shut

```

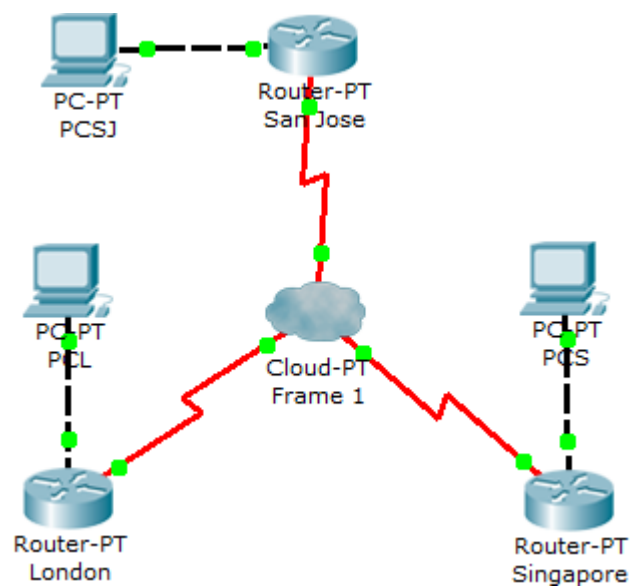
```

router1(config-if)# interface serial0.102 point-to-point
router1(config-subif)# ip address 215.10.1.1 255.255.255.0
router1(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 215.10.1.2 255.255.255.0
router2(config-subif)# frame-relay interface-dlci 201

```

show ip interface command on both routers. brief . You should see assigned addresses and active interface states. (status = up and up). Note that the command “ show frame relay map ” Not shows addresses For subinterfaces , and displays the subinterface -DLCI ratio. The same information is displayed by the show command. frame relay pvc ”. Ping both routers.

2. we'll use one computer per branch as a local network model.



Drawing 11.

Let's appoint DLCI according to drawing

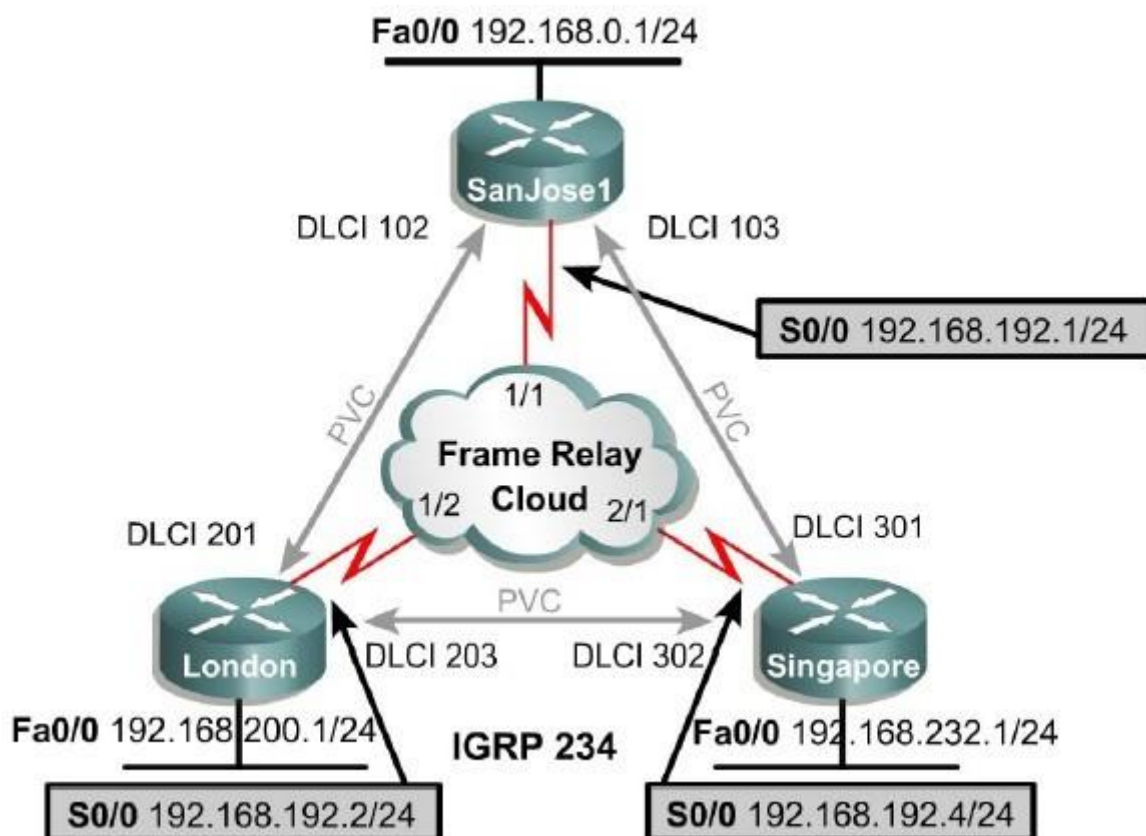


Fig. 12.

Configuring three routers for Frame A relay network for connecting three company branches using a mesh topology. We use OSPF as the routing protocol.

2.1. Dynamic tuning On the

SanJose1 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 shut**

SanJose(config-if)#**interface Ethernet0**

SanJose(config-if)#**ip address 192.168.0.1 255.255.255.0**

SanJose (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**

На маршрутизаторе 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

```

```

На маршрутизаторе 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 “show ip interface brief” commands and “show interfaces serial0 ”. You can see the interface states. Enter the command on both routers “ show frame relay pvc ” You you can see the states of frame channels 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 see active channels on San Jose (DLCI=301) And London (DLCI=302).

In real Frame networks Relay channel states can be ACTIVE, INACTIVE and DELETED. ACTIVE is a working end-to-end (DTE to DTE) circuit. INACTIVE indicates a successful connection to the Frame switch. Relay (DTE to DCE) in the absence of a router (DTE) at the other end of the PVC. This condition occurs when the router at the other end of the PVC is either not participating in the Frame Relay or is not configured for our network. The DELETED state occurs when the router (DTE) and switch Frame Relay We couldn't agree on the Frame parameters. 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 recognize them? When the Singapore router receives a list of DLCIs via the LMI protocol, it sends inverse ARP requests to each of its discovered PVCs. The router on the other end of the PVC returns its IP address.

From the table, we see that broadcast is enabled, allowing routing protocols to exchange routing information. Using the show command IP route, make sure there is a route from London 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 a route to network 192.168.232.0/24 Singapore to address 192.168.192.4 via Serial0.

We see, What only **With one physical communication** To Frame Relay every The router has **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 check from the router in San Jose whether connection from the PCL branch computer in London To branch computer PCS in 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 Sun

```

e

Pings successful.

2.2. Static setting

Use simulator versions 6.0 Final beta .

Network engineers may be dissatisfied with implicit dynamic configuration. The benefits of dynamic DLCI-IP mapping are minimal due to the static nature of most global links. Once a connection is established, it remains unchanged for years.

Let's unite branches V global net statically. For this follows create Recreate the new configuration. Load the previously created topology into the simulator and configure the 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
SanJose (config-if)# no shut
SanJose(config-if)#interface Ethernet0
SanJose(config-if)#ip address 192.168.0.1 255.255.255.0
SanJose (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 broadcast
London(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 broadcast
Singapore (config-if)# frame-relay map ip 192.168.192.2 302 broadcast
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**

We used the **no command frame relay inverse-arp** , since without it the simulator displays addresses both statically and dynamically.

Team frame relay map associates The next-hop IP address with the local DLCI. The broadcast keyword allows broadcast traffic, for example, for routing information for routing protocols.

show command on all routers. IP interface brief” and “ show interfaces serial0 ”. You can see the interface states. Enter the following commands on both routers: “ show frame relay pvc ” and “ show frame relay lmi ”. You can see the frame states relay . The show command frame relay map will show a statically assigned mapping of "external IP address" to "local DLCI for Canada" pvc to a 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 the show command IP route , make sure there's a route from London to Singapore. Unfortunately, the simulator is version 6.0 Final. beta routing issues.

Let's configure local networks branches How V table 1.

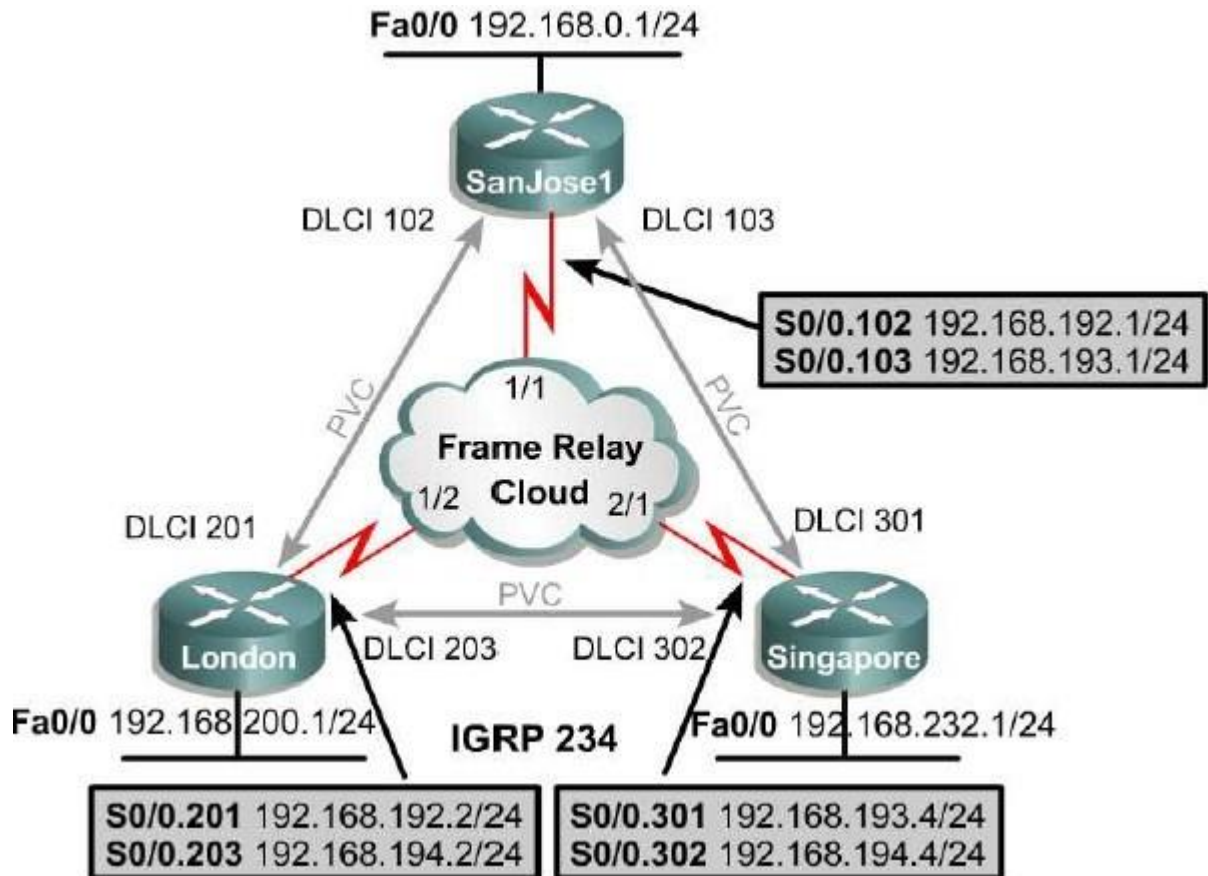
Let's check the full configuration using the extended ping command . For example, we can check from the router in San Jose whether connection from the PCL branch computer in London To branch computer PCS in Singapore.

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.

To improve connection customization, network engineers initially considered using individual physical links between each branch office. However, the overall cost of the project proved prohibitive. It was decided to use subinterfaces and Frame. Relay . This allows you to create a separate logical channel between every two branches. Each router still has one physical line for connection to Frame Relay , but two subinterfaces are configured for each serial interface . This makes it possible to use multiple PVC channels for each physical interface of the router. The overall cost of the project is acceptable.



Drawing 13.

To do this, you need to create a new configuration again. Restart the simulator and load the previously created topology (Figure 11). Configure the subinterfaces on the routers as shown in Figure 13. Use a separate subnet for each PVC channel.

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 SanJose1 Router (config)# **hostname San Jose**

SanJose(config)# **interface serial 0**

SanJose(config-if)# **encapsulation frame-**

relay SanJose1(config-if)# **no shutdown**

We don't assign an IP address to the entire interface . We assign addresses to each subinterface .

Frame Interfaces Relays can be switched to either point- to - point mode or V mode multipoint (multipoint). Configuring subinterface point- point,

using DLCI. It is common practice to use the DLCI number as subinterface numbers. Then it's easier to determine which channel PVC uses each subinterface. For example, the 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 interface command s0.103 point-to-point. Use

? For issuance hints after input another one words teams.

Team frame relay interface-dlci is used to determine which DLCI each subinterface uses. A point-to-point subinterface can only use one DLCI. If a subinterface for a DLCI is not defined, the DLCI is associated with the 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 SanJose routing
(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-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 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 shutdown
London(config-if)#exit
London(config)#router ospf 100
London(config-router)#network 192.168.0.0 0.0.255.255 area 1
```

Сингапур

```
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 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 using the show command. frame relay pvc . Show commands frame relay map in case of subinterfaces does not have two DLCI mappings to an IP address. Each subinterface is treated as a separate physical interface for each PVC. In this case, each PVC contains only two hosts, and there is no need to identify the next hop.

For to check the correctness of address assignments and to ensure that all subinterfaces are active state, use the **show command IP interface brief** . Using the **show command IP route** , make sure 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 see that OSPF has worked so that London has a route to Singapore's network 192.168.232.0/24 via Serial0.201 on address 192.168.192.1. Route, through

via Serial0.203 to address 192.168.194.4 In short. How are you? Route optimization issues are not discussed here .

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 check from the router in San Jose whether connection from the PCL branch computer in London To branch computer PCS in Singapore.

All pings should be successful. IN particulars between by everyone PC.

3. Topology star

Traffic between London and Singapore proved insignificant, so it was decided to abandon the PVC link between them and use a star topology. All traffic between London and Singapore will go through San Jose .

Let's load the old topology into the designer. Right-click on the Frame cloud in it. 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	

Drawing 14.

We use subinterfaces V mode point-to-point SanJose :

```
Router(config)# hostname SanJose
```

```
SanJose(config)# interface Serial0
```

```
SanJose(config-if)# encapsulation frame-
```

```
relay SanJose(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 commands on both routers **show frame relay PVC** and **show frame - relay lmi** . You can see the frame states relay . Note the absence of a PVC between London and Singapore. For subinterfaces, **the show command frame relay map** won't display the DLCI address. Use **show IP interface brief** .

Using the show command IP route , make sure there is a route from London to 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
0      192.168.193.0/24 [110/1] via 192.168.192.1, 00:00:39, Serial0.201
0      192.168.0.0/24 [110/1] via 192.168.192.1, 00:00:43, Serial0.201
0      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 to network 192.168.232.0/24 Singapore.

Let's configure the branch local area networks according to Table 1. We'll check the full configuration using the extended ping command . For example, we can check from the San Jose router whether connection from the PCL branch computer in London To branch computer PCS in Singapore.

All pings should be successful. IN particulars between by everyone PC.

Let's look at the packet path from the PCL branch computer in London To branch computer PCS in 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 SanJose (192.168.192.1).

Control questions

1. Name it types sequential channels connections.
2. Where is located device CSU/DSU And which functions it performs?
3. What such DTE and DCE?
4. How DTE connected With DCE?
5. Formulate idea networks With switching packages SKP.
6. What such virtual chains V Investigative Committee?
7. Name it types Investigative Committee?
8. Which physical channels connections use Investigative Committee?
9. How is being carried out access consumer To Investigative Committee?
10. Which technologies transmissions data are used V Investigative Committee?
11. IN how difference Frame Relay And X.25?
12. Protocol Frame Relay Not corrects errors. Where They then they are corrected?
13. What such ATM?
14. Name it protocols global networks And For what kind types of serial communication channels 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 in PVC from SVC?
19. What such DLCI And How it correlates With PVC?
20. What necessary do, to transfer IP plastic bag through net Frame Relay ?
21. How display DLCI on remote IP?
22. What such LMI?
23. Describe work protocol Inverse ARP.

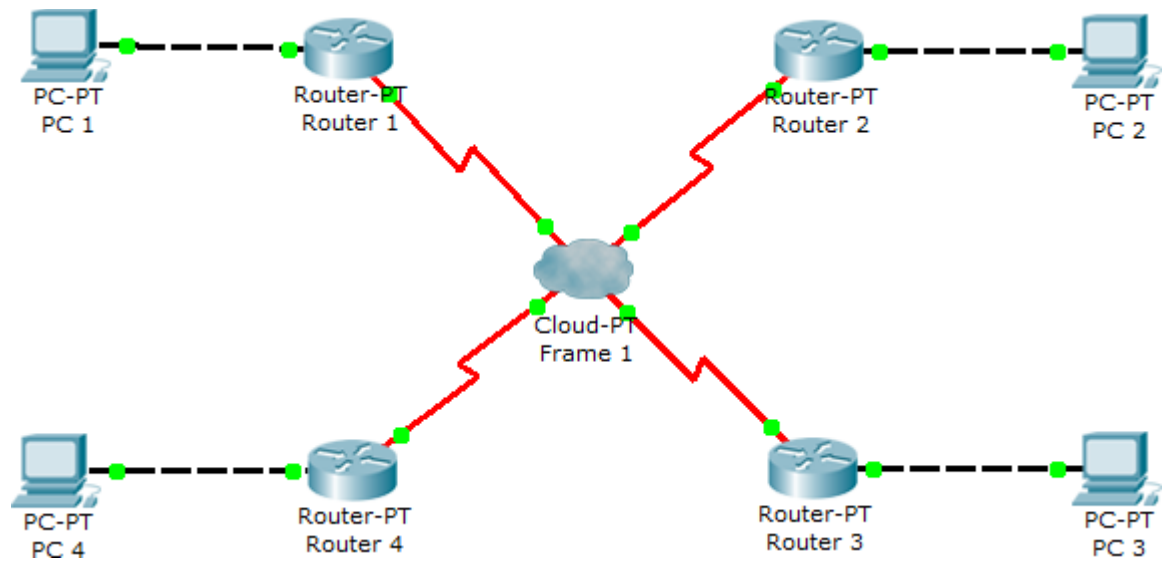
24. How to configure a router's serial interface to connect to Frame Relay .
25. When is used static display addresses?
26. How on router see To what PVC He connected?
27. How on router For interfaces see displays DLCI to a remote IP?
28. How on router For subinterfaces see displays DLCI to a remote 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. Study theoretical And practical part.
2. Pass to the teacher theory work by way answer on control questions.
3. Execute contract All points practical parts.
4. Create All screenshots, given V practical parts.
5. Show to the teacher result execution points 1, 2 And 3 practical part.
6. Do it V Packet Tracer exercise For independent work.
7. Show to the teacher result execution points 1, 2 And 3 tasks for independent work.
8. Make out report. Content report Look below.
9. Protect report.

Exercise For independent work

1. For a fully meshed topology of four sites with local area networks (Figure 15) design Frame Relay network with:
 - A) dynamic appointment addresses; B)
 - subinterfaces .
 - Use protocol routing OSPF.
 - 16 subnet at your disposal , where v is the variant number. Assign the network and interface addresses yourself.
 - Do it screenshots:
 1. 4-x tables routings For each router.
 2. Teams extended ping from any router For two arbitrary pairs of computers.
 3. The output of **the show frame-relay map** command for each router



Drawing 15.

2. Incompletely connected topology

In the designer, right-click on the Frame cloud Relay and selecting Set Frame Relay Parameters , you can edit the DLCI table

TO ROUTER					
FROM 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 four A) Star (fork)

TO ROUTER					
FROM 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

TO ROUTER					
F R O M R O U T E R		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)

TO ROUTER					
F R O M R O U T E R		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	in	3.1.0.0/16
4	and	4.1.0.0/16
5	b	5.1.0.0/16
6	in	6.1.0.0/16
7	and	7.1.0.0/16
8	b	8.1.0.0/16
9	in	9.1.0.0/16
10	and	10.1.0.0/16
11	b	11.1.0.0/16
12	in	12.1.0.0/16

Assign network and interface addresses yourself. Use subinterfaces . Take screenshots:

1. 4 tables routings For each router.
2. Teams extended ping from any router For two arbitrary pairs of computers.
3. The output of **the show frame-relay map** 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 part.
2. All screenshots, created at execution practical parts.
3. Configurations of all of configuration .txt files , created during the practical part.
6. Configuration routers from configuration .txt files, created while completing assignments for independent work.
7. All screenshots, specified V task For independent work.

Lab #9: Virtual Local Area Networks (VLANs)

Theoretical Part.

Local area networks are currently built using switched Ethernet technology. The goal is to minimize the number of hubs used and use primarily switches. A virtual channel (virtual) is created between the receiver and transmitter during the connection. circuit) point-to-point. Such a network can be considered as a set of independent stream receiver-transmitter, each from which uses the entire bandwidth. The switch allows to carry out parallel transmission of information. Switching reduces the likelihood of network congestion. Ethernet.

If a switch needs to transmit a packet to an output port and that port is busy, the packet is placed in buffer memory. This allows the speeds of packet transmitters and receivers to be matched.

For dispatches frame through switch are used two method:

Dispatch with intermediate storage (store-and-forward). A package must be accepted in its entirety before it can be sent.

Cut-through method. The switch receives the beginning of the packet, reads it in the address of the point is there appointments and starts sending the packet even before it is complete receipt.

An Ethernet switch learns the MAC addresses of devices on the network. by reading source addresses in received packets. The switch stores information in its internal tables about which ports and from which Packets arrive at MAC addresses. When connecting multiple devices to a single port via a hub, In the table, one port will correspond to several MAC addresses. Tables are stored in content-addressable memory. memory, CAM): if the address If the sender is not in the table, it is entered there. Along with address-port pairs, the table stored And label time. Label time V line the table changes or when a packet with the same address arrives at the switch, or when the switch contacts at this address. If a table row has not been used for a certain period of time, it is deleted. This allows the switch to maintain a correct list of device addresses for packet forwarding.

Using CAM The switch, using the address table and the recipient address contained in the incoming packet, creates a virtual connection between the sender port and the recipient port and transmits the packet through this connection.

The virtual connection between the switch ports is maintained for the duration of the transmission of one packet, i.e. for each packet the virtual connection is re-established based on the recipient address contained in the packet.

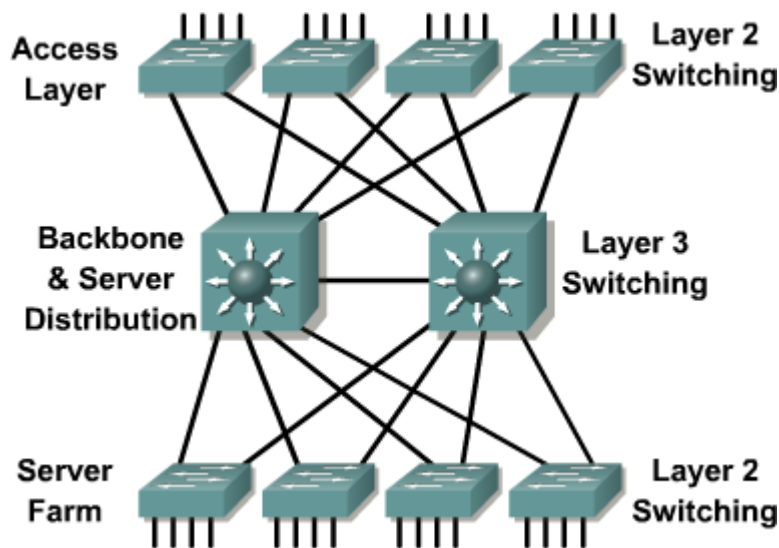
Since the packet is transmitted only to the port to which the recipient is connected, other devices connected to the switch, will not receive this package.

In Ethernet switches, data transmission between any pair of ports occurs independently and, therefore, the entire channel bandwidth is allocated for each virtual connection.

When transmitting a broadcast packet, a fan is formed in the switch channels on a one-to-many basis. Examples of sources of broadcast traffic include ARP and routing protocols.

Switches Can unite Friend With friend. At this group in pairs directly A set of indirectly connected switches forms a single logical switch with a theoretically arbitrary number of ports. This means that switches allow the creation of a theoretically arbitrarily large local area network. Properly connecting switches, or choosing a network topology, is one of the most important tasks in local area network design.

It is recommended to connect switches by layers (Figure 1): server layer, distribution layer (distribution) and access layer (access). Regular computers connect To layer access, A servers To server layer.



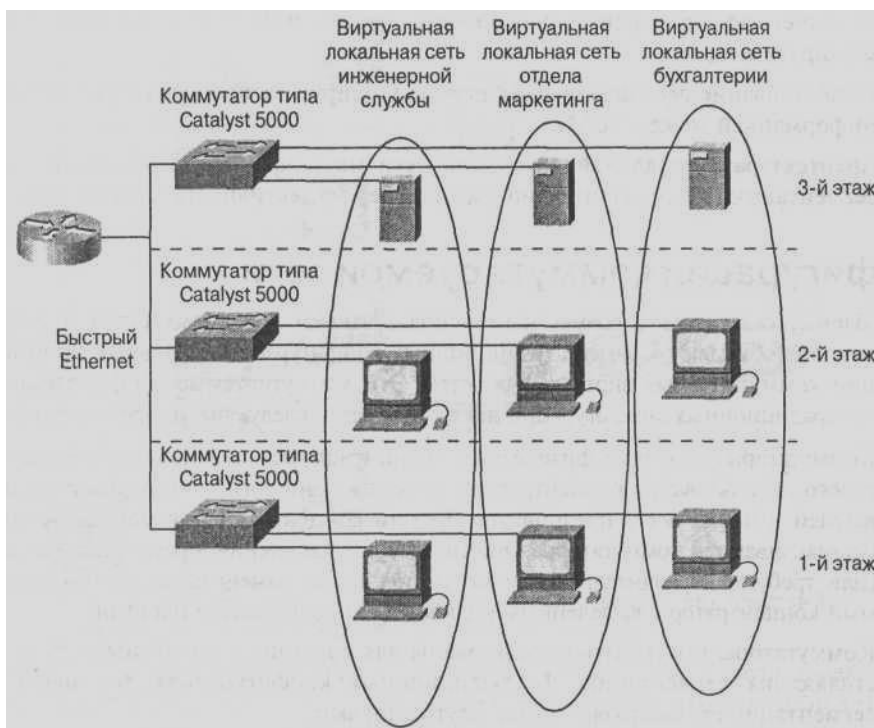
Drawing 1.

The main obstacle to creating large local area networks using switches alone is the nonlinear growth of broadcast traffic as the number of devices on the network increases. When the number of devices on the network exceeds 2,000 (some estimates say 500, others say 4,000 – it all depends on the network topology and the type of tasks being solved), the volume of broadcast traffic increases sharply. Adding new devices dramatically reduces network performance.

For example, if in a network of several thousand devices one computer A makes an IP connection to another computer B in this network for the first time, it must first send a broadcast ARP request to all devices on the network to determine the MAC address of computer B.

A local area network created using only switches is One broadcast domain. A broadcast domain can be reduced by physically dividing the local network into independent subnets (independent groups of paired switches) and connecting them into a single unit using routers. This can only be accomplished during the network construction phase, not during its operation. This is where virtual local area networks (VLANs) come in . local area network).

Virtual local net VLAN represents by yourself totality ports one or more switches (Figure 2).



Drawing 2.

VLANs allow you to logically split a single local area network into multiple independent local area networks without physically breaking network connections. To do this, the administrator networks must on each switchboard appoint, which his ports Which VLANs do they belong to? By default, all switch ports belong to the same VLAN. with number 1. The maximum number of VLANs in a switch is equal to the total number of its ports. The correct breakdown of the local VLAN networking is one of the most important design tasks.

VLANs behave the same as physically separated LANs. That is, after breakdowns networks on VLAN We we will receive some local networks, which further

must be combined into a single whole using routing at the third network layer.

Concept VLAN, besides solutions problems With broadcast traffic also provides a number of additional advantages: the formation of local networks not at the location of the nearest switch, and according to the computers' assignment to solving a particular production task; creation of a network based on the type of computing resource consumed and the required server service (file server, database server) data). VLANs allow you to maintain different security policies for different virtual networks; transfer a computer from one networks to another without physically moving or reconnecting.

Switches use a trunking protocol to exchange VLAN information. To exchange VLAN information between switches, you must create trunk ports. A trunk port is a port used to transmit VLAN information to other network devices connected to that port. Regular ports do not advertise VLAN information, but any port can be configured to receive/transmit VLAN information. You must activate the main line protocol on necessary ports, So How He disabled by default.

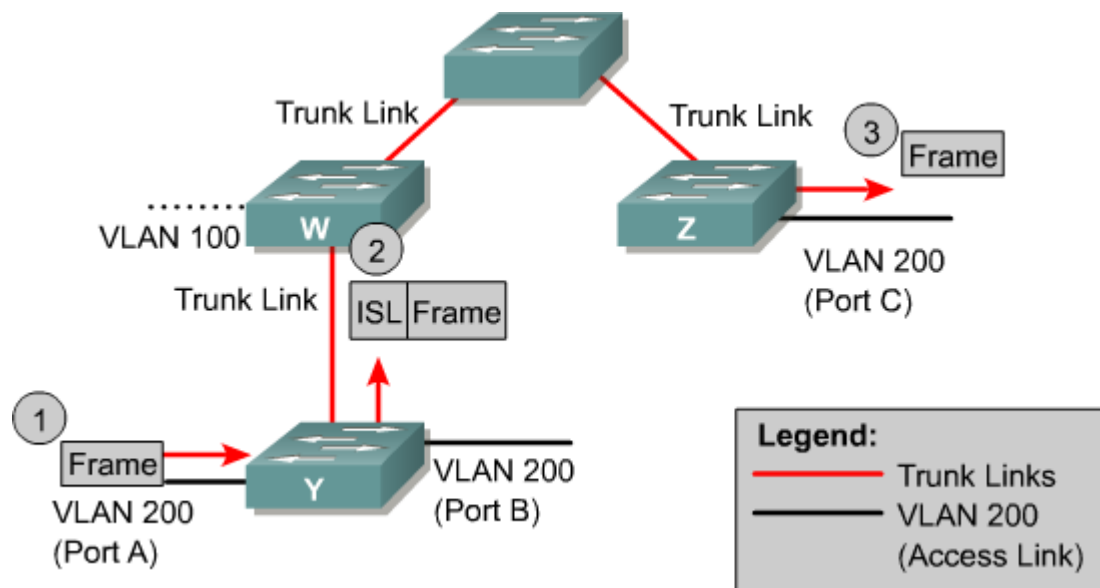
A switch port operates in either access mode or trunk mode. Accordingly, the link connected to the port is Either an access link or a trunk link. In access mode, a port belongs to only one VLAN. The access port is connected to an end device: a PC, workstation, server, or hub. Frames passing through the access port are regular Ethernet frames.

Trunk links are capable of supporting multiple VLANs. VLANs on different switches are linked via the trunk protocol. Trunk ports do not belong to a specific VLAN and are used to connect to other switches, routers, or servers that have network adapters with the ability to connect to multiple VLANs.

Trunks can extend VLANs throughout the network. For trunk purposes, high-speed switch ports are assigned: Gigabit Ethernet and 10 Gigabit.

For multiplexing VLAN traffic There are special protocols that allow receiving ports to determine which VLAN a packet belongs to. T h e Inter-Switch protocol is used to communicate between Cisco devices. Link (ISL). When the network contains equipment from multiple manufacturers, the IEEE 802.1Q protocol is used.

Without trunk links to support VLANs, it must be organized according to one access link for each VLAN. This approach is expensive and inefficient, so backbone connections are absolutely necessary when designing local area networks.



Drawing 3.

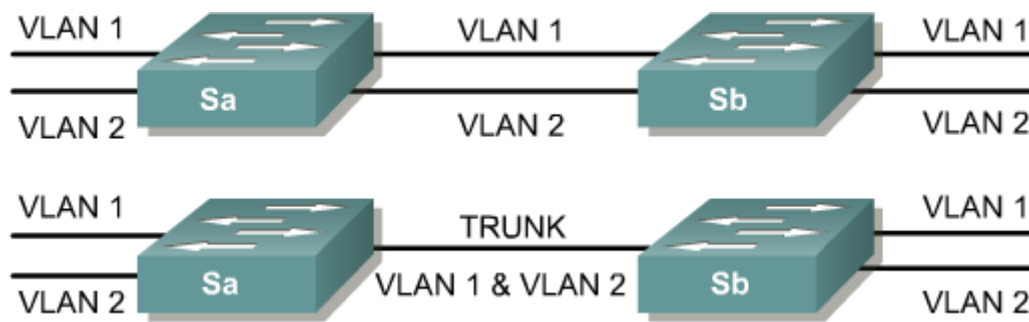
On In Figure 3, ports A and B on switch Y are defined as access links on the same VLAN 200. By definition, they can only belong to the same VLAN and cannot receive Ethernet frames containing a VLAN ID. For example, when Y receives traffic from port A to port B, it does not add the ISL header to the Ethernet frames.

Port C on switch Z is also an access port and also belongs to VLAN 200. If port A forwards a frame to port C, the following happens:

1. Switch Y receives the frame and, by matching the destination port number with the VLAN number, identifies it as traffic destined for VLAN 200 on the other switch,
 2. Switch Y adds a header with the number to the ISL frame VLAN and forwards the frame through an intermediate switch to the backbone link.
 3. This process repeats on each switchboard on the way frame to the final port of S.
 4. Switch Z receives frame, removes ISL title and directs frame on port
- WITH.

If port located V main mode, That He Maybe be configured or For transport of all VLANs or a limited set of VLANs. Trunk links are used to connect switches to other switches, routers, or VLAN-enabled servers.

According to basic terminology, a trunk is a point-to-point link supporting multiple VLANs. The purpose of a trunk is to preserve port numbers when creating a connection between two devices that form a VLAN.



Drawing 4.

The top figure in Figure 4 shows a method for creating VLANs using two physical links between switches (one for each VLAN). This solution scales poorly: adding a third VLAN requires sacrificing two more ports. This solution is also inefficient in terms of load sharing: low traffic on some links may not be worth the fact that this link is a bundle of virtual links over a single physical link. In the bottom figure, a single physical link can carry traffic for any VLAN. To achieve this, the switch Sa formats frames so that Sb knows which VLAN they are being sent to. This packet formatting uses either the IEEE 802.1Q standard or the Cisco protocol. ISL (Inter-Switch Link).

For large networks, manual VLAN configuration becomes a labor-intensive task. Cisco VLAN Trunk The VTP Protocol (VTP) is used to automatically exchange VLAN information through trunk ports. The advantage of using VTP is that you can control the addition, removal, and modification of VLANs from the switches on which VTP servers are created. After configuring your switches as VTP servers, the remaining switches in your network can be configured as clients that only receive VLAN information. The disadvantage is unnecessary traffic generated on trunk ports for devices that may not need this information.

If your network will contain many switches containing multiple virtual networks located on different switches, it may make sense to use VTP. If your network will remain fairly static, and VLANs will not be added or changed from the initial configuration, then static VLAN definition is better.

Loops are possible in local area network topologies. For example, three switches connected to each other in a circular pattern form a loop in the topology. Loops lead to ambiguity in determining the path from the source of packets to the destination. solutions this serious problems was developed protocol binder tree STP

(spanning tree For the topology graph of each VLAN defined in the network, a minimum spanning tree (a graph without cycles) is constructed with a vertex at a specific switch. To physically implement these trees, STP puts redundant ports into a blocking state. Tree calculation is performed in parallel on all switches. Packets in the VLAN then travel only along paths defined in the constructed spanning trees. When the topology changes or ports are activated or stopped, the spanning trees are recalculated.

To create a spanning tree topology, there are special frames called modules data bridge protocol (bridge protocol data units , BPDU). These frames are sent and received by all switches in the network at regular intervals.

Configuration static VLAN

1. Static A VLAN is a collection of ports on a switch that are manually assigned by an IOS command when configuring the interface.

To create an empty VLAN with the number №VLAN on switches Cisco 2950 series commands used

```
Switch#vlan database
Switch(vlan)#vlan №VLAN
Switch(vlan)# exit
Например, команды
Switch#vlan database
Switch(vlan)#vlan 33
Switch(vlan)# exit
```

will create empty VLAN With number 33 And the system will give VLAN Name VLAN0033.

Note, What teams are being carried out Not V mode configurations.

Switchport command **mode** used to set the interface to dynamic mode, modes access or trunk mode .

```
Switch(config- if)# switchport mode [access | dynamic | trunk]
```

Although the regime access is a regime By by default, But V in a row cases device attached to the port switch, can put it into trunk mode. Therefore, it is recommended to put all non-trunk ports into access mode using the **switchport command. mode access** .

For static premises current interface in VLAN are used commands Switch (config- if)# **switchport mode access**

```
Switch(config- if)# switchport access vlan №number
```

Where № **number** – number - number VLAN.

Interface command **range** defines a range of interfaces for subsequent configurations. For example, ports one through six can be placed in VLAN 10 using the command

```
Switch(config)# interface range fa0/1 - 6
```

Switch(config-if- range)# **switchport access vlan 10**

After Check your VLAN settings setting teams **show running-config** , **show vlan** And **show vlan brief** .

At setting VLAN remember, What By default All ports are located in VLAN 1.

To create or configure a VLAN trunk, you must configure a port as a trunk.

Switch(config-if)#**switchport mode trunk**

By default last one team defines port How main For all VLANs in the network.

However, there are situations where the backbone should not support All VLAN. Typical is situation With suppression broadcasting. The broadcast is sent to every port in the VLAN. The trunk link acts as a member of the VLAN and must miss All broadcasting. If on friend at the end highways No ports required VLAN, That bandwidth and processor time devices is wasted.

If the VLAN is not used at the other end of the trunk, there is no need to enable it. VLANs on this trunk. By default, trunk ports receive and transmit traffic. with everyone VLAN V networks. For abbreviations main traffic use

команду

Switch(config-if)#**switchport trunk allowed vlan vlan-list**

Например, команда

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 VLANs allowed on the trunk can be seen using the **show command. running-config** .

For deletions big number of VLANs from highways easier at the beginning delete all VLANs and then selectively allow.

The simplest way to switch a connection to access mode is to set the command on the interfaces on both sides of it

SwitchA (config- if)# **switchport mode access**

The simplest way to switch a connection to access mode is to set the command on the interfaces on both sides of it

SwitchA (config- if)# **switchport mode trunk**

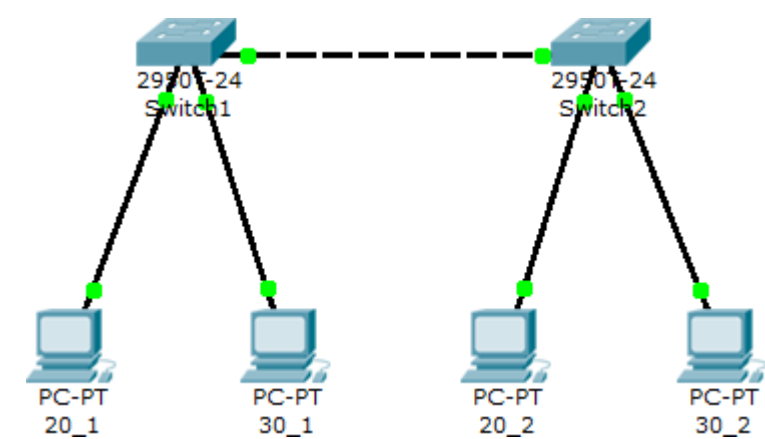
Practical Part

1. Assemble the topology shown in Figure 5. Connect the switches with two GigabitEthernet (gi1/1 and gi1/2) connections. Connect the computers to the interfaces according to Table 1. Assign addresses to the computers according to Table 1. All computers are part of the same subnet 172.16.0.0 255.255.0.0. Default routes on the computers Do not install. Ping the network.

Let's create two VLANs in our network. We'll place computers 20_1 and 20_2 in VLAN 20, and we'll place computers 30_1 and 30_2 in VLAN 30.

Switch1(conf)# **interface fa0/2**

```
Switch1(conf-if)#switchport access vlan 20
Switch1 (conf-if)#interface fa0/3
Switch1(conf-if)#switchport access vlan 30
Switch2 (conf)#interface fa0/2
Switch2(conf-if)#switchport access vlan 20
Switch2 (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 creation VLAN, for example Switch1# 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 only ping themselves.

We organize highways on switches. For this we use Gigabit Ethernet port Switch1(conf)#
interface gi1/1

Switch1 (conf-if)#**switchport trunk allowed vlan add 20**

Switch1 (conf-if)#**switchport trunk allowed vlan add 30**

Switch1 (conf-if)#**no shutdown**

Switch2 (conf)#**interface gi1/1**

Switch2 (conf-if)#**switchport trunk allowed vlan add 20**

Switch2 (conf-if)#**switchport trunk allowed vlan add 30**

Switch2 (conf-if)#**no shut**

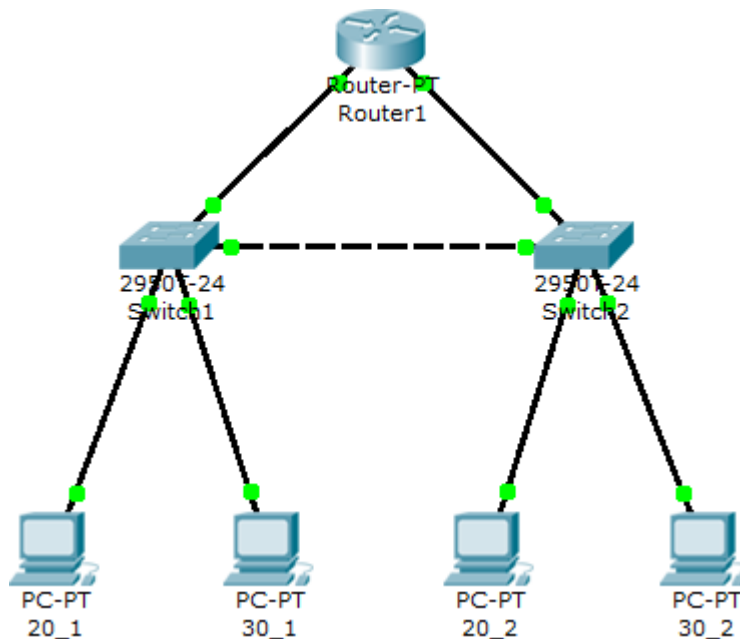
Now computers within the same VLAN should be pingable , and computers in different VLANs should not be pingable (see Table 2).

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 the topology from the previous task in a new file. In this topology, the router is connected by two links to the fa0/1 interfaces of the switches (Figure 6). Again, check that computers within the same VLAN can be pinged, while computers in different VLANs cannot.



Drawing 6.

Let's set the task of connecting virtual networks using a router. To do this, we need to split our network 172.16.0.0/16 into two subnets: 172.16.20.0/24 and 172.16.30.1/24. To do this, simply change the masks on the computers to 255.255.255.0.

Now computers can ping within the same VLAN and within the same IP subnet, which means only to themselves.

We will introduce interfaces on the switches connected to the router in virtual networks

```
Switch1(conf)#interface fa0/1
```

```
Switch1(conf-if)#switchport access vlan 20
```

```
Switch2(conf)#interface fa0/1
```

```
Switch2(conf-if)#switchport access vlan 30
```

Настроим IP адреса на маршрутизаторе

```
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
```

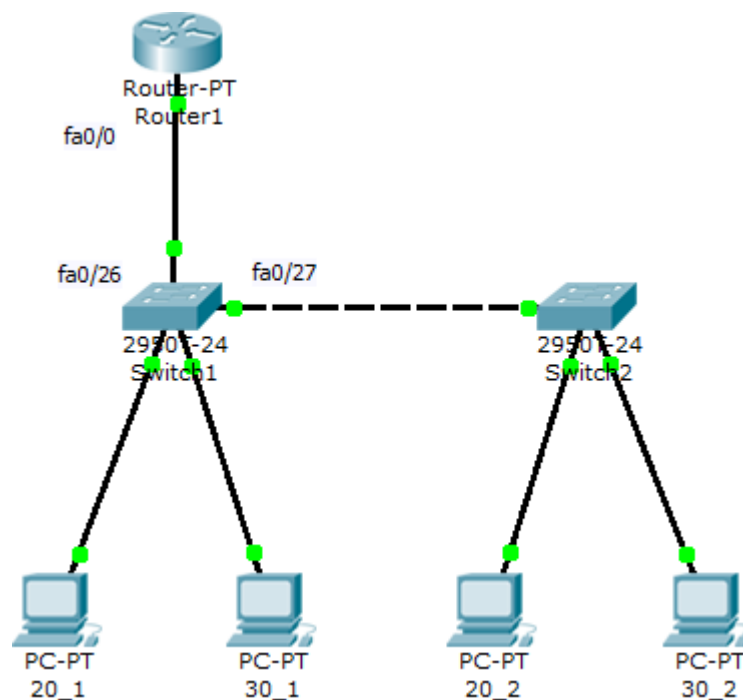
Now the router routes our two networks. 172.16.20.0/24 and 172.16.30.1/24. Let's add default routing to the router interfaces on our computers.

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 iso 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 backbone from the switches to the router's fa0/0 interface (Figure 7). Load the topology into the simulator. Load the saved configurations one by one to each device except the router. Note that in the Switch2 configuration , installing the backbone on gi1/2 is not necessary, although it doesn't interfere.



Drawing 7.

On the router, split the fa0/0 interface into two subinterfaces , fa0/0.20 and fa0/0.30. We'll define dot1q insaptation 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 routes Router# **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. Run on Router team extended ping from addresses 172.16.20.1 computer 20_1 from VLAN 20, connected To switchboard Switch1 To address 172.16.30.2 of computer 30_2 from VLAN 30 connected to 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 do people prefer to build local area networks using switches rather than hubs?
2. Which exist methods For dispatches frame through switch?
3. How switch recognizes MAS addresses connected devices?
4. Where And How V switch are stored addresses connected devices?
5. What such virtual compound And How for a long time it exists?
6. How much big local net Can create With help switches?
7. How accepted build big local networks?
8. What is the main obstacle to creating large local area networks? with the help of some only switches?
9. What such domain broadcasting?
10. How decrease domain broadcasting?
11. What such VLAN?
12. Which problems local networks decides VLAN?
13. How V local networks organize exchange information O VLAN?
14. IN what kind modes they work 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 without using highways?
18. For what needed protocols ISL And IEEE 802.1Q?

19. For what needed highways V V local network?
20. Which tasks decides VTP?
21. Which tasks decides 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 is eleven VLAN. How many routers are needed to combine all 11 VLANs into a single unit?

Order execution And surrender work

1. 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, show the teacher the ability to perform an extended ping between any addresses for the topologies in Figures 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 to the options.
The practical part was done for the 172.16.0.0/16 network.

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 part.

Content report.

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

1. Screenshots topologies, created at execution practical part.
2. Configurations of all routers from the configuration .txt files created during the practical part.

3. Configurations of all routers from .txt files created during the independent work assignment.
5. All screenshots, specified V task For independent work