HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

Network Protocols

LAB 1

MODELING A SIMPLE NETWORK

Instructors

Elena Boldyreva, Associate Professor eaboldyreva@itmo.ru

Yuriy Boldyrev, Assistant Professor

HDU-ITMO Joint Institute

杭州电子科技大学 圣光机联合学院

PREREQUISITES

1. Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross (Chapter 1 and Chapter 2)

REPORT

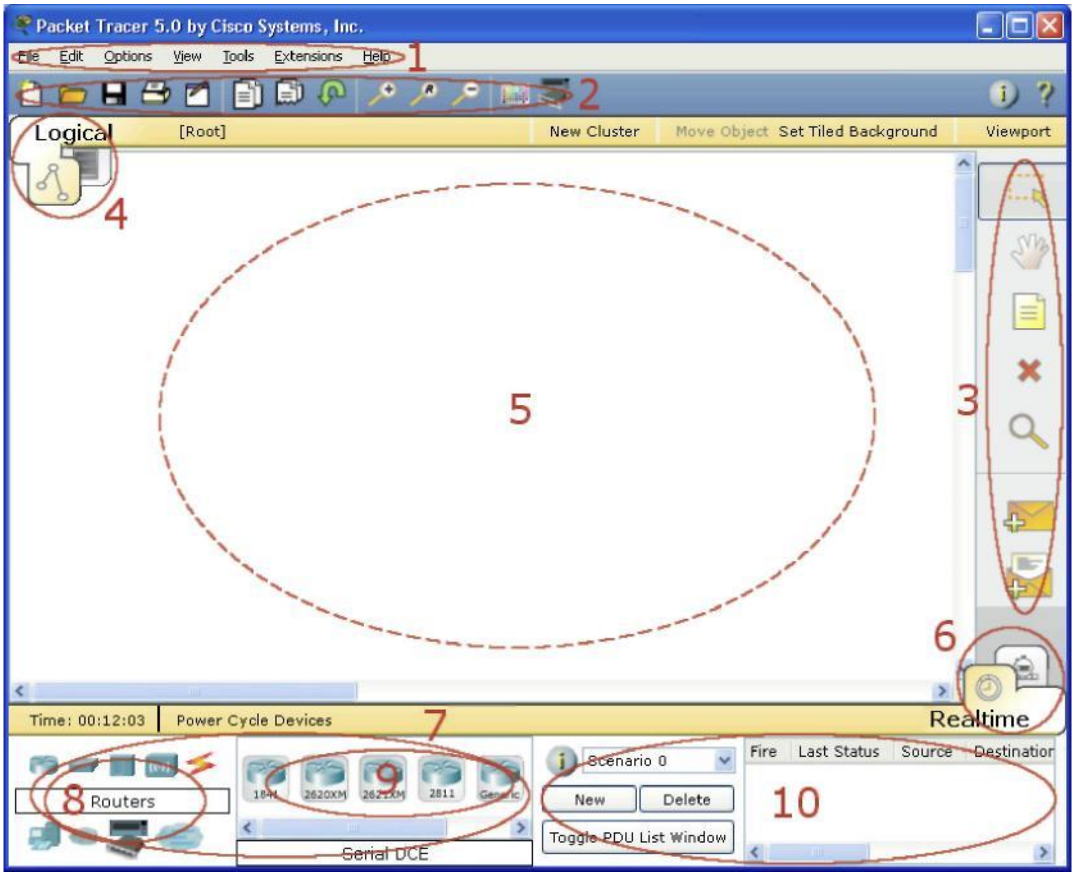
After completion the task the students need to submit:

- **The format of the report file is *pdf*.**
- Upload reports for the GitLab repository (to your personal project)
- Do not forget to write your name and ID inside the report

Theoretical part

To start Cisco Packet Tracer, you must call the executable file (.exe) with PacketTracer

General view of the program:



The workspace of the program window consists of the following elements:

1. Menu Bar-a Panel that contains the menu File, Edit, Options, View, Tools, Extensions, Help.
2. the Main Tool Bar contains graphic images of shortcuts for accessing the File, Edit, View, and Tools menu commands, as well as the Network Information button.
3. Common Tools Bar-a Panel that provides access to the most used tools of the program: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU and Add Complex PDU.

4. Logical/Physical Workspace and Navigation Bar-a Panel that allows you to switch the workspace: physical or logical, and also allows you to move between cluster levels.
5. Workspace - the Area where the network is created, the simulation is monitored, and various information and statistics are viewed.
6. Realtime / Simulation Bar-use the bookmarks in this panel to switch between Realtime and Simulation mode. It also contains buttons related to Power Cycle Devices, Play Control buttons, and the Event List switch in Simulation mode.
7. Network Component Box Is the area where devices and connections are selected to be placed in the workspace. It contains the Device-Type Selection area and the Device-Specific Selection area.
8. Device-Type Selection Box-this area contains the available types of devices and connections in Packet Tracer. The Device-Specific Selection area changes depending on the selected device
9. Device-Specific Selection Box-this area is used to select specific devices and connections needed to build in the network workspace.
10. User Created Packet Window-this window manages packets that were created on the network during the scenario simulation.

To create a topology, select a device from the Network Component panel, and then select the device type from the Device-Type Selection panel. After that, click the left mouse button in the workspace field. You can also move the device directly from the Device-Type Selection area, but the default device model will be selected.

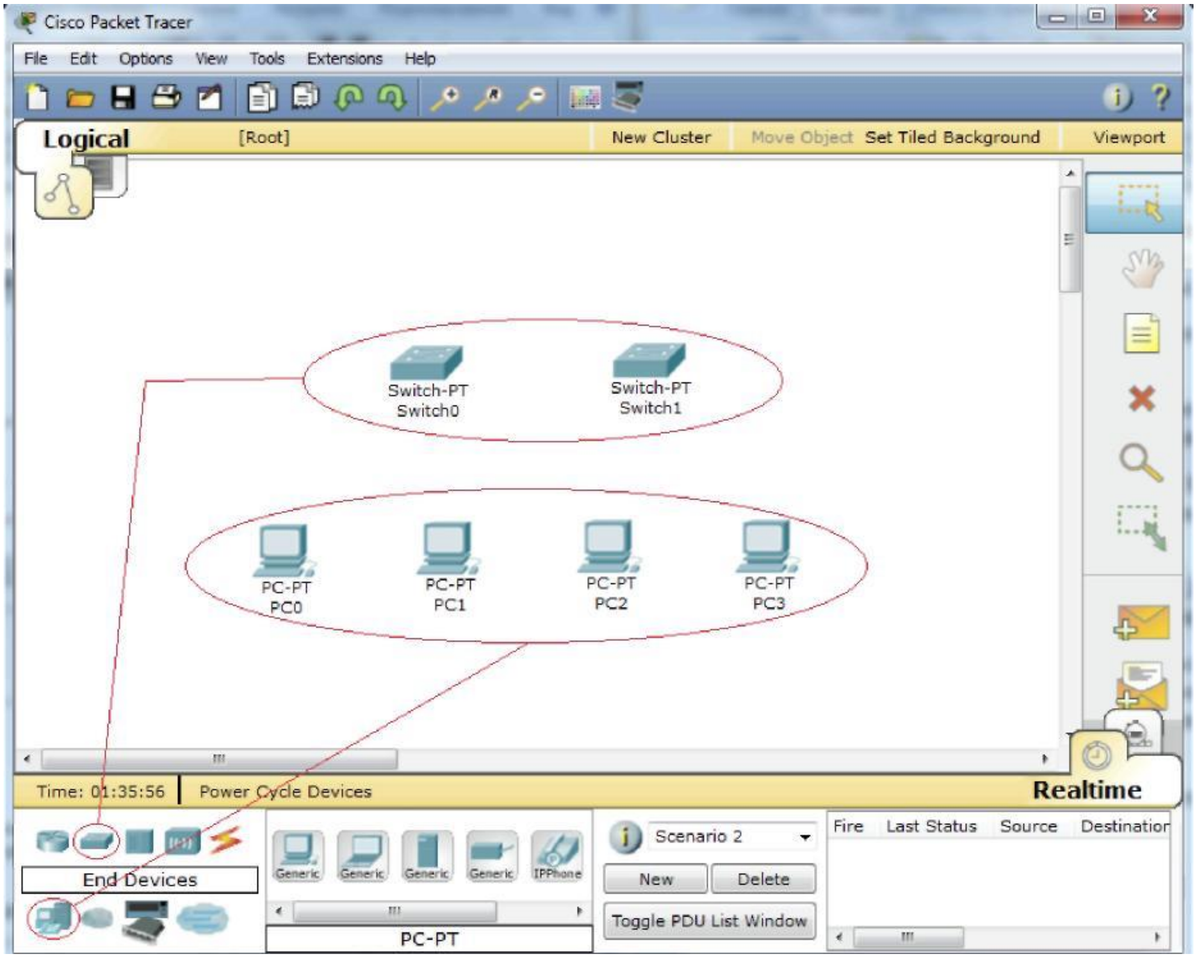
To quickly create multiple instances of the same device, hold down the Ctrl key, click on the device in the Device-Specific Selection area, and then release the Ctrl key. After that, you can click several times on the workspace to add copies of the device.

Packet Tracer provides the following types of devices:

- Routers;
- Switches (including bridges);

- Hubs and repeaters;
- End devices-PCs, servers, printers, GP phones;
- Wireless devices: access points and wireless router;
- Other devices - cloud, DSL modem, and cable modem.

Adding the necessary elements to the program workspace



When you add each item the user has the option to give it a name and set the required parameters. To do this, click on the desired element with the left mouse button (LCM) and go to the Config tab in the device dialog box.

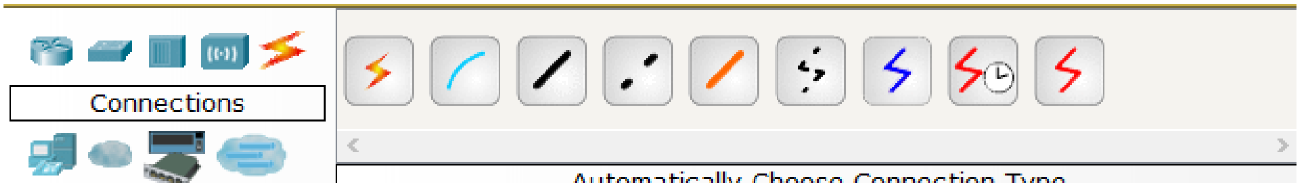
The properties dialog box for each element has two tabs:

- Physical-contains the graphical interface of the device and allows you to simulate working with it on the physical level.
- Config-contains all the necessary parameters for configuring the device and has a user-friendly interface.

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

To delete unnecessary devices from the program workspace, use the Delete (Del) button.

We will link the added elements using connecting links. To do this, select the Connections tab from the Network Component Box panel. We will see all possible types of connections between devices. Select the appropriate cable type. The mouse pointer changes to the "connection" cursor (it looks like a connector). Click on the first device and select the appropriate interface to connect to, and then click on the second device, performing the same operation. You can also connect using the Automatically Choose Connection Type (automatically connects items in the network). Select and click on each of the devices that you want to connect. A cable connection will appear between the devices, and indicators at each end will show the connection status (for interfaces that have an indicator).



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

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

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

You can connect switches or routers to the ICS by clicking on the required device and going to the CLI tab in the properties window.

To simulate the operation of the command line on the target device (computer), select the Desktop tab in the properties, and then click the Command Prompt shortcut.

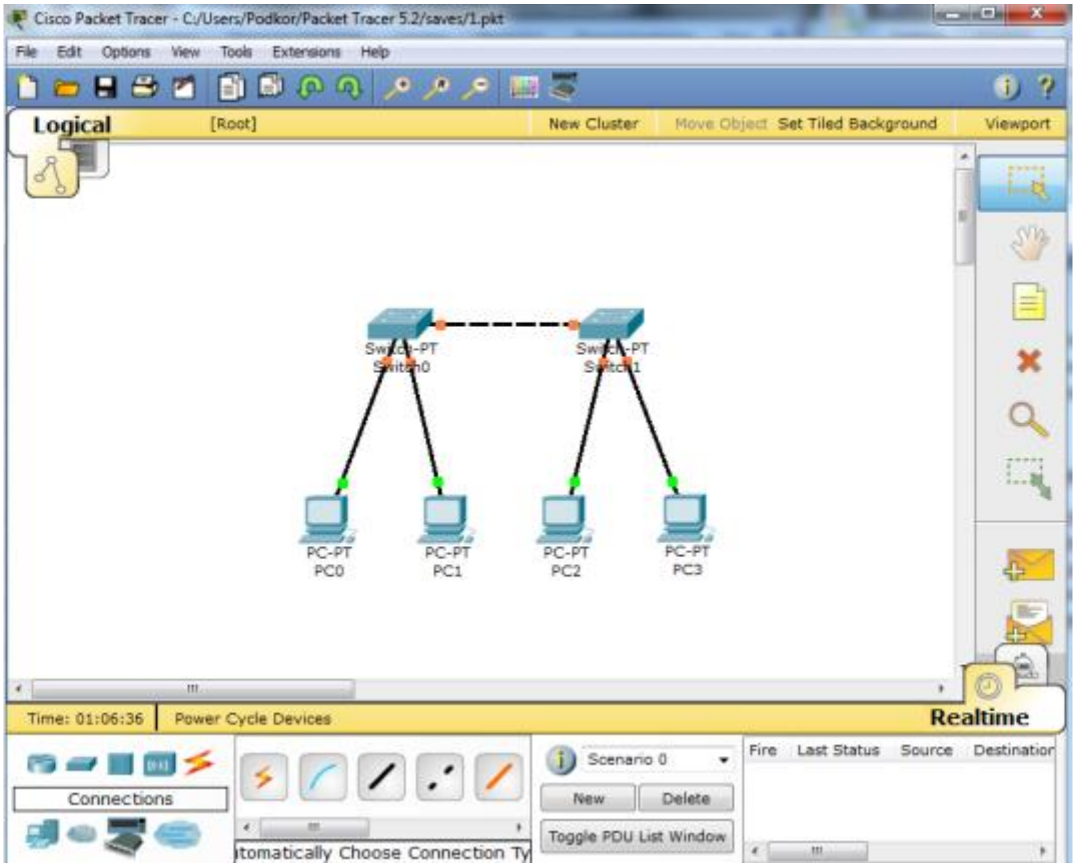
Working with files in the simulator

Packet Tracer allows the user to store the configuration of certain devices, such as routers or switches, in text files. To do this, go to the properties of the required device and click the "Export..." button in the Config tab to export the Startup Config or Running Config configuration. So we get a dialog box for saving the necessary configuration to a file that will have the extension *. txt. Text of the device configuration file running-config.txt (default name) is similar to the text of information received when using the show running-config command on IOS devices.

Note that the configuration of each device is saved in a separate text file. The user can also change the configuration in the saved file manually using a custom text editor. To provide the device with saved or edited settings, click the "Load..." button in the Config tab to load the required Startup Config configuration, or the "Merge..." button to load the Running Config configuration.

Практическая часть

Add 2 Switch-PT switches to the program workspace. By default, they have names - Switch and Switch 1. Add to the working field four computers with the default names RSO, PCI, PC2, RSZ. Connect the devices to an Ethernet network, as shown here:



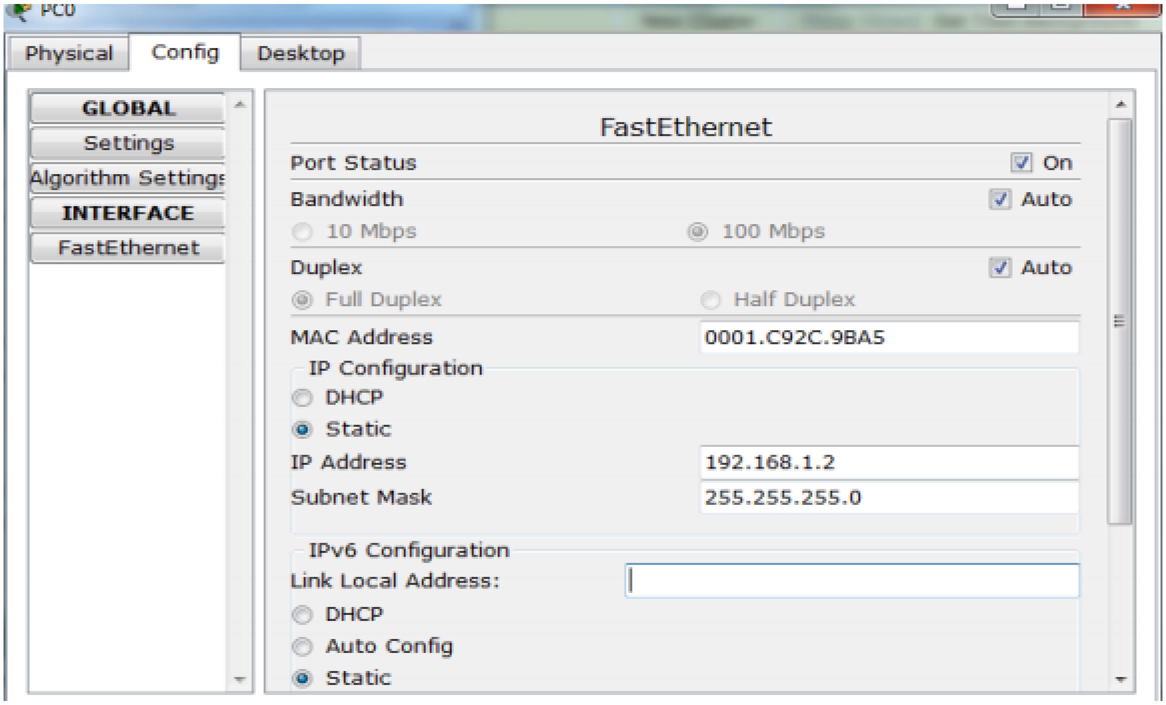
Save the created topology by clicking the Save button (in the File -> Save menu).

Open the properties of the RSO device by clicking on its image. Go to the Desktop tab and simulate run by clicking Command Prompt.

We get a list of commands if we enter "? " and press Enter. To configure the computer, use the ipconfig command from the command line, for example:

```
ipconfig 192.168.1.2 255.255.255.0
```

You can also enter the IP address and network mask in the convenient graphical interface of the device. Gateway default gateway-GATEWAY ADDRESSES are NOT IMPORTANT, since the network you are creating does not require routing.



FastEthernet

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

● Full Duplex ○ Half Duplex

MAC Address: 0001.C92C.9BA5

IP Configuration

○ DHCP

● Static

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

IPv6 Configuration

Link Local Address:

○ DHCP

○ Auto Config

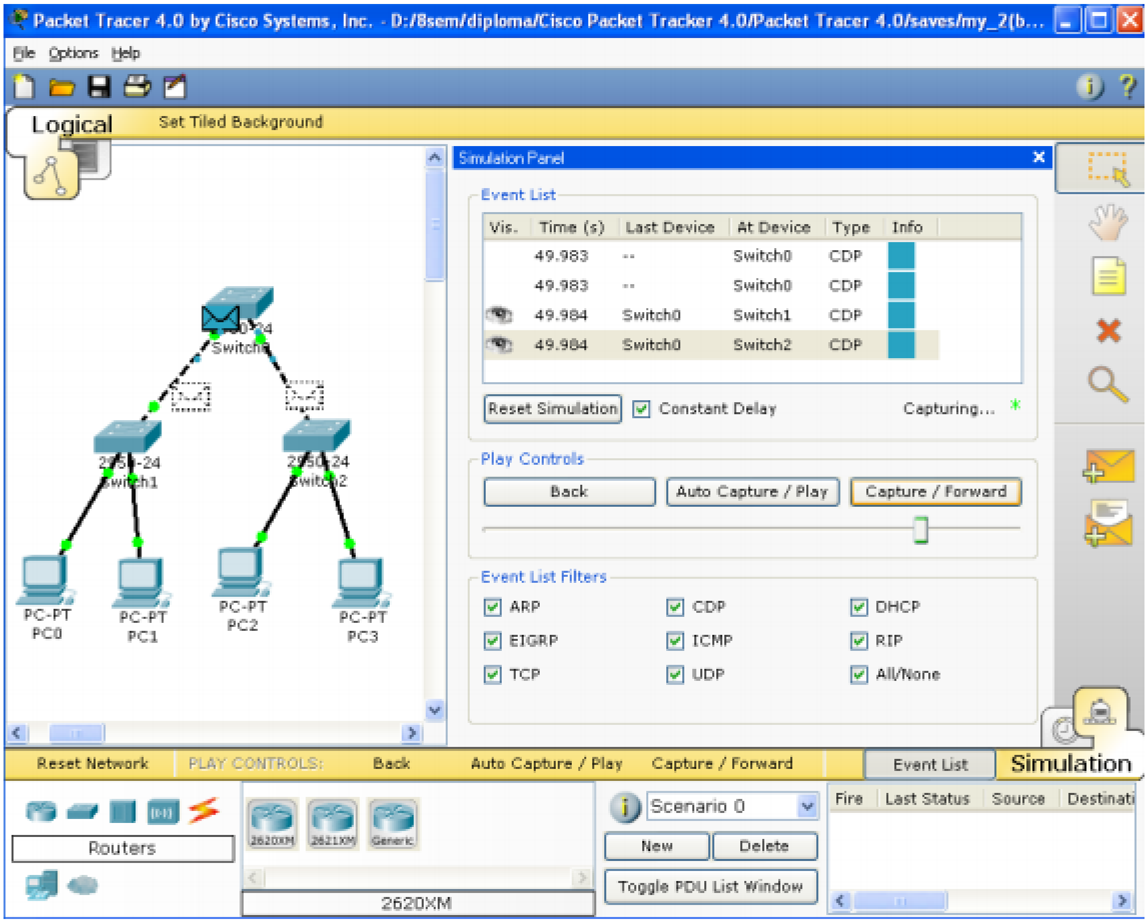
● Static

We will configure each host in the same way.

Устройство	IP ADRESS	SUBNET MASK
PCO	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

On each computer, view the assigned addresses with the *ipconfig* command without parameters.

Packet Tracer 5 provides a simulation mode that describes and shows in detail how the Ping utility works. Therefore, you need to switch to this mode by clicking on the icon of the same name in the lower-left corner of the workspace, or by using the Shift+s key combination. The "modeling Panel" opens, which displays all events related to the ping process execution.



Vis.	Time (s)	Last Device	At Device	Type	Info
	49.983	--	Switch0	CDP	■
	49.983	--	Switch0	CDP	■
👁	49.984	Switch0	Switch1	CDP	■
👁	49.984	Switch0	Switch2	CDP	■

☑ Constant Delay

☑ ARP ☑ CDP ☑ DHCP
☑ EIGRP ☑ ICMP ☑ RIP
☑ TCP ☑ UDP ☑ All/None

The modeling panel

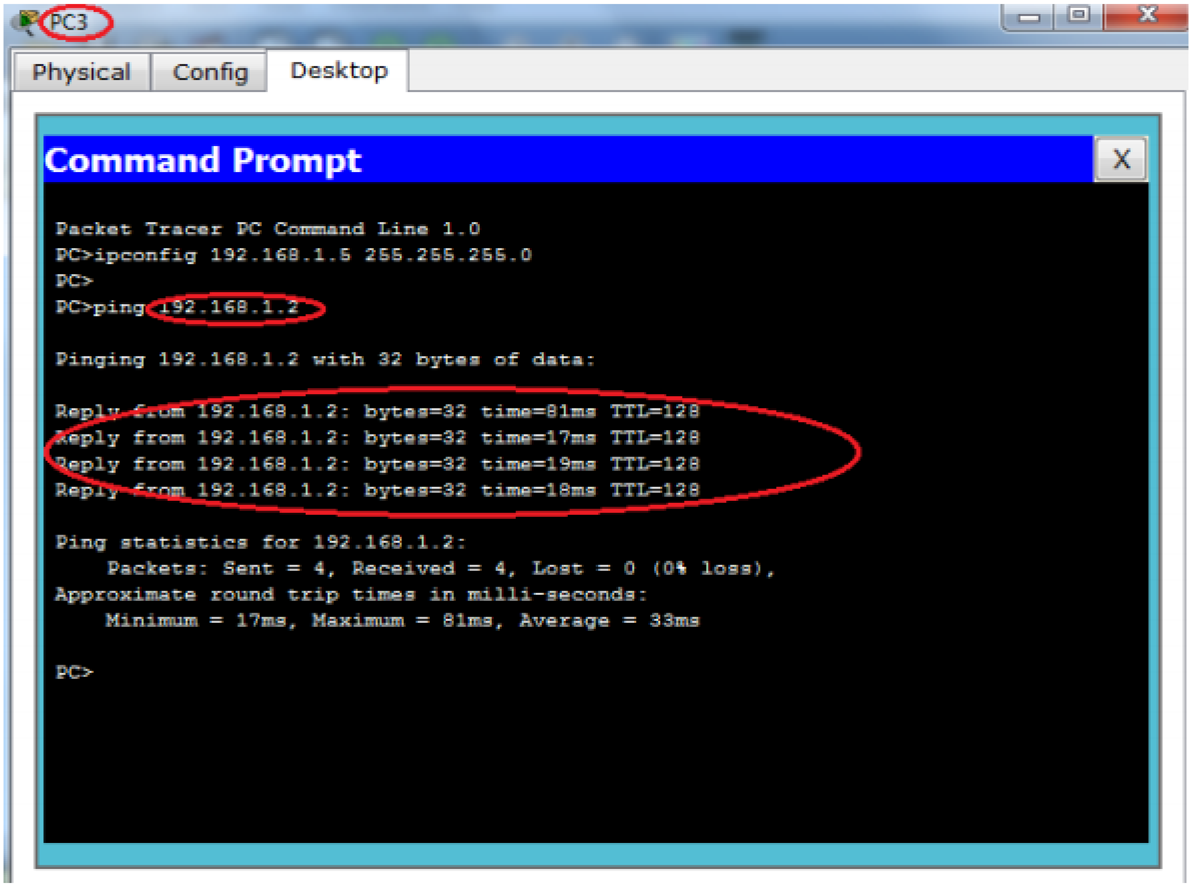
Now you need to start the ping process again. After starting it, you can move the "modeling Panel" to monitor the sending/receiving of packets on the diagram of the designed network.

The "Automatic" button implies modeling the entire ping process in a single process, while" step-by-Step " allows you to display it step-by-step.

To find out the information that the package contains and its structure, just right-click on the colored square in the "Information" column.

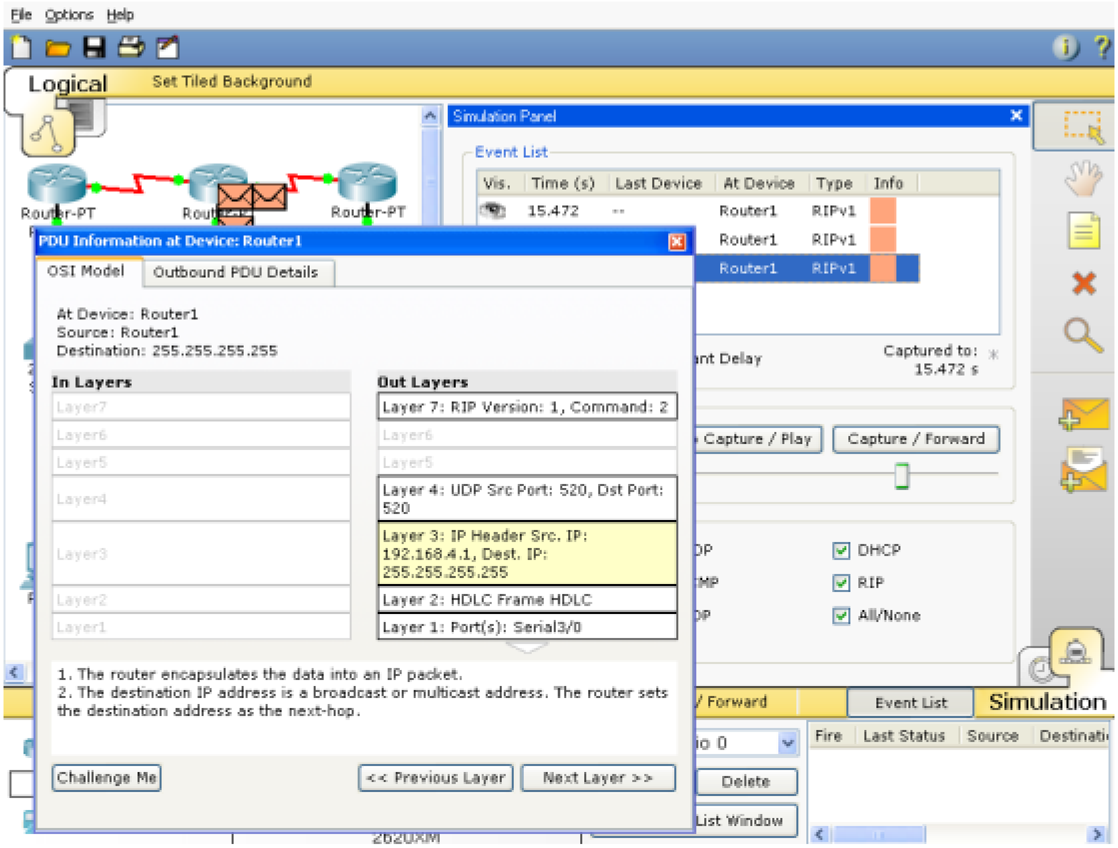
The simulation stops either when the ping process is completed or when the corresponding workstation's Edit window is closed.

If everything is done correctly, we can ping any of any computer. For example, go on the computer PC3 and make *ping* to computer PC0. We should see a ping report similar as here:



```
Packet Tracer PC Command Line 1.0
PC>ipconfig 192.168.1.5 255.255.255.0
PC>
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=81ms TTL=128
Reply from 192.168.1.2: bytes=32 time=17ms TTL=128
Reply from 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 81ms, Average = 33ms

PC>
```

However, this is not all the advantages of Packet Tracer: in "simulation Mode" you can not only track the protocols used, but also see which of the seven levels of the OSI model this Protocol is used:



Vis.	Time (s)	Last Device	At Device	Type	Info
👁	15.472	--	Router1	RIPv1	🟧
			Router1	RIPv1	🟧
			Router1	RIPv1	🟧

Captured to: 15.472 s

PDU Information at Device: Router1

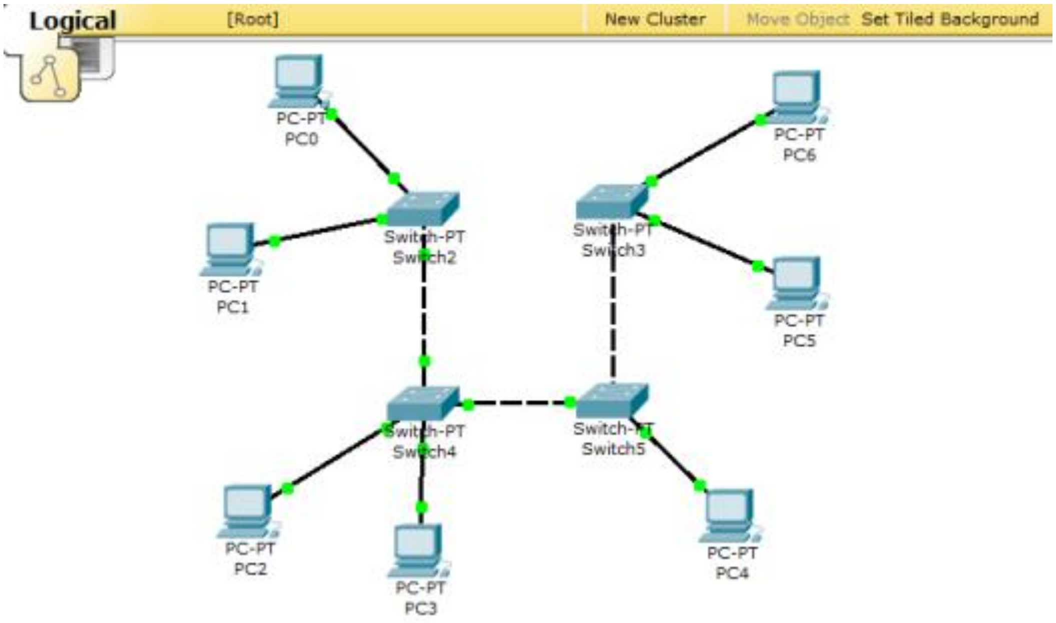
At Device: Router1
Source: Router1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer 7: RIP Version: 1, Command: 2
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 520, Dst Port: 520
Layer3	Layer 3: IP Header Src. IP: 192.168.4.1, Dest. IP: 255.255.255.255
Layer2	Layer 2: HDLC Frame HDLC
Layer1	Layer 1: Port(s): Serial3/0

1. The router encapsulates the data into an IP packet.
2. The destination IP address is a broadcast or multicast address. The router sets the destination address as the next-hop.

TASK FOR INDEPENDENT WORK:

1. Create a topology in figure



2. Assign addresses to computers, according to option “v”. “v” – is your last digit of your HDU ID.

For example, for option 7 (v=7) and PC5 computer, we have IP ADDRESS 70.7.1.5, SUBNET MASK - 255.255.255.0.

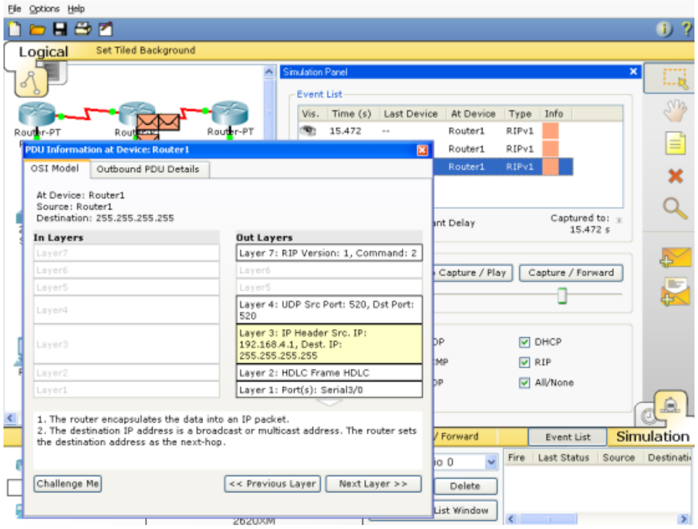
Host	IP ADDRES	SUBNET MASK
PC1	v*10. v.1.1	255.255.255.0
PC2	v*10. v.1.2	
PC3	v*10. v.1.3	
PC4	v*10. v.1.4	
PC5	v*10. v.1.5	
PC6	v*10. v.1.6	

If you have done everything correctly you will be able to ping any computer from any.

3. Run the ping utility, according to the table.

Variant v	Ping from	Ping to	Variant v	Ping from	Ping to
1	PC1	PC6	8	PC6	PC5
2	PC2	PC6	9	PC1	PC6
3	PC3	PC1	0	PC2	PC6
4	PC4	PC2			
5	PC5	PC3			
6	PC6	PC4			
7	PC6	PC5			

4. In" simulation Mode", track the movement of packets and the protocols used (see figure)



Vis.	Time (s)	Last Device	At Device	Type	Info
	15.472	--	Router1	RIPv1	
			Router1	RIPv1	
			Router1	RIPv1	

Captured to: 15.472 s

PDU Information at Device: Router1

At Device: Router1
Source: Router1
Destination: 255.255.255.255

In Layers	Out Layers
Layer7	Layer 7: RIP Version: 1, Command: 2
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 520, Dst Port: 520
Layer3	Layer 3: IP Header Src. IP: 192.168.4.1, Dest. IP: 255.255.255.255
Layer2	Layer 2: HDLC Frame HDLC
Layer1	Layer 1: Port(s): Serial3/0

1. The router encapsulates the data into an IP packet.
2. The destination IP address is a broadcast or multicast address. The router sets the destination address as the next-hop.

5. Switching to "Simulation Mode" to review and explain the process of data exchange over the ICMP Protocol between devices (by executing the *Ping* command from one computer to another item. Include a detailed explanation in the report.

6. Make sure that all network objects are reachable using the IP Protocol.

7. Make screenshots and add to report. Write your explanation on item 5.

Answer on the questions:

1. What is difference between hub and switch?
2. What layer of OSI model is used for the switching?
3. Describe the aims of subnet mask?
4. Do we have one subnetwork or 4 (because we have 4 switches)? Explain.
5. What will happen if we will change the address of PC6 to v*10. v.2.6 and make ping-request from PC1 to PC6? Is it successful or not? Explain, please, why?

REPORT

After completion the task the students need to submit:

- **The format of the report file is *pdf*.**
- Upload reports for the GitLab repository (to your personal project)
- Do not forget to write your name and ID inside the report

HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

COMPUTER NETWORKS

LAB 1 (part 2)

A SIMPLE NETWORK ROUTING

HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

GOAL: to study the simulation mode of Cisco Packet Tracer, ARP and ICMP protocols on the example of $ping$ and $tracert$ commands.

PLAN:

1. Building a network topology, configuring end nodes;

2. To configure the router;

3. Checking network operation in simulation mode;

4. Sending ping inside the network;

5. sending a ping request to an external network;

6. Sending ping request to a nonexistent IP address of the host;

7. Completing an individual task.

THEORETICAL PART:

The ARP Protocol

The address Resolution Protocol (ARP) is used to determine a physical address from an IP address. The ARP Protocol works in different ways depending on which link layer Protocol is running on the given network with the ability to broadcast access to all network nodes simultaneously.

The ARP Protocol allows you to dynamically determine the MAC address by IP address. A MAC address is a unique serial number assigned to each network device to identify it in the network, also called a physical or hardware address. The LAN Protocol supported in the lab is Ethernet. In Ethernet networks that use the TCP/IP stack, the network interface has a 48-bit physical address. Frames exchanged at the link layer must contain the hardware address of the network interface. However, TCP / IP uses its own addressing scheme: 32-bit IP addresses. The value of the receiver's IP address is not sufficient to send a datagram to this host. The Ethernet driver must know the MAC address of the destination interface in order to send data there. The task of ARP is to provide dynamic correspondence between 32-bit IP addresses and 48-bit MAC addresses used by various network technologies. The ARP Protocol works within a single subnet and automatically starts when it is necessary to convert an IP address to a hardware address.

A node that needs to map an IP address to a local address generates an ARP request, inserts it into a link-layer Protocol frame, specifying a known IP address in it, and sends the request broadcast. All local network nodes receive an ARP request and compare the IP address specified there with their own. If they match, the node generates an ARP response, in which it specifies its IP address and its local address, and sends it already directionally, since the sender specifies its local address in the ARP request.

In order to reduce the number of ARP requests sent, each device on the network that uses the ARP Protocol must have a special buffer memory. It stores address pairs (IP address, physical address) of devices on the network. Whenever the device receives an ARP response, it stores the corresponding pair in buffer memory. If the address is in the list of pairs, there is no need to send an ARP request. This buffer memory is called an ARP table.

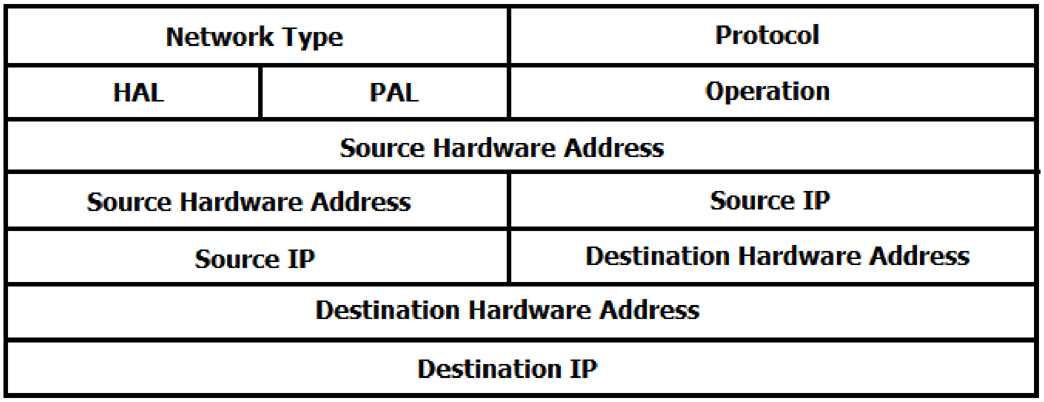
An ARP table can contain both static and dynamic entries. Dynamic entries are added and deleted automatically, while static entries are entered manually.

Since most devices on the network support dynamic address resolution, the administrator usually does not need to manually specify ARP Protocol entries in the address table.

Each entry in the ARP table has its own lifetime. ARP table cleanup policies are dictated by the operating system used. When you add an entry, a timer is activated for it.

ARP messages are encapsulated in the frame data field when transmitted over the network. They do not contain an IP header. Unlike most protocols, ARP messages do not have a fixed header format. This is because the Protocol was designed so that it is applicable to address resolution in various networks.

ARP requests and responses use the same packet format. Since local addresses can have different lengths in different types of networks, the format of the ARP Protocol packet depends on the type of network. Figure shows the structure of the request and response package.



Network Type		Protocol
HAL	PAL	Operation
Source Hardware Address		
Source Hardware Address		Source IP
Source IP		Destination Hardware Address
Destination Hardware Address		
Destination IP		

* Network Type – type of channel Protocol

For Ethernet-1.

• Protocol - the network layer Protocol

• HAL - length of the channel address

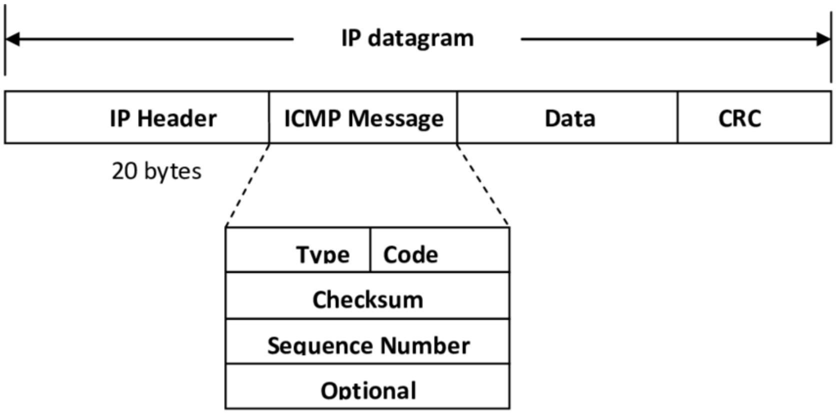
* PAL-length of the network address

• Operation - type of operation (1-request, 2-response)

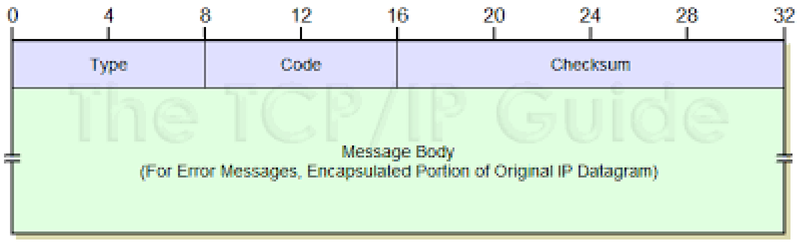
The node that sends the ARP request fills in all fields in the packet, except for the local address field that is being searched for. The value of this field is filled in by the host that recognized its IP address.

The ICMP Protocol

The ICMP Protocol is used for transmitting control and diagnostic messages. It is used to send messages about errors, as well as situations that require special attention. The Protocol belongs to the network layer of the TCP/IP model. ICMP messages are generated and processed by network (IP) and higher-level protocols (TCP or UDP). When some ICMP messages appear, error messages are generated and passed to user processes. ICMP messages are transmitted inside IP datagrams:



The format of the ICMP message is shown in figure. The ICMP header includes 8 bytes, but only the first 4 bytes are the same for all messages, and the rest of the message header and body fields are determined by the message type.

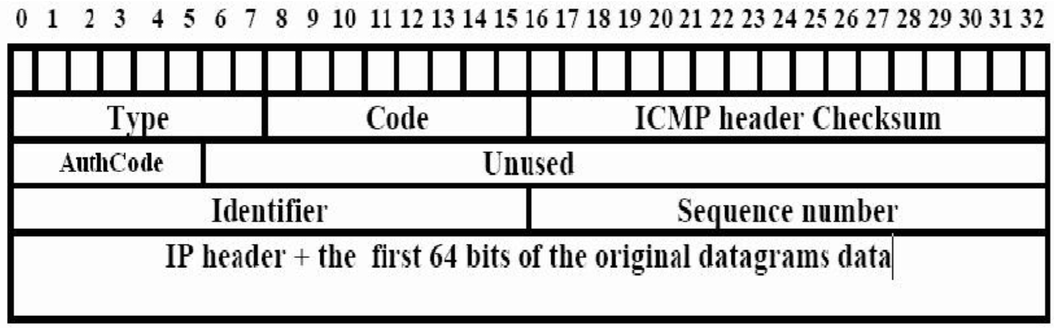

0
4
8
12
16
20
24
28
32
Type
Code
Checksum
The TCP/IP Guide
Message Body
(For Error Messages, Encapsulated Portion of Original IP Datagram)

The checksum field covers the entire ICMP message.

The message type is determined by the value of the “Type” field in the header. Some types of ICMP messages have internal granularity (code), and the specific type of message is determined by both the message type and the message code. For more information about types and codes of ICMP messages, see the ICMP Protocol specification RFC 792. [Electronic resource]. URL: http://tools.ietf.org/html/rfc792.

Ping program

The *ping* program was designed to check the availability of a remote host. The program sends an ICMP echo request to the node and waits for the ICMP echo response to return. The hing program is usually the first diagnostic tool that begins identifying a problem in networks. In addition to availability, you can use ping to estimate how long it takes for a packet to return from a node, which gives you an idea of "how far away" the node is. In addition, Ping has options for recording the route and timestamp. The echo request and echo response messages have the same format:



- • Type – type of package
- 8-echo request
- 0 – response to the echo request
- * Code-decryption of the packet destination inside the type (in this case 0)
- * The checksum is calculated for the entire package
- * ID (identifier) – number of the message stream
- * Serial number – the number of the packet in the stream

Just as with other ICMP requests, the echo response must contain the ID and sequence number fields. In addition, any additional data sent by the computer must be echoed.

The ID field of the ICMP message sets the ID of the process sending the request. This allows the ping program to identify the returned response if multiple ping programs are running on the same host at the same time.

The sequence number starts at 0 and is incremented each time the next echo request is sent.

How the ping program works you studied in the lab 1

Tracert program

The tracert program allows you to view the route that IP datagrams travel from one host to another.

The tracert program does not require any special server applications. It uses standard functions of the ICMP and IP protocols. To understand how the program works, remember how to process the TTL field in the IP datagram header.

Each router that processes a datagram reduces the value of the TTL field in its header by one. When a datagram with a TTL of 1 is received, the router destroys it and sends an ICMP "time expired"message to the host that sent it. However, the datagram containing this ICMP message has the router's IP address as the source address.

This is what is used in the tracert program. An IP datagram is sent to the destination host with the TTL field set to one. The first router on the path of the datagram, destroys it (since TTL is 1) and sends an ICMP message about the expiration of time. This determines the first router in the route. Tracert then sends a datagram with a TTL field of 2, which allows you to get the IP address of the second router. Similar actions continue until the datagram reaches the destination host. When a response is received from this node, the tracing process is considered complete.

The first line, without a number, contains the name and IP address of the destination and indicates that the TTL value cannot be greater than 30.

The following output lines start with a printout of the TTL value (1, 2, 3, etc.) and contain the name (IP address) of the host or router and the time when the ICMP message was returned.

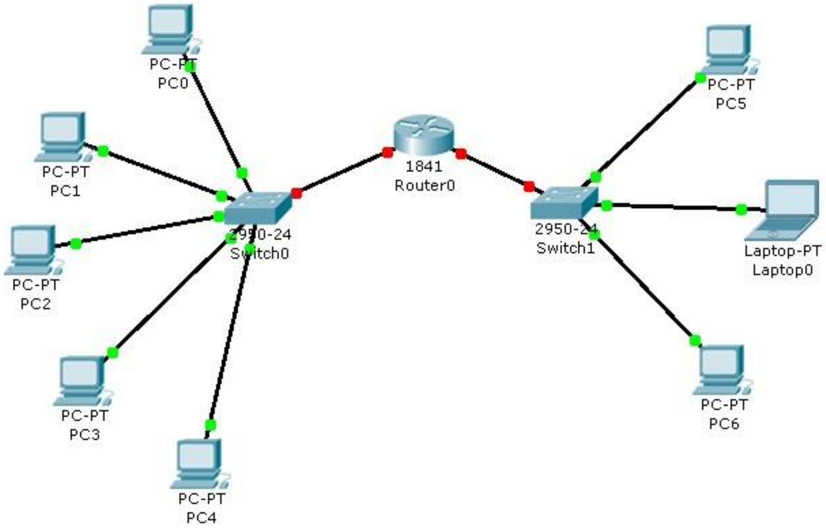
For each TTL value, 3 datagrams are sent. For each returned ICMP message, the return time is calculated and printed.

If a response to a datagram is not received within five seconds, an asterisk is printed and the next datagram is sent.

PRACTICAL PART

1. Creating a network topology

At the end of the first part, we created the following network topology, consisting of end nodes (PCs), switches, and a router:



The workspace view

Router 0 Router has two interfaces and connects the two subnets. Let’s configure the end nodes.

2. Configuring the end nodes

On PC0-PC4 devices, set the specified IP addresses and subnet mask (table 1). the gateway IP address for all nodes is 192.168.3.1. the DNS server IP address is optional, because it will not be used in this work.

Table 1

Host	IP-address	Subnet mask
PC0	192.168.3.3	255.255.255.0
PC1	192.168.3.4	255.255.255.0
PC2	192.168.3.5	255.255.255.0
PC3	192.168.3.6	255.255.255.0

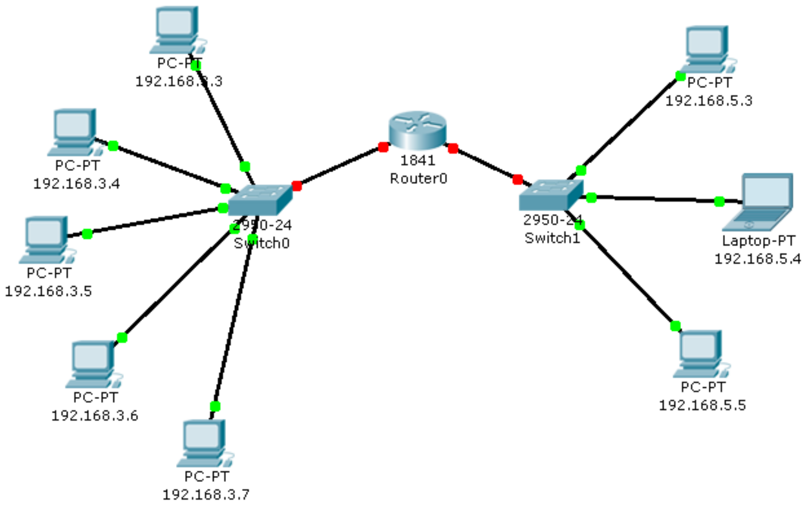
PC4	192.168.3.7	255.255.255.0

On PC 5, Laptop 0, and PC6 devices, set the specified IP addresses and subnet mask (table 2). the gateway IP address for all nodes is 192.168.5.1. the DNS server IP address is optional.

Table 2

Host	IP-address	Subnet mask
PC5	192.168.5.3	255.255.255.0
Laptop0	192.168.5.4	255.255.255.0
PC6	192.168.5.5	255.255.255.0

Rename each node by its own IP address, and you will get the following:



The workspace view

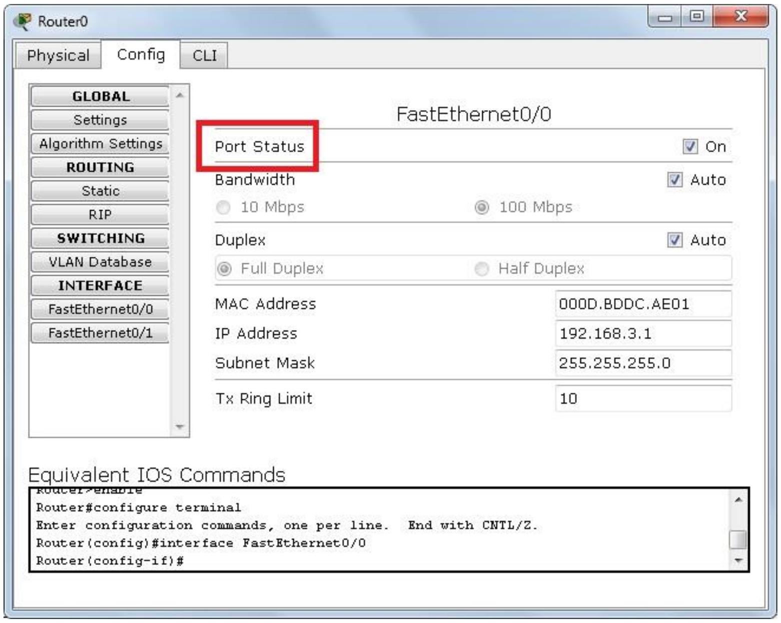
3. Configuring the router

When configuring end nodes, it was already mentioned that the router in this network topology has two interfaces. Configuring the fastethernet0/0 interface:

1) One click on the device (router);
2) Select the “Config " tab”;

3) Find the fastethernet0/0 interface, set the desired IP address and subnet mask.

Important: the router interface is disabled by default; you must enable it by clicking the mouse next to”On".



Router0

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1

FastEthernet0/0

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

● Full Duplex ○ Half Duplex

MAC Address 000D.BDDC.AE01

IP Address 192.168.3.1

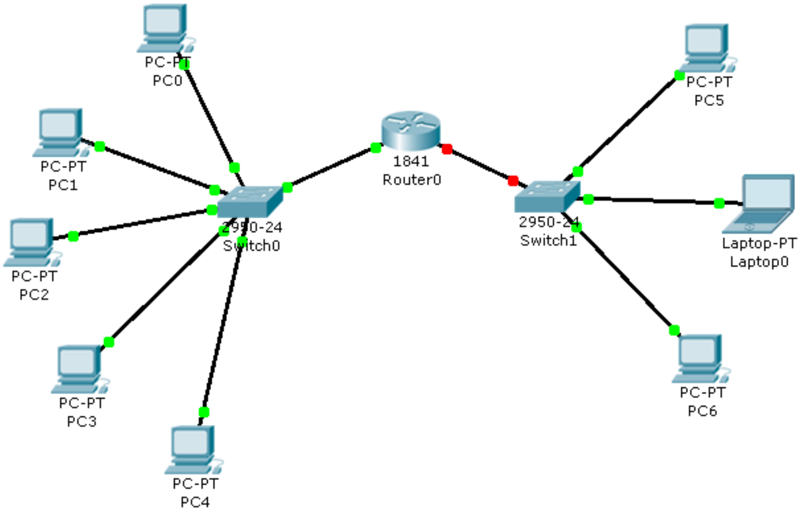
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

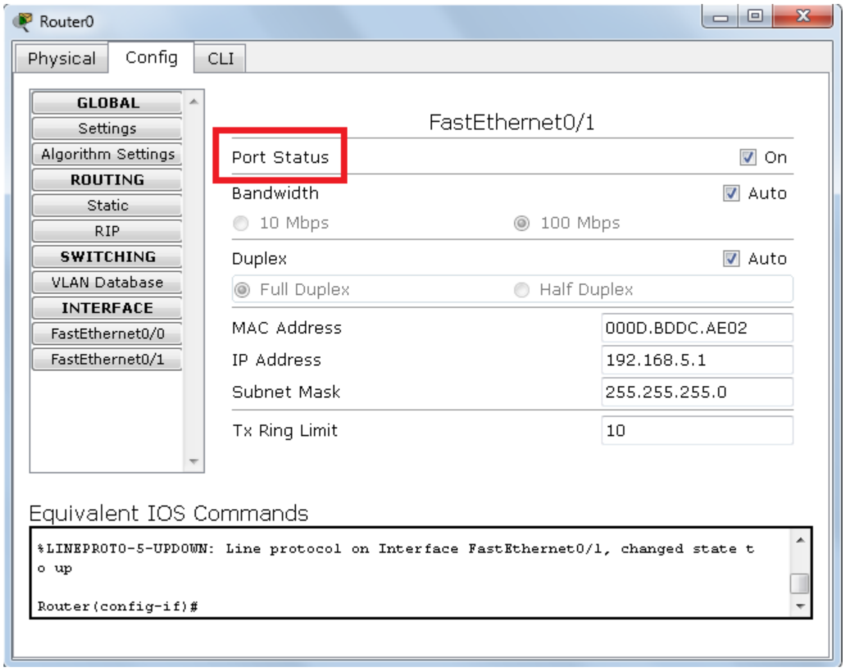
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

4) Close the window and look at the entire network topology. Green status indicators on the link between Router0 and Switch0 indicate that the interface is connected correctly



The workspace view

Similarly, we configure the FastEthernet0/1 interface.



FastEthernet0/1

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

● Full Duplex ○ Half Duplex

MAC Address 000D.BDDC.AE02

IP Address 192.168.5.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up

Router(config-if)#
```

You can add labels to the router interfaces using the Place Note tool in the Common Tools panel . You need to click on the tool, then click in the right place on the workspace.

4. Simulation mode Cisco Packet Tracer

Make sure that you are in simulation mode. To do this, click on the simulation icon in the lower-right corner of the simulator workspace. Simulation

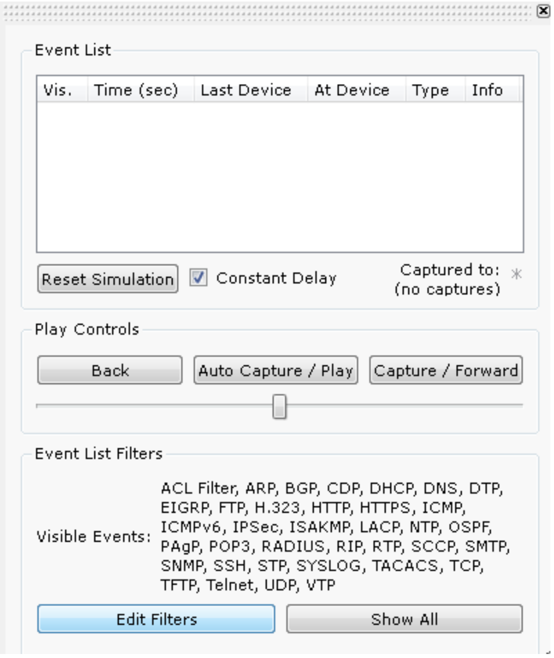
The event window opens, where you will see a list of events, control buttons, and the specified filters. By default, the packets of all possible protocols are filtered, i.e. they will be displayed. you need to correct and limit this list to the protocols under investigation.

Control buttons:

• Back – to-back

* Auto Capture / Play-automatically capture packets from source to receiver and back

* Capture/Forward-capture packets only from one device to another



☑ Constant Delay

Captured to: (no captures)

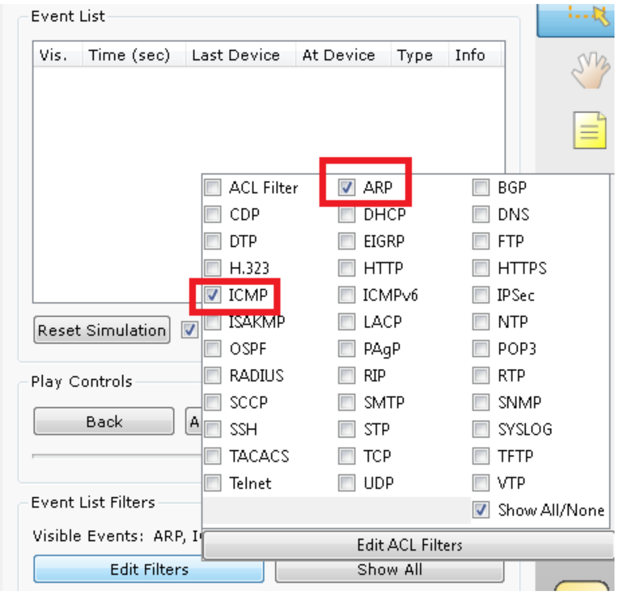
Visible Events: ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PAgP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Figure – Event List

In this part, we are interested in two types of ARP and ICMP packets.

Therefore, you need to set a filter only for messages of the specified type:

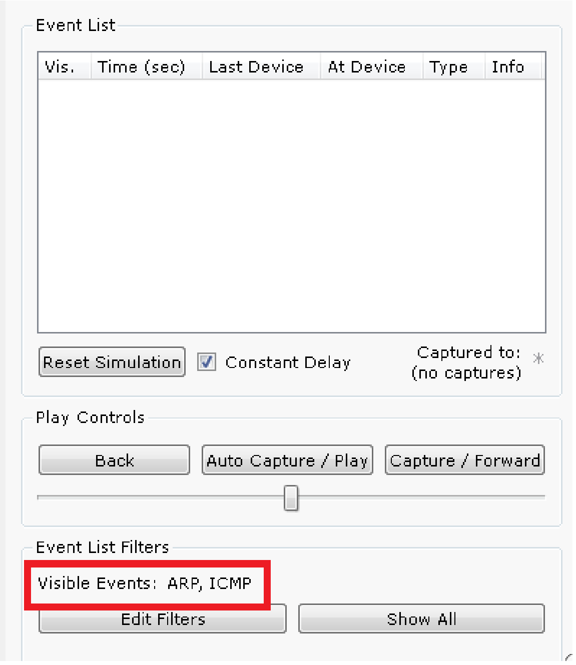
1) Click on the "Edit Filters" button”
2) Remove the label from " Show All/None”
3) Select ARP and ICMP



☐ ACL Filter	☑ ARP	☐ BGP
☐ CDP	☐ DHCP	☐ DNS
☐ DTP	☐ EIGRP	☐ FTP
☐ H.323	☐ HTTP	☐ HTTPS
☑ ICMP	☐ ICMPv6	☐ IPSec
☐ ISAKMP	☐ LACP	☐ NTP
☐ OSPF	☐ PAgP	☐ POP3
☐ RADIUS	☐ RIP	☐ RTP
☐ SCCP	☐ SMTP	☐ SNMP
☐ SSH	☐ STP	☐ SYSLOG
☐ TACACS	☐ TCP	☐ TFTP
☐ Telnet	☐ UDP	☐ VTP
		☑ Show All/None

Visible Events: ARP, I

4) Make sure that the specified filtering protocols are assigned



☑ Constant Delay

Captured to: (no captures)

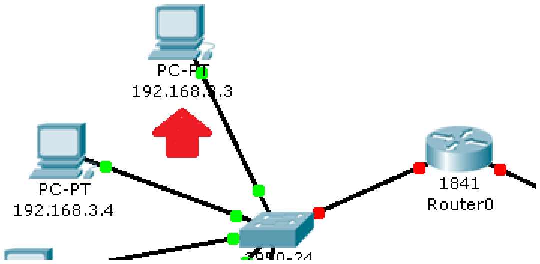
Visible Events: ARP, ICMP

5. Verification of network operation in the simulation mode

Send a test ping request from the destination node with the IP address 192.168.3.3 to the host with the IP address 192.168.3.5.

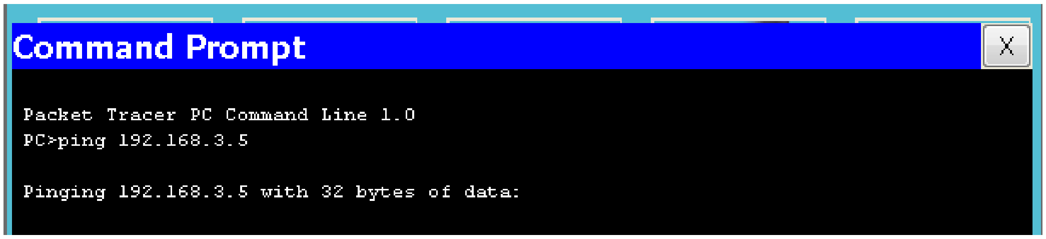
Important: both nodes are located within the same network segment

1) One click on the selected device



Choise of PC-PT 192.168.3.3

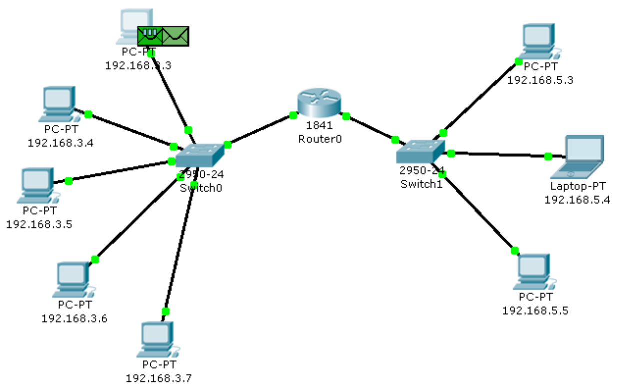
2) Select the Desktop tab, which contains simulators of some programs available on your computer
3) Select "Command Prompt", a program that simulates the computer's command line.
4) Use the ping utility to send a ping request. (Don't forget to press “Enter”).



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:
```

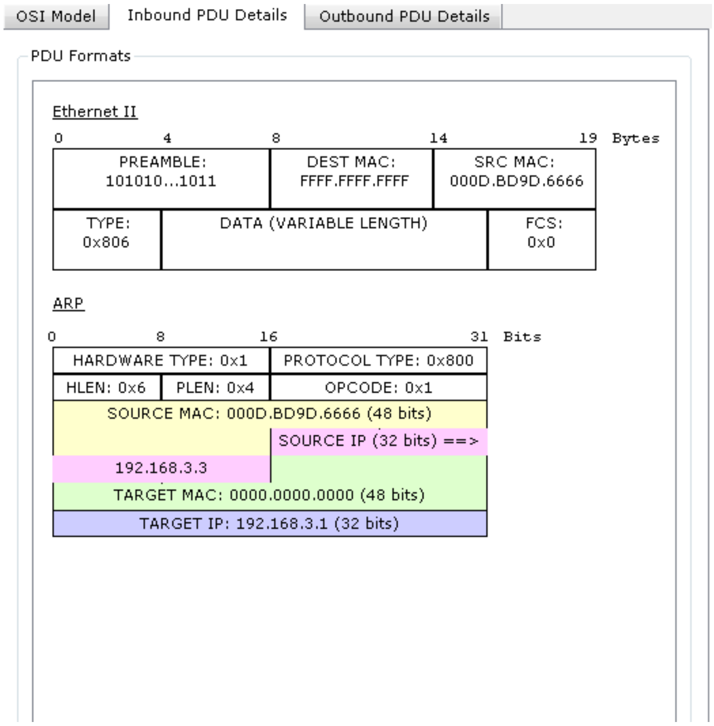
Host 192.168.3.3command promt

Two ARP and ICMP Protocol packets are generated on the source device. an ARP request is always generated when a host tries to communicate with another host.



The workspace view

Click on the “Auto Capture/play” or “Capture/Forward " button, the latter will allow you to control the movement of packets from device to device yourself. We see that the ARP Protocol packet is sent first, since the ARP table of the host 192.168.3.3 is empty, and it still "does not know" who to send the ping request to. Make a single click on the package itself (the envelope) and see what levels of the OSI model are involved. Go to the “Inbound PDU Details " tab, which contains the packet structure.



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000D.BD9D.6666

TYPE: 0x806	DATA (VARIABLE LENGTH)	FCS: 0x0

ARP

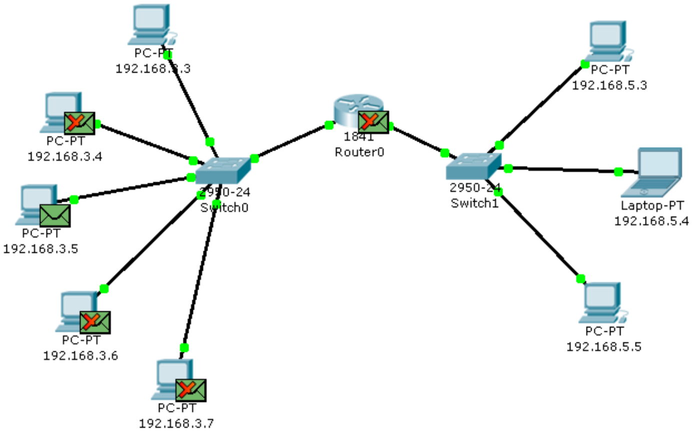
0 8 16 31 Bits

HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1
SOURCE MAC: 000D.BD9D.6666 (48 bits)		
		SOURCE IP (32 bits) ==>
192.168.3.3		
TARGET MAC: 0000.0000.0000 (48 bits)		
TARGET IP: 192.168.3.1 (32 bits)		

Format of the ARP request packet

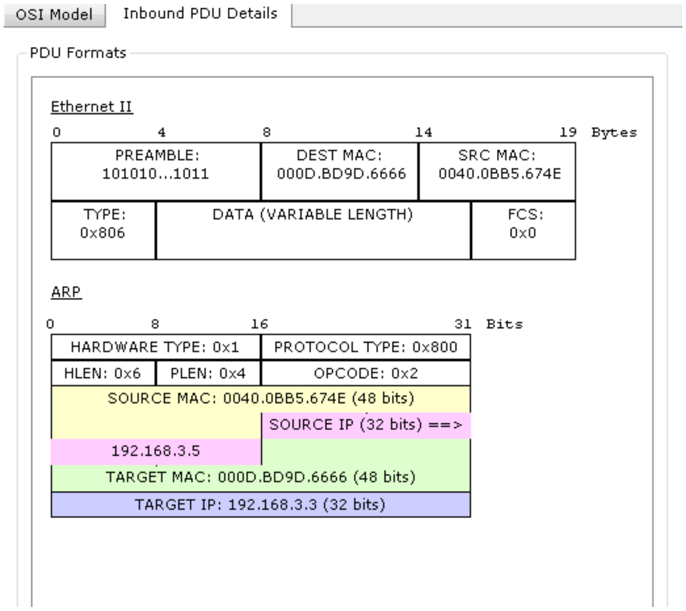
Node 192.168.3.3 has built a request and sends it as a broadcast message to all hosts on the subnet. In addition to the destination IP address, the request contains the sender's IP address and MAC address so that the receiving party can respond.

When viewing the packet flow, make sure that only host 192.168.3.5 responds to the ARP request. Each host in the subnet receives the request and checks its IP address for compliance. If it does not match the specified address in the request, the request is ignored.



The workspace view

View the contents of the ARP response packet sent to host 192.168.3.3.



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: 000D.BD9D.6666	SRC MAC: 0040.0BB5.674E
TYPE: 0x806	DATA (VARIABLE LENGTH)	FCS: 0x0

ARP

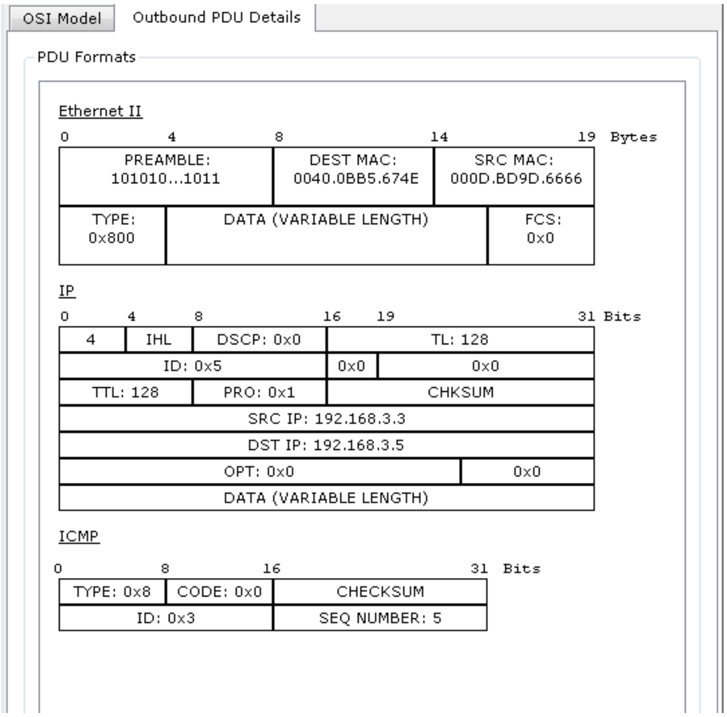
0 8 16 31 Bits

HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2
SOURCE MAC: 0040.0BB5.674E (48 bits)		
		SOURCE IP (32 bits) ==>
192.168.3.5		
TARGET MAC: 000D.BD9D.6666 (48 bits)		
TARGET IP: 192.168.3.3 (32 bits)		

Format of the ARP request packet

Node 192.168.3.5. sent an ARP response directly to the sender using its MAC address, specifying its own MAC address in the “Target MAC " field.

Next, an ICMP ping request message is sent. View the contents of the package by clicking on the package (envelope).



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: 0040.0BB5.674E	SRC MAC: 000D.BD9D.6666
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 128
ID: 0x5		0x0	0x0
TTL: 128	PRO: 0x1	CHKSUM	
SRC IP: 192.168.3.3			
DST IP: 192.168.3.5			
OPT: 0x0			0x0
DATA (VARIABLE LENGTH)			

ICMP

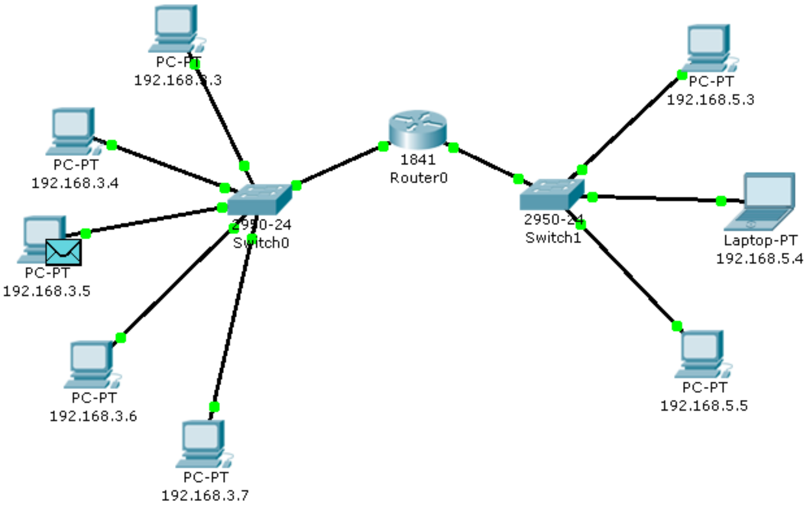
0 8 16 31 Bits

TYPE: 0x8	CODE: 0x0	CHECKSUM
ID: 0x3		SEQ NUMBER: 5

Format of the ICMP echo request packet

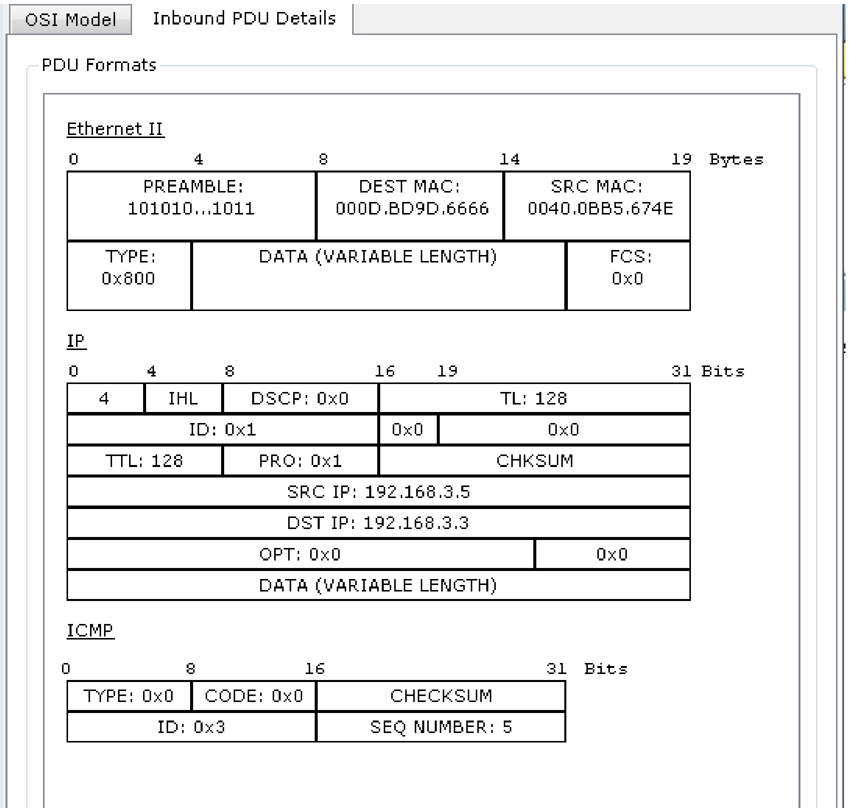
The physical addresses of the nodes are known. The source IP address is 192.168.3.3. the destination IP address is 192.168.3.5. the ICMP message Type is 8 (echo request).

The request is made to the host 192.168.3.5 via the switch:



The workspace view

View the contents of the ping response packet sent to host 192.168.3.3.



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: 000D.BD9D.6666	SRC MAC: 0040.0BB5.674E

TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 128
ID: 0x1		0x0	0x0
TTL: 128	PRO: 0x1	CHKSUM	
SRC IP: 192.168.3.5			
DST IP: 192.168.3.3			
OPT: 0x0			0x0
DATA (VARIABLE LENGTH)			

ICMP

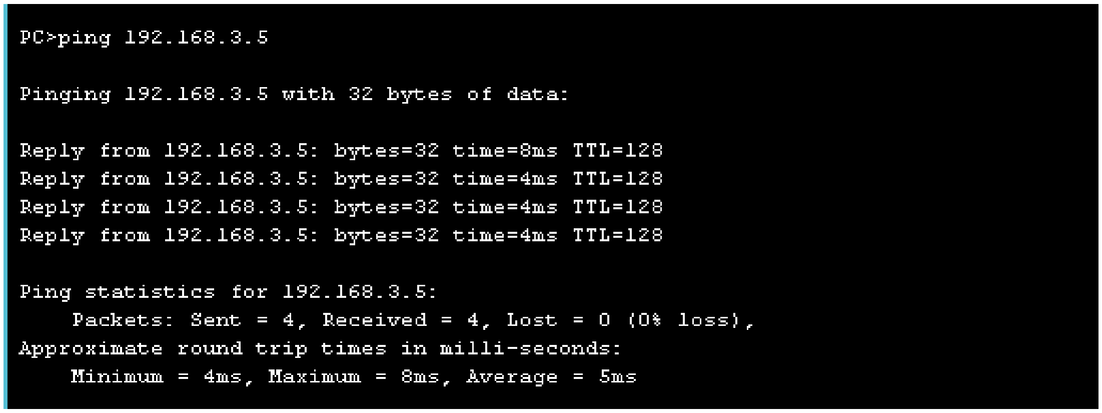
0 8 16 31 Bits

TYPE: 0x0	CODE: 0x0	CHECKSUM
ID: 0x3		SEQ NUMBER: 5

Format of the ICMP echo request packet

IP source address 192.168.3.5. IP destination address – 192.168.3.3. The ICMP message type 0 (echo reply).

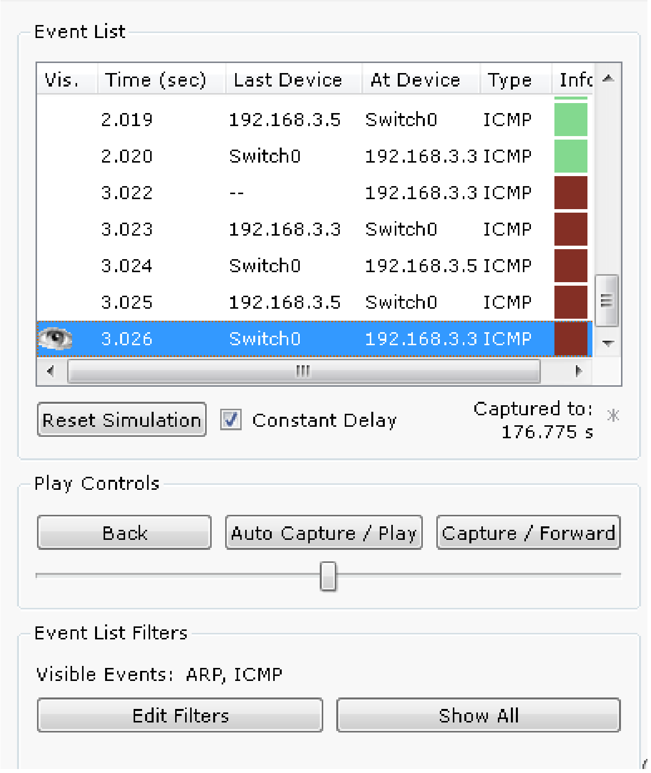
See the ping response in the command line of the host 192.168.3.3.



```
PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=8ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Ping output

The event window also shows the ARP and ICMP request routes: which devices the packets passed through.



Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	2.019	192.168.3.5	Switch0	ICMP	🟩
	2.020	Switch0	192.168.3.3	ICMP	🟩
	3.022	--	192.168.3.3	ICMP	🟥
	3.023	192.168.3.3	Switch0	ICMP	🟥
	3.024	Switch0	192.168.3.5	ICMP	🟥
	3.025	192.168.3.5	Switch0	ICMP	🟥
👁	3.026	Switch0	192.168.3.3	ICMP	🟥

☑ Constant Delay

Captured to: 176.775 s

Visible Events: ARP, ICMP

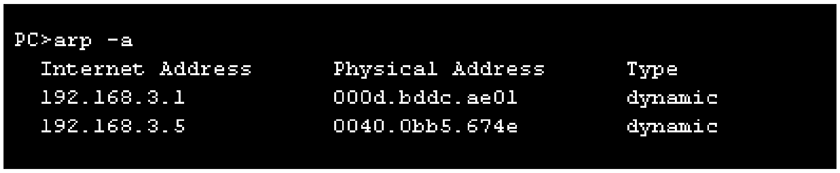
The event window of the simulation mode

You can delete the simulation script using the “Reset Simulation "button or use the "Delete" button in the User Created Packet Window.

Now the ARP tables of hosts 192.168.3.3 and 192.168.3.5 are not empty, they contain a single entry. To view the contents of the ARP table, run the command

“arp-a " on the command line.

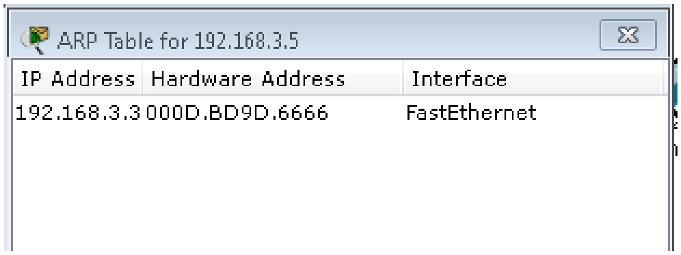
Contents of the ARP table of node 192.168.3.3:



```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.3.1           000d.bddc.ae01        dynamic
  192.168.3.5           0040.0bb5.674e        dynamic
```

ARP table of node 192.168.3.3 on the command promt

You can use another method: click on the "Inspect" button, click on the selected device, select "ARP table" and view the node's ARP table entries.



ARP Table for 192.168.3.5

IP Address	Hardware Address	Interface
192.168.3.3	000D.BD9D.6666	FastEthernet

ARP table of node 192.168.3.5, shown using the "Inspect" tool

If you set the ping request to host 192.168.3.5 again, only one ICMP message packet will be generated at once, because the corresponding local address is already stored in the source computer's ARP table.

Try sending the ping request again.

To delete all entries in the ARP table, use the “arp –d " command”.

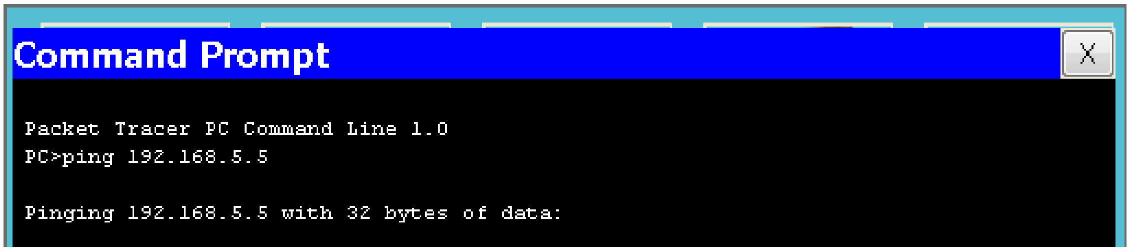
6. Sending a ping request to an external network

Send a test ping request from the destination node with the IP address 192.168.3.4 to the host with the IP address 192.168.5.5.

Important: one node tries to transmit a packet to another node that is on different networks with it.

In point 5 of the laboratory work, the case of sending an ARP request inside a local network was considered. In this case, the ARP Protocol directly determined the MAC address of the receiving node of the request. Now consider a situation where the source node and the destination node are located in different networks. The ARP Protocol operates within a network segment, so in this case it will be used to determine the MAC address of the router. This way, the packet will be passed to the router for further retransmission.

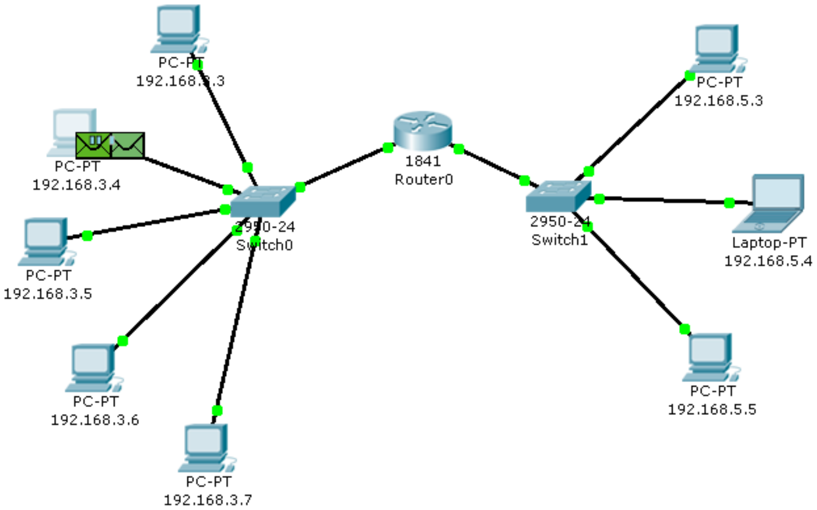
Open "Command Promt", which simulates the command line, on the computer 192.168.3.4 and send a ping request to the host 192.168.5.5.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:
```

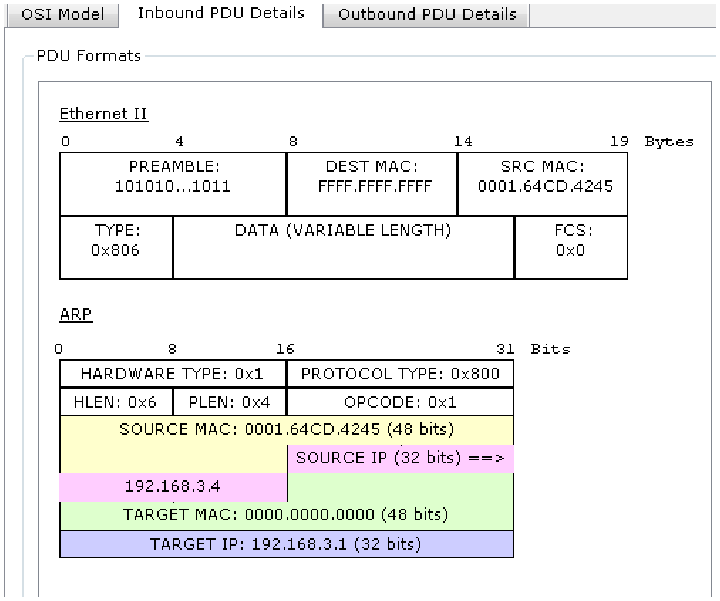
Host 192.168.3.4 commend promt

In this case, an ARP request is initiated to the router, which forwards packets to the destination network. Two ARP and ICMP Protocol packets are generated on the source node.



The workspace view

The format of the ARP request packet contains the same information as for resolving the local address of the device, and is broadcast to all nodes in the subnet.



OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 0001.64CD.4245

TYPE: 0x806	DATA (VARIABLE LENGTH)	FCS: 0x0

ARP

0 8 16 31 Bits

HARDWARE TYPE: 0x1 | PROTOCOL TYPE: 0x800

HLEN: 0x6 | PLEN: 0x4 | OPCODE: 0x1

SOURCE MAC: 0001.64CD.4245 (48 bits)

SOURCE IP (32 bits) ==>

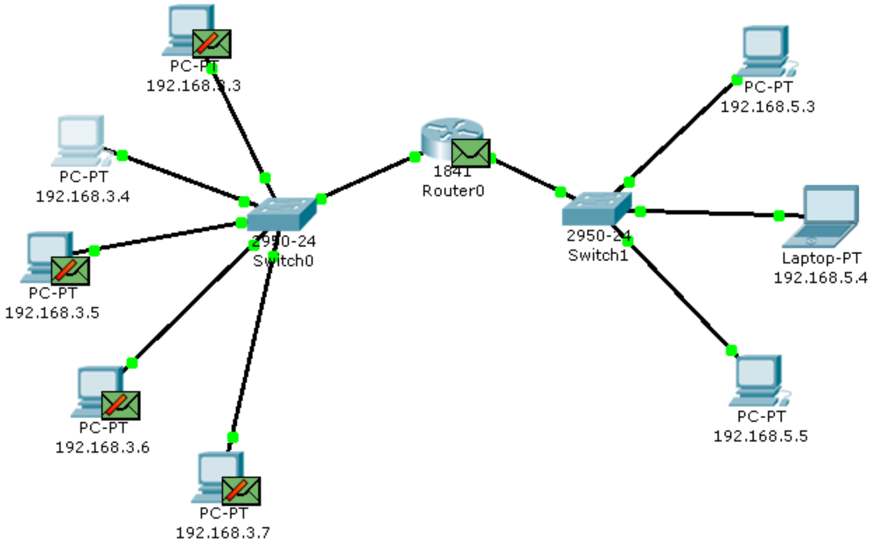
192.168.3.4

TARGET MAC: 0000.0000.0000 (48 bits)

TARGET IP: 192.168.3.1 (32 bits)

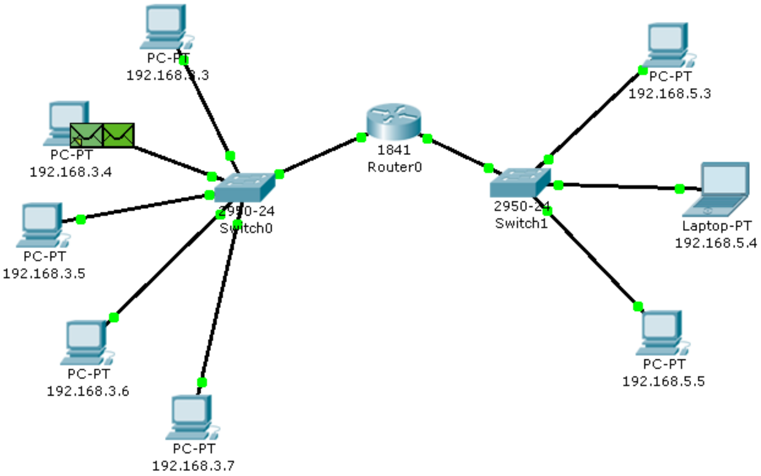
Format of the ARP request packet

All nodes ignore the packet, except the router that the packet was intended for.



The workspace view

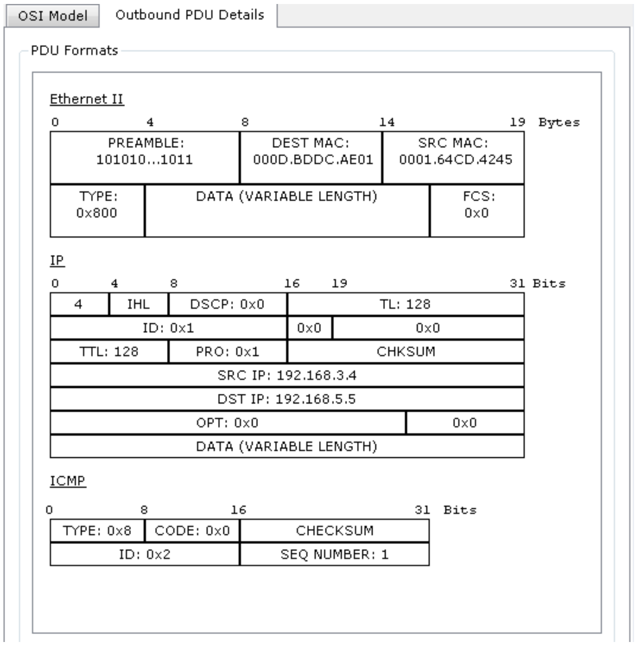
The router generates an ARP response specifying its physical address and sends it to node 192.168.3.4.



The workspace view

After receiving an ARP response, host 192.168.3.4 sends an ICMP ping request message through the router to the destination network.

View the contents of the package by clicking on the package (envelope).



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: 000D.BDDC.AE01	SRC MAC: 0001.64CD.4245
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 128	
ID: 0x1			0x0	0x0
TTL: 128		PRO: 0x1	CHKSUM	
SRC IP: 192.168.3.4				
DST IP: 192.168.5.5				
OPT: 0x0				0x0
DATA (VARIABLE LENGTH)				

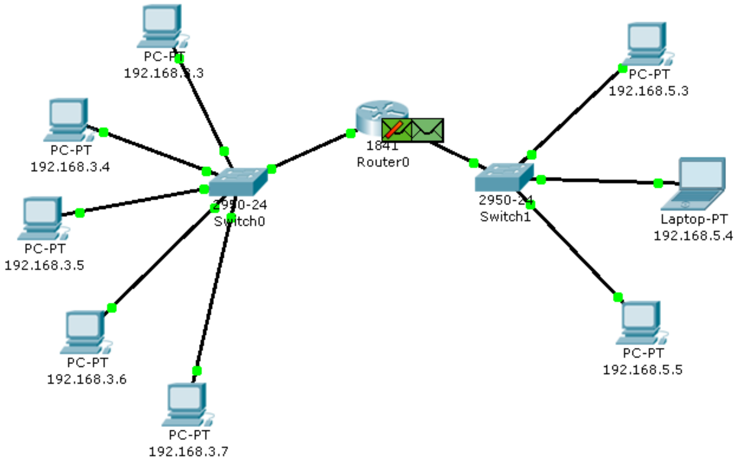
ICMP

0 8 16 31 Bits

TYPE: 0x8	CODE: 0x0	CHECKSUM
ID: 0x2		SEQ NUMBER: 1

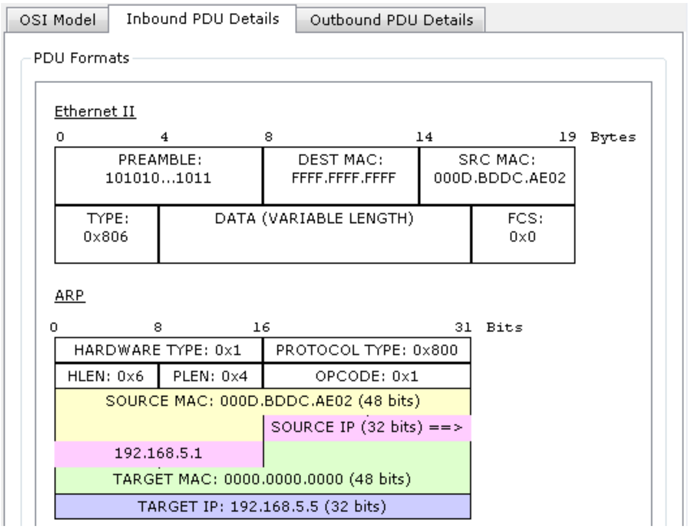
Format of the ICMP echo request packet

The source IP address is 192.168.3.4. the destination IP address is 192.168.5.5. the ICMP message Type is 8 (echo request). When a request arrives at the destination network, the router determines the Mac address of the recipient, if there is no Mac address in the router's ARP table. This again solves the problem of resolving the local address.



The workspace view

The router must first find out the physical address of the recipient before it can send a ping request to the destination, so the ping request packet that arrived at the router is rejected. A new ARP request is sent as a broadcast message from the router, containing its IP address and MAC address. The destination IP address is node 192.168.5.5.



PDU Formats

Ethernet II

0 4	8	14 19 Bytes
PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000D.BDDC.AE02

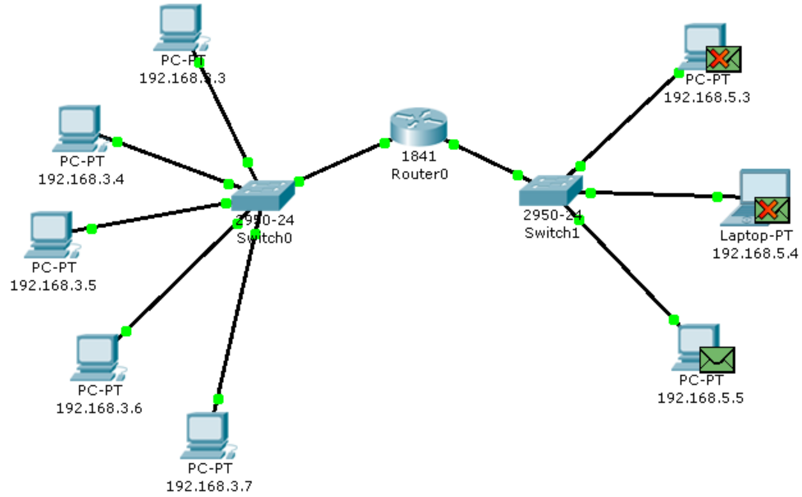
TYPE: 0x806	DATA (VARIABLE LENGTH)	FCS: 0x0

ARP

0 8		16 31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1
SOURCE MAC: 000D.BDDC.AE02 (48 bits)		
		SOURCE IP (32 bits) ==>
192.168.5.1		
TARGET MAC: 0000.0000.0000 (48 bits)		
TARGET IP: 192.168.5.5 (32 bits)		

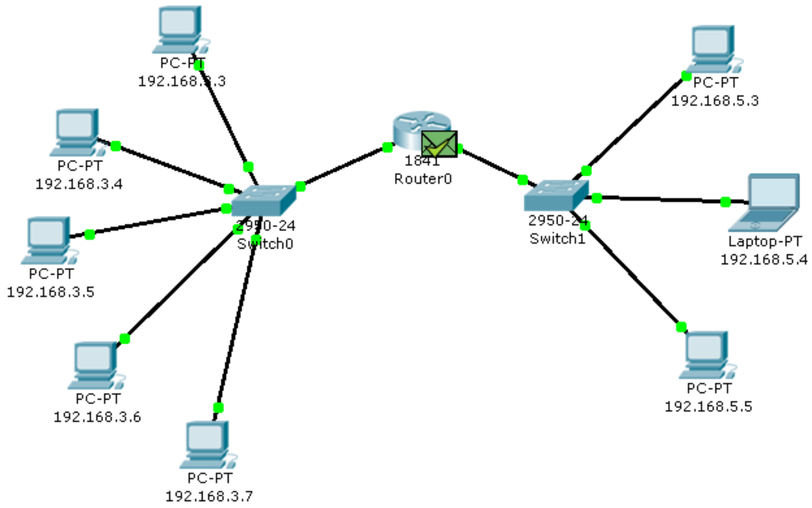
Format of the ARP request packet

Subnet nodes that do not receive the packet ignore it.



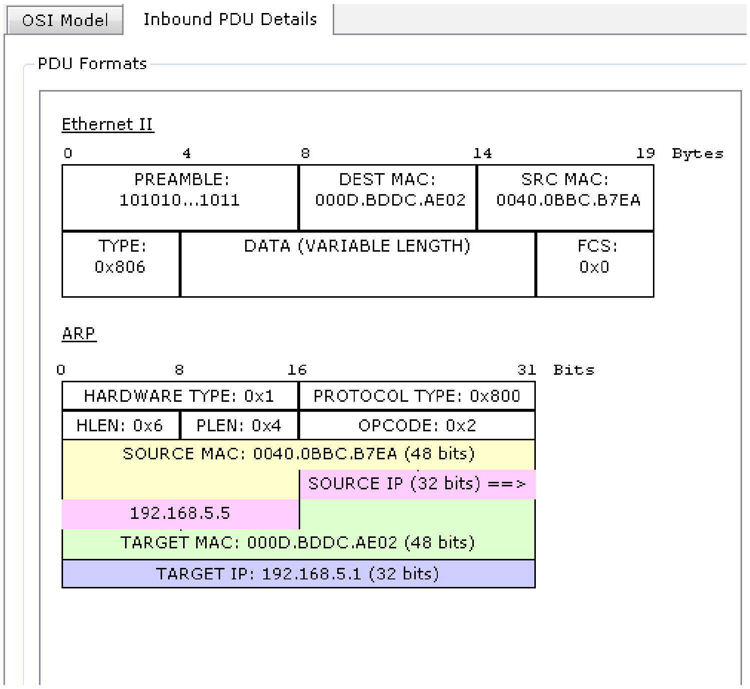
The workspace view

Node 192.168.5.5. generates an ARP response and sends it back to the router, specifying its MAC address, as evidenced by the contents of the packet.



The workspace view

After the router determines the Mac address of the recipient of an incoming ping request, it sends an ICMP response to the router of the sender's host. (In this case, it is the same router Router0).



Ethernet II

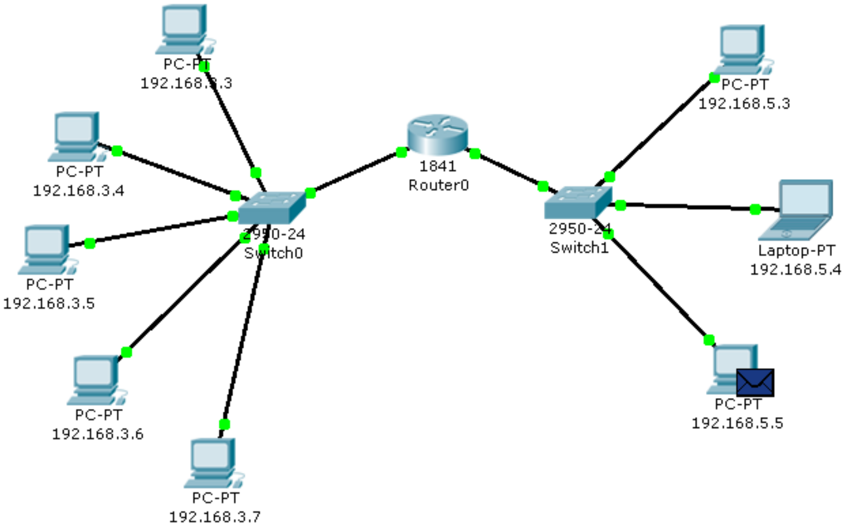
0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: 000D.BDDC.AE02	SRC MAC: 0040.0BBC.B7EA	
TYPE: 0x806	DATA (VARIABLE LENGTH)		FCS: 0x0	

ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2	
SOURCE MAC: 0040.0BBC.B7EA (48 bits)			
		SOURCE IP (32 bits) ==>	
192.168.5.5			
TARGET MAC: 000D.BDDC.AE02 (48 bits)			
TARGET IP: 192.168.5.1 (32 bits)			

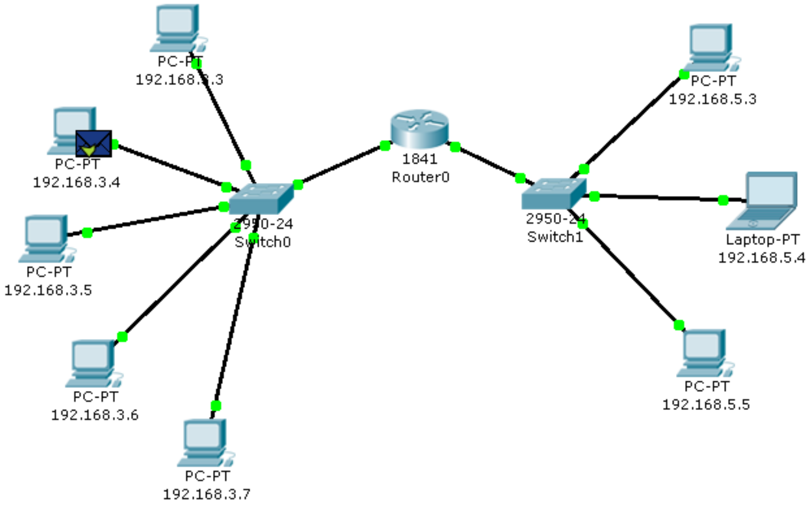
Format of the ARP response packet

Node 192.168.3.4. tries again to send a ping request to the external network to node 192.168.5.5. Its route must lie through Switch 0, router Router0, switch1 and reach the destination node. **FOLLOW THE ROUTE OF THE PACKAGE YOURSELF.**



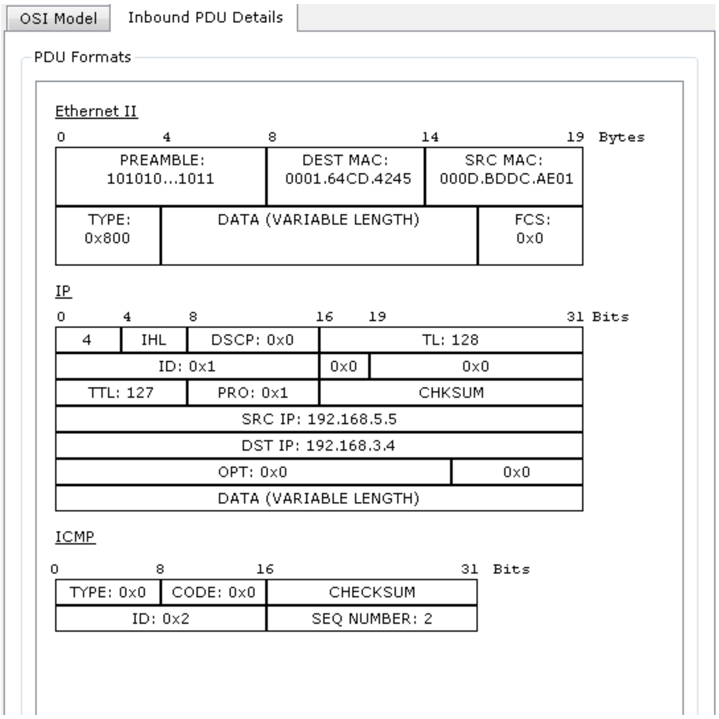
The workspace view

The node generates a ping response that is sent back to the node 192.168.3.4.



The workspace view

View the contents of the ping response packet sent to host 192.168.3.4.



PDU Formats

Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: 0001.64CD.4245	SRC MAC: 000D.BDDC.AE01
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 128
ID: 0x1		0x0	0x0
TTL: 127	PRO: 0x1	CHKSUM	
SRC IP: 192.168.5.5			
DST IP: 192.168.3.4			
OPT: 0x0			0x0
DATA (VARIABLE LENGTH)			

ICMP

0 8 16 31 Bits

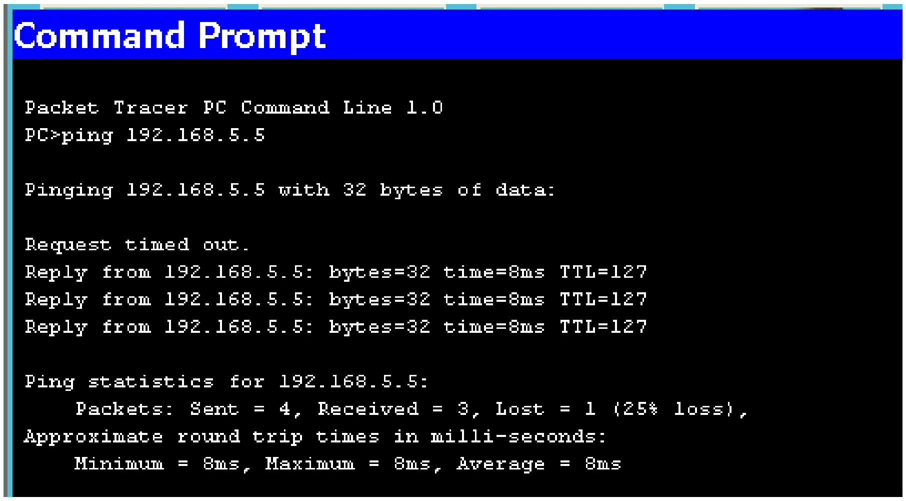
TYPE: 0x0	CODE: 0x0	CHECKSUM
ID: 0x2		SEQ NUMBER: 2

ICMP echo response packet format

IP source address 192.168.5.5. IP destination address – 192.168.3.4. The ICMP message type

0 (echo reply).

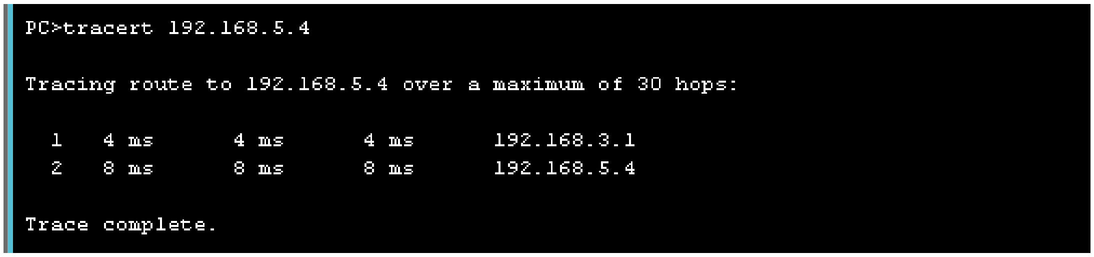
See the ping response in the command promt of the host 192.168.3.4.



```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Ping output

You can view the packet route using the tracert command. Run this command, for example, in the command line of the computer 192.168.3.5:



```
PC>tracert 192.168.5.4

Tracing route to 192.168.5.4 over a maximum of 30 hops:

  1   4 ms      4 ms      4 ms      192.168.3.1
  2   8 ms      8 ms      8 ms      192.168.5.4

Trace complete.
```

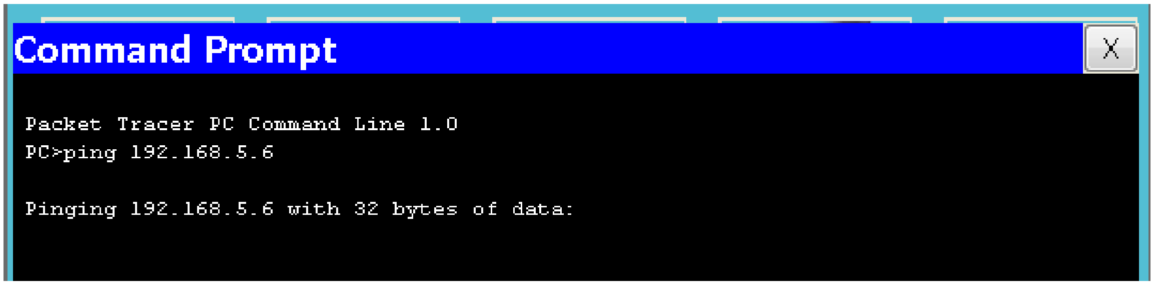
Tracert outline

There is one intermediate router on the packet path to host 192.168.5.4.

7. Sending a ping request to a non-existent host

Send a ping request to a non-existent address in the network 192.168.5.0/24.

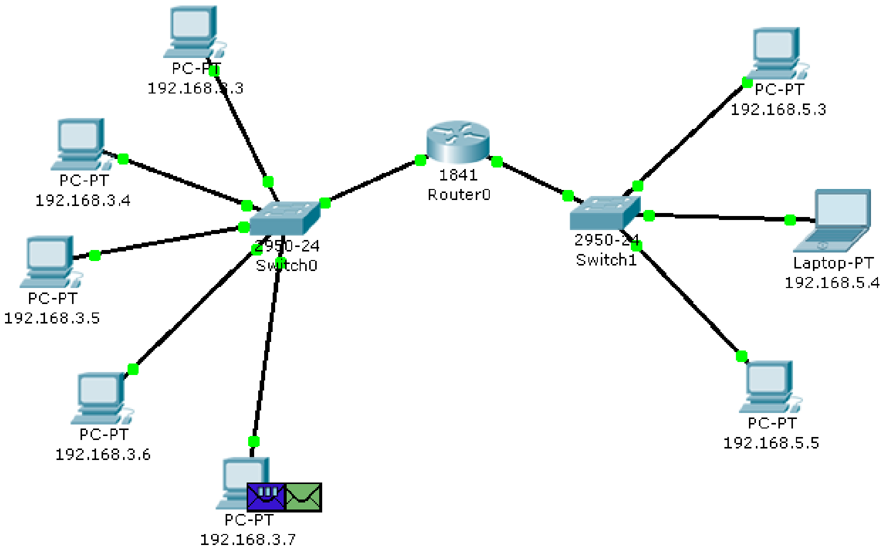
Open the "Command Promt" program on node 192.168.3.7 and try to send a ping request to a non-existent host with the IP address 192.168.5.6.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:
```

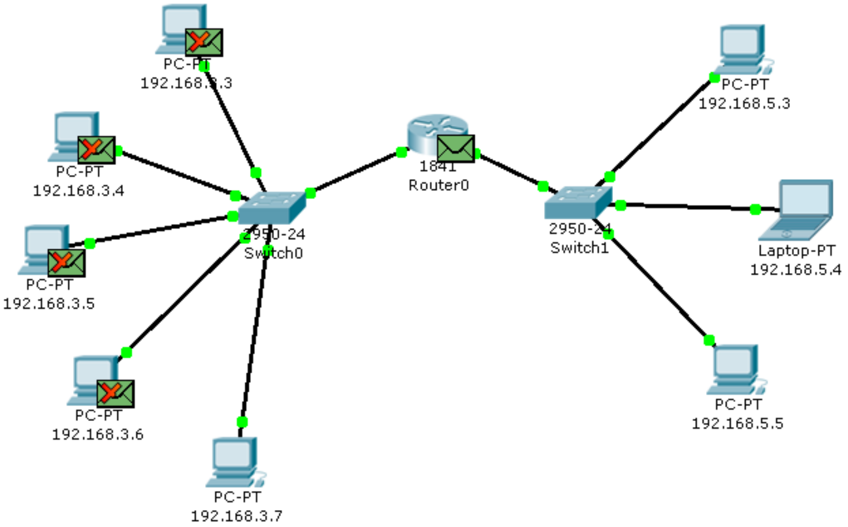
Host command line 192.168.3.7

The ARP table on the source node does not contain a corresponding entry about the MAC address of the node 192.168.5.6, so an ARP request is generated.



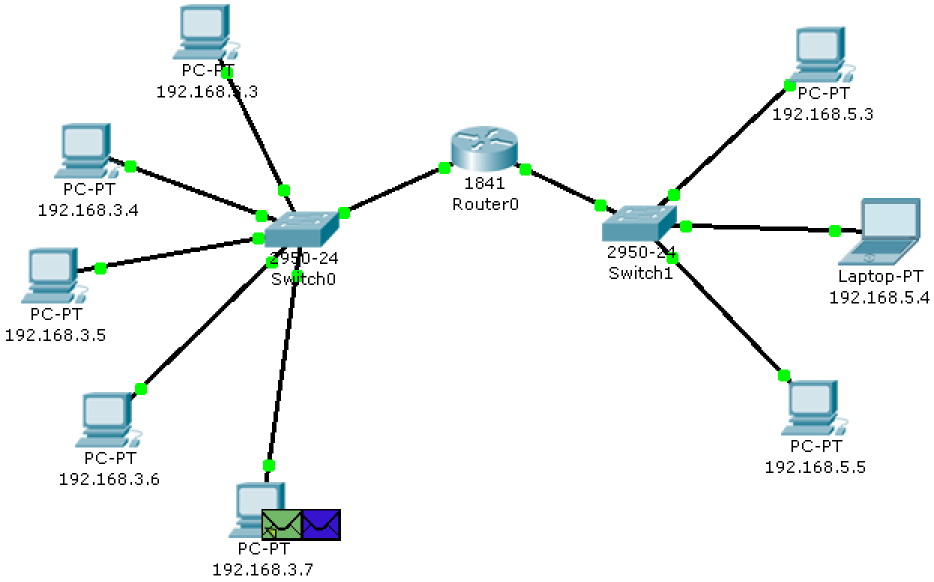
The workspace view

All nodes ignore the packet, except the router that the packet was intended for.



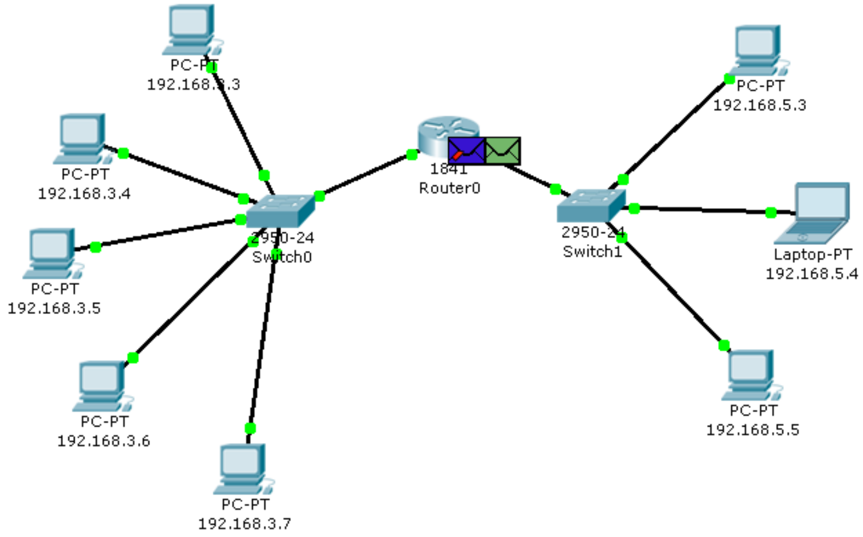
The workspace view

Node 192.168.3.7 receives an ARP response with the MAC address of the router. Now, knowing its hardware address, the host sends a ping request to node 192.168.5.6.



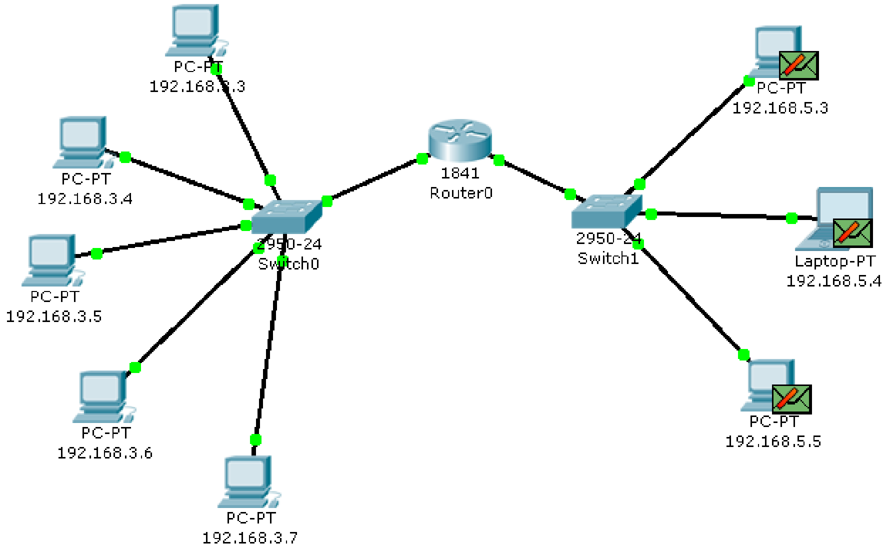
The workspace view

The router destroys the incoming packet, because it cannot redirect it to the specified address, because it "does not know" the corresponding MAC address. In this regard, the router generates an ARP request at the address 192.168.5.6.



The workspace view

All nodes in the subnet ignore the packet because the IP address in the request does not match their own. However, no response is received from anyone by router.

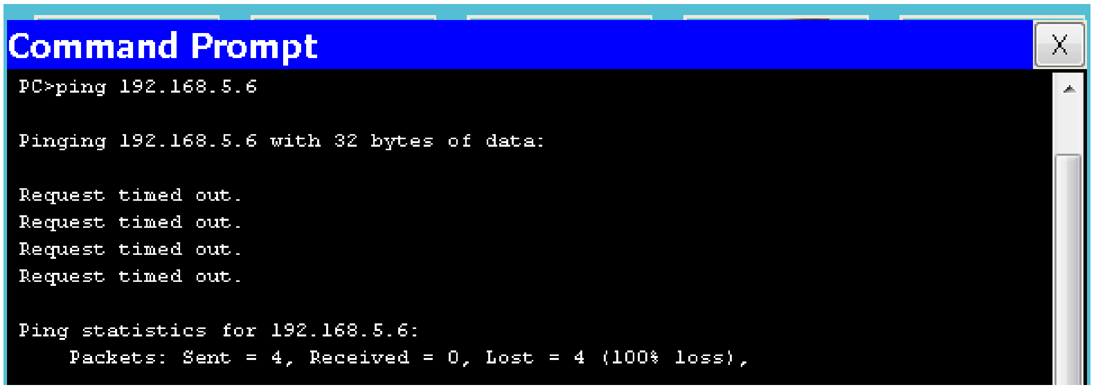


The workspace view

The procedure for passing packets is repeated throughout the simulation scenario: the router still "does not know" the MAC address of the IP address 192.168.5.6 specified in the ping request and continues to send ARP requests. None of the subnet nodes respond to these requests. Without receiving a response, the router itself is "silent", without notifying the host source of the ping request about the error.

Note: in fact, in this case, the router should send an ICMP message "host unreachable»: type 3 message with code 1. However the experiment carried out with the theory went.

Let's look at the response to the ping request in the command line of the source node 192.168.3.7: "timeout exceeded".

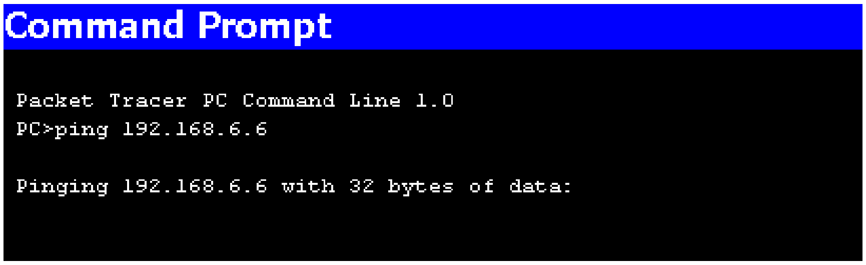


```
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping output

Let's try sending a ping request containing the host's IP address to a network that doesn't have a route.

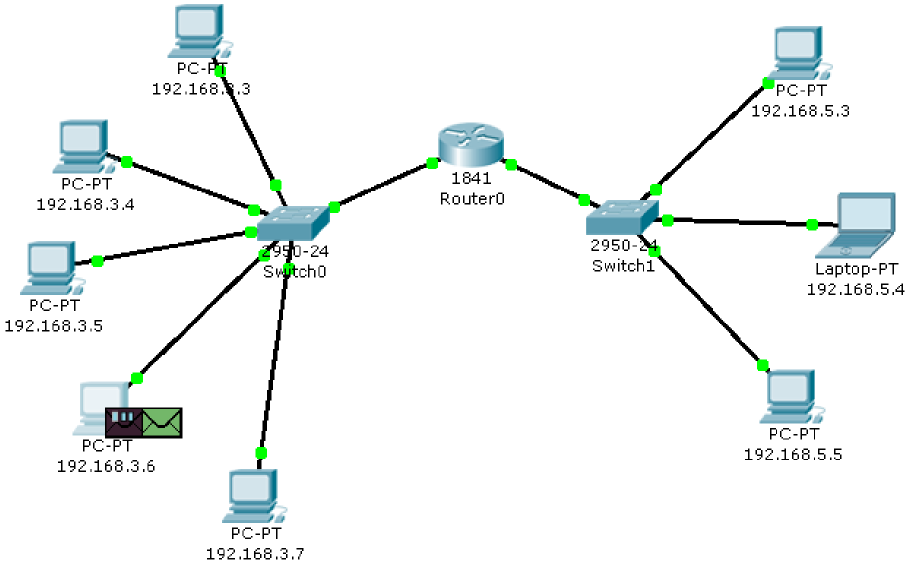
Open the "Command Promt" program on node 192.168.3.6 and try to send a ping request to a non-existent host with the IP address 192.168.6.6.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:
```

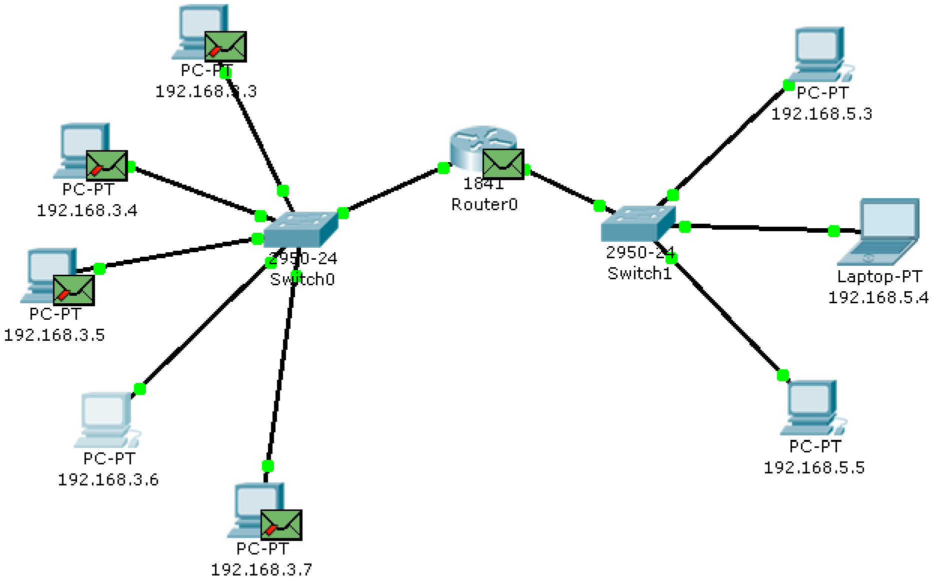
Commant prompt of the node 192.168.3.6

Since the source node's ARP table does not have a corresponding entry, an ARP request is generated for the specified node with the IP address 192.168.6.6.



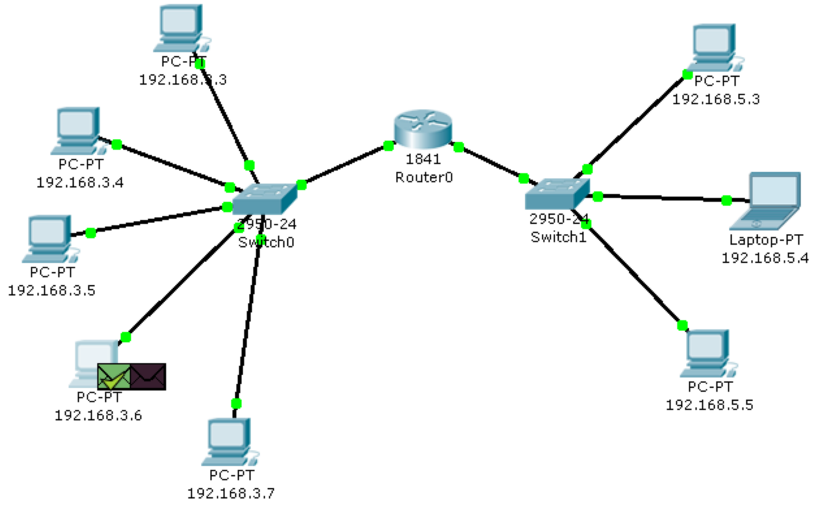
The workspace view

All nodes ignore the packet, except the router that the packet was intended for.



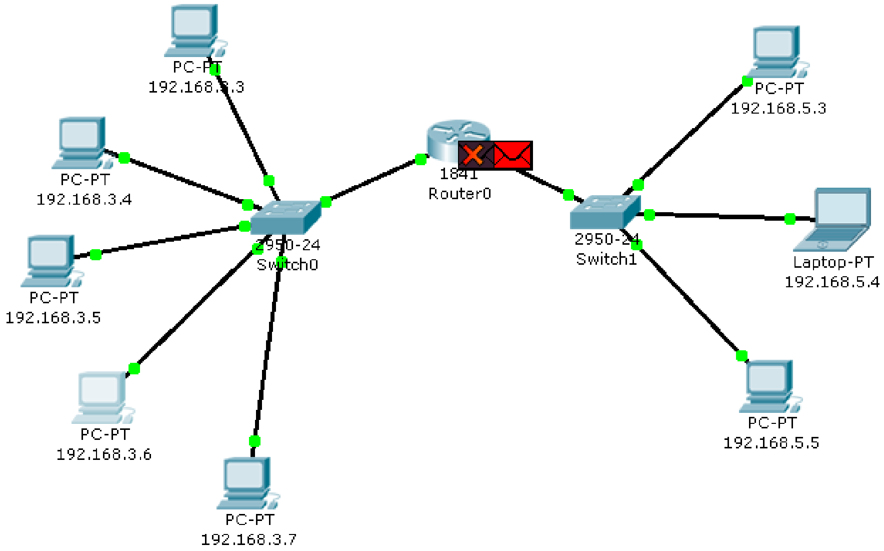
The workspace view

Node 192.168.3.6 receives an ARP response with the MAC address of the router. Now, knowing its hardware address, the host sends a ping request.



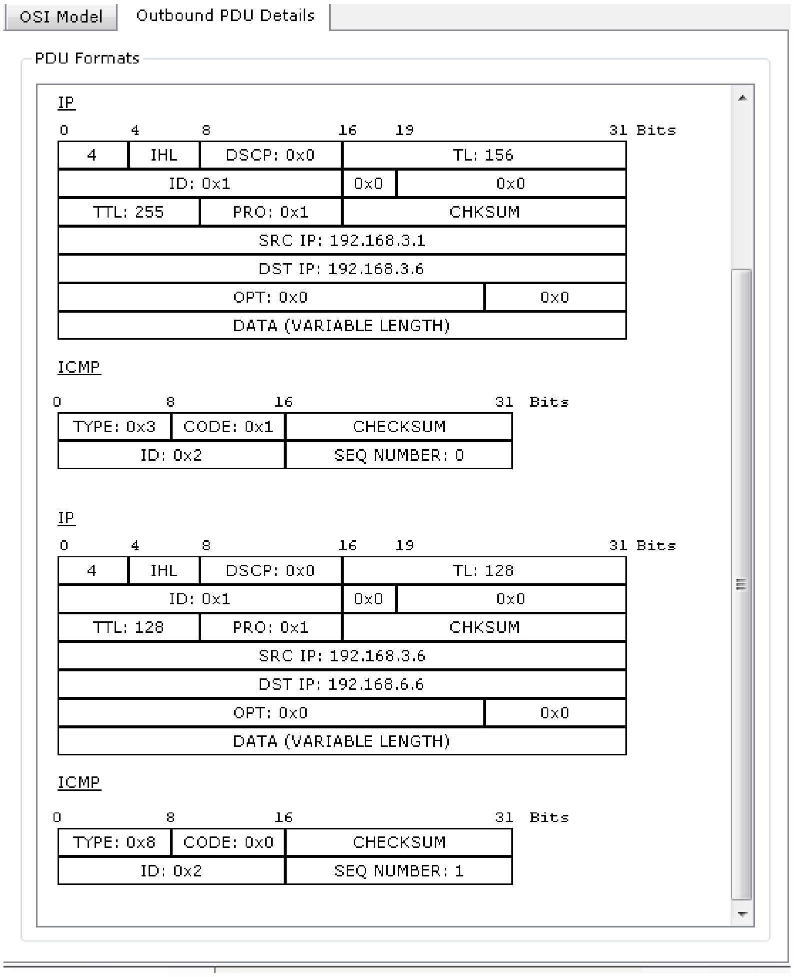
The workspace view

When a ping request reaches the router, it cannot redirect it to any of its interfaces, because the IP addresses of its interfaces do not match the address specified in the ping request. Accordingly, this packet is destroyed and a new ICMP message is generated.



The workspace view

Let's look at the contents of the packet generated by the router.



IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 156	
ID: 0x1			0x0	0x0
TTL: 255		PRO: 0x1	CHKSUM	
SRC IP: 192.168.3.1				
DST IP: 192.168.3.6				
OPT: 0x0				0x0
DATA (VARIABLE LENGTH)				

ICMP

0 8 16 31 Bits

TYPE: 0x3	CODE: 0x1	CHECKSUM
ID: 0x2		SEQ NUMBER: 0

IP

0 4 8 16 19 31 Bits

4	IHL	DSCP: 0x0	TL: 128	
ID: 0x1			0x0	0x0
TTL: 128		PRO: 0x1	CHKSUM	
SRC IP: 192.168.3.6				
DST IP: 192.168.6.6				
OPT: 0x0				0x0
DATA (VARIABLE LENGTH)				

ICMP

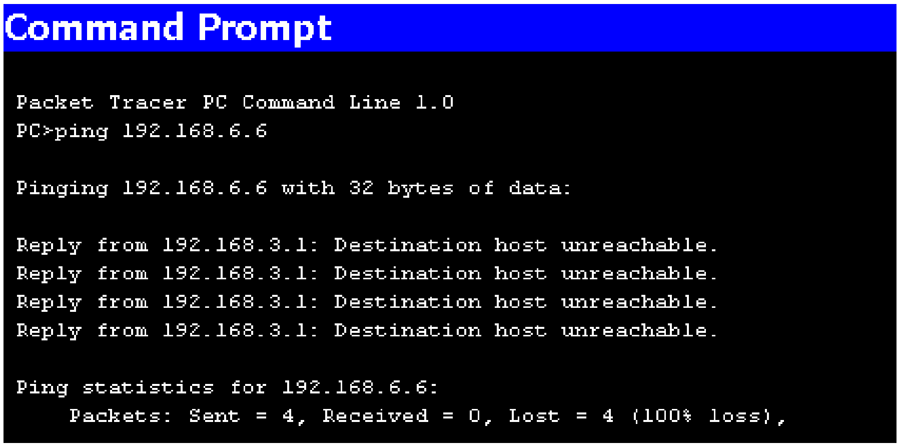
0 8 16 31 Bits

TYPE: 0x8	CODE: 0x0	CHECKSUM
ID: 0x2		SEQ NUMBER: 1

The packet format of an ICMP “host unreachable”

IP source address – 192.168.3.1. IP destination address – 192.168.3.6. The ICMP message type 3 code 1 means "host unreachable". This packet arrives at node 192.168.3.6.

Result of a ping request in the command line of node 192.168.3.6: "destination host unreachable".



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping output

Thus, the router "responded" to a ping request for which it did not have a corresponding route with a new ICMP message "host unreachable".

Note: did the router respond correctly in this situation by sending an ICMP "host unreachable" message to the source host? To answer this question, refer to the ICMP Protocol specification RFC 792 and learn about other types of ICMP messages. [Electronic source]. URL: http://tools.ietf.org/html/rfc792.

8. Individual task

According to the option, filter ARP and ICMP messages for the specified source-receiver pairs. Each option provides 2 ping request options: inside the network and to the external network. Use the tracert command to view the route of a packet addressed to the external network.

In the report for each test, specify the packet routes, their contents, and explain the results.

REPORT

After completion the task the students need to submit:

- **The format of the report file is *pdf*.**
- Upload reports for the GitLab repository (to your personal project)
- Do not forget to write your name and ID inside the report

Options for individual tasks (table 3).

Table 3

#	Sender	Receiver
1	192.168.3.3 192.168.3.4	192.168.3.4 192.168.3.6
2	192.168.3.4 192.168.3.5	192.168.3.7 192.168.5.3
3	192.168.3.5 192.168.3.6	192.168.3.6 192.168.3.7
4	192.168.3.6 192.168.3.7	192.168.5.4 192.168.3.4
5	192.168.3.3 192.168.3.7	192.168.3.7 192.168.5.5
6	192.168.5.3 192.168.3.6	192.168.5.4 192.168.3.4
7	192.168.3.3 192.168.3.5	192.168.5.3 192.168.3.7
8	192.168.3.3 192.168.3.4	192.168.5.4 192.168.3.5
9	192.168.3.4 192.168.3.5	192.168.5.3 192.168.3.4
10	192.168.5.4 192.168.3.6	192.168.5.5 192.168.3.3
11	192.168.3.4 192.168.3.7	192.168.5.3 192.168.5.4

12	192.168.3.5 192.168.3.6	192.168.5.5 192.168.3.7
13	192.168.3.5 192.168.3.7	192.168.5.4 192.168.3.3
14	192.168.3.6 192.168.3.7	192.168.5.3 192.168.5.5