

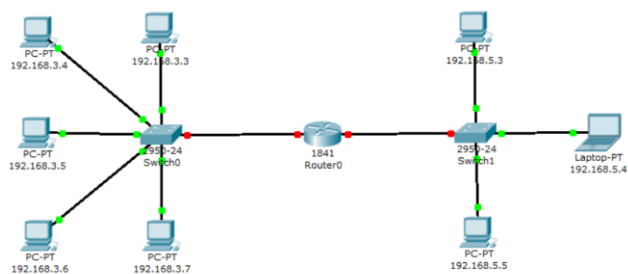
Computer Networks Lab 2

Name: CAO Xinyang
HDU ID: 20321308
Variant: 14

Sender	Receiver
192.168.3.6	192.168.5.3
192.168.3.7	192.168.5.5

1. Creating a network topology

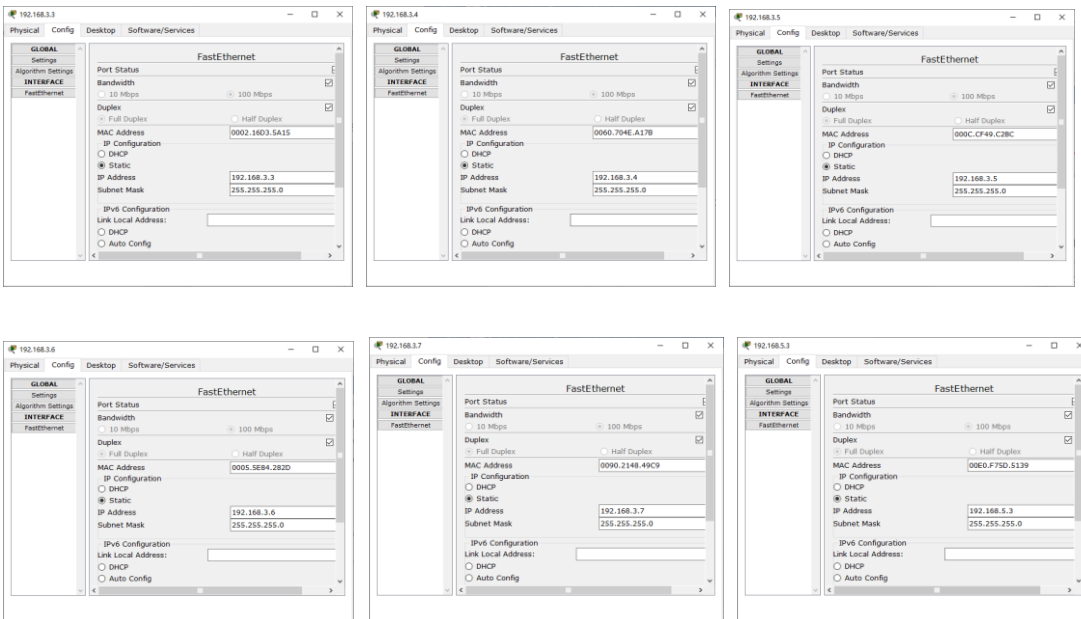
At the end of the first part, we created the following network topology, consisting of end nodes (PCs), switches, and a router:

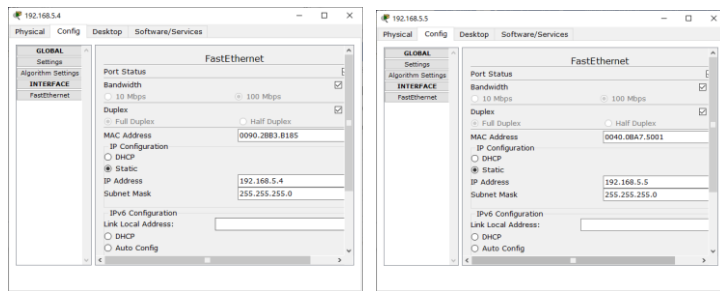


2. Configuring the end nodes

On PC0-PC4 devices, set the specified IP addresses and subnet mask. The gateway IP address for all nodes is 192.168.3.1.

On PC 5, Laptop 0, and PC6 devices, set the specified IP addresses and subnet mask. the gateway IP address for all nodes is 192.168.5.1.





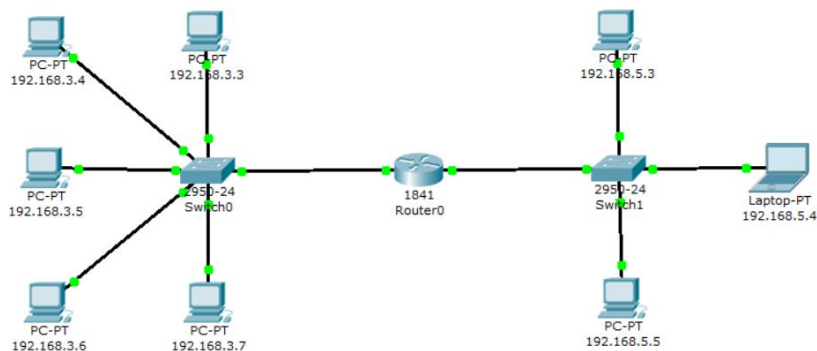
3. Configuring the router

During the configuration process of end nodes, it was previously stated that the router in this network topology possesses two interfaces. To configure the fastethernet0/0 interface, follow these steps:

1. Click once on the router device.
2. Choose the "Config" tab.
3. Locate the fastethernet0/0 interface and assign the desired IP address and subnet mask.

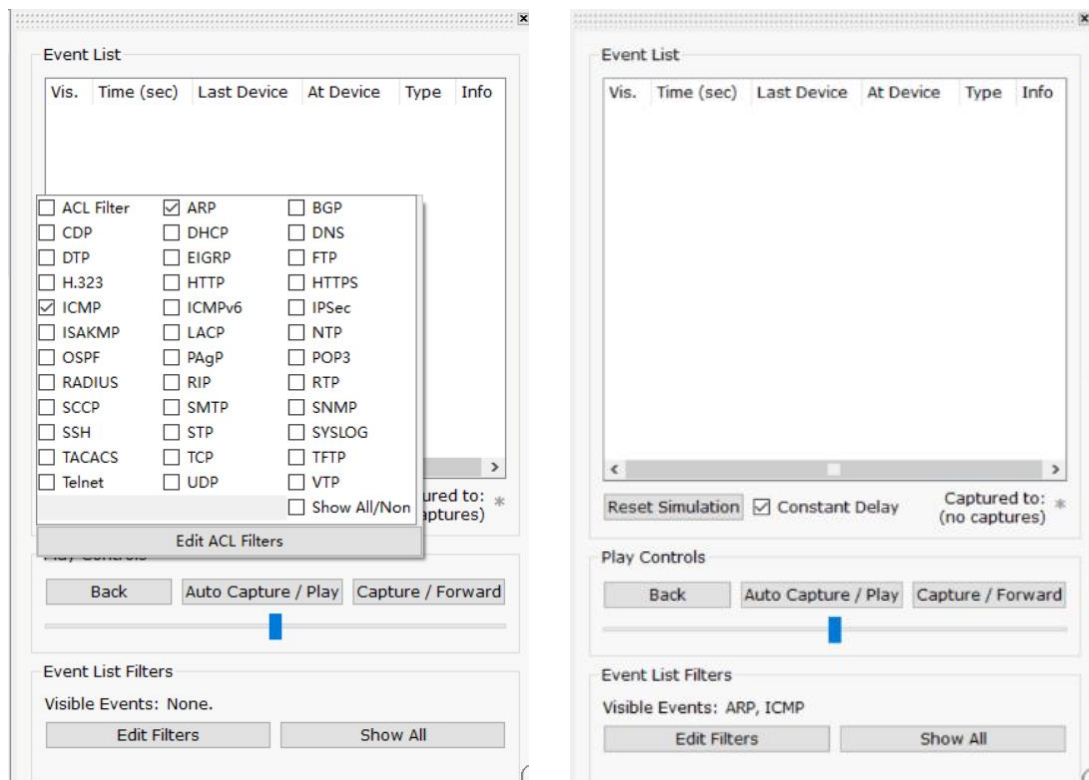
FastEthernet0/0		FastEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On	Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto	Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps	<input checked="" type="radio"/> 100 Mbps	<input type="radio"/> 10 Mbps	<input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto	Duplex	<input checked="" type="checkbox"/> Auto
<input checked="" type="radio"/> Full Duplex	<input type="radio"/> Half Duplex	<input checked="" type="radio"/> Full Duplex	<input type="radio"/> Half Duplex
MAC Address	0090.2BD7.5701	MAC Address	0090.2BD7.5702
IP Address	192.168.3.1	IP Address	192.168.5.1
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Tx Ring Limit	10	Tx Ring Limit	10

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.



4. Simulation mode Cisco Packet Tracer

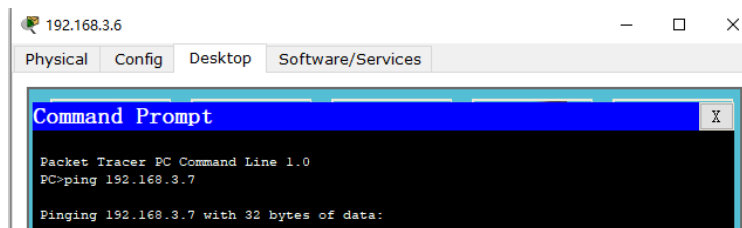
1. Open simulation mode
2. Click the "Edit Filters" button.
3. Remove the checkmark from "Show All/None" label.
4. Choose ARP and ICMP from the available options.
5. Ensure that the designated filtering protocols (ARP and ICMP) are properly assigned.



5. Verification of network operation in the simulation mode

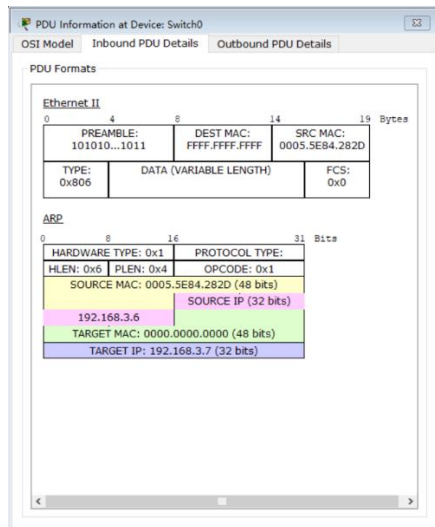
Send a test ping request from the destination node with the IP address 192.168.3.6 to the host with the IP address 192.168.3.7.

- 1) Single-click on the chosen device.
- 2) Navigate to the Desktop tab, which comprises simulators of various programs accessible on your computer.
- 3) Choose "Command Prompt," a program that emulates the computer's command line interface.
- 4) Utilize the ping utility to dispatch a ping request.



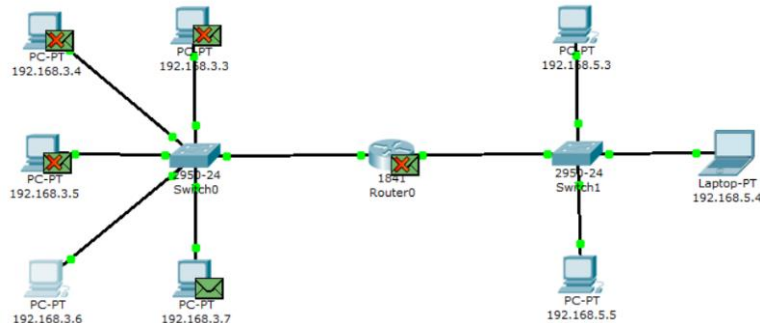
Two packets, one for the ARP protocol and another for the ICMP protocol, are generated on the source device. It is important to note that an ARP request is always generated when a host attempts to communicate with another host.

To control packet movement between devices, choose either the "Auto Capture/play" button or the "Capture/Forward" button. The latter option allows you to manually manage packet flow. Initially, an ARP Protocol packet is sent when the host with the IP address 192.168.3.3 has an empty ARP table and doesn't know where to send the ping request. Click on the package (envelope) to see the involved OSI model layers. Access the "Inbound PDU Details" tab to view the packet's structure.

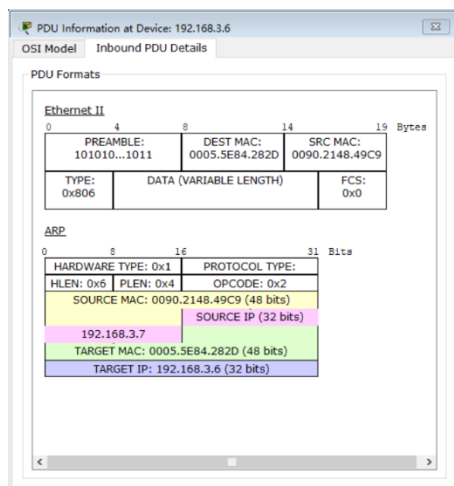


Node 192.168.3.6 has generated a request and broadcasted it as a message to all hosts within the subnet. The request includes not only the destination IP address but also the sender's IP address and MAC address, enabling the recipient to respond accordingly.

When examining the packet flow, ensure that only host 192.168.3.7 replies to the ARP request. Each host within the subnet receives the request and verifies its own IP address for a match. If the IP address does not align with the specified address in the request, the request is disregarded.



View the contents of the ARP response packet sent to host 192.168.3.6.



An ARP response was sent by Node 192.168.3.7, directly addressing the sender and utilizing its MAC address. The response specifies the MAC address of Node 192.168.3.7 in the "Target MAC" field.

Following that, an ICMP ping request message is transmitted. To examine the contents of the package, kindly click on the package (envelope) to access its details.

PDU Information at Device: 192.168.3.6

OSI Model Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Byte
PREAMBLE: 101010...1011		DEST MAC: 0090.2148.49C9		SRC MAC: 0005.5E84.282D	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

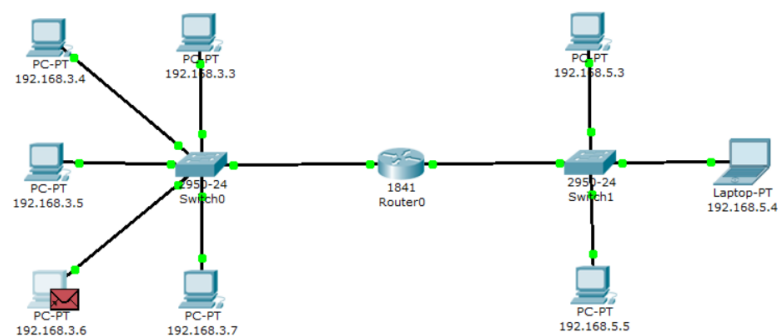
0	4	8	16	19	31	Bits
IHL: 0x5		DSCP: 0x0		TL: 128		
ID: 0x1		0x0		0x0		
TTL: 128		PRO: 0x1		CHKSUM		
SRC IP: 192.168.3.6				DST IP: 192.168.3.7		
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHKSUM
ID: 0x2		SEQ NUMBER: 1		

The source IP address is 192.168.3.6. The destination IP address is 192.168.3.7. the ICMP message Type is 8 (echo request).

The request is directed to the host 192.168.3.7 through the switch.



View the contents of the ping response packet sent to host 192.168.3.6.

PDU Information at Device: 192.168.3.6

OSI Model Inbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Byte
PREAMBLE: 101010...1011		DEST MAC: 0005.5E84.282D		SRC MAC: 0090.2148.49C9	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
IHL: 0x5		DSCP: 0x0		TL: 128		
ID: 0x1		0x0		0x0		
TTL: 128		PRO: 0x1		CHKSUM		
SRC IP: 192.168.3.7				DST IP: 192.168.3.6		
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x0		CODE: 0x0		CHKSUM
ID: 0x2		SEQ NUMBER: 1		

IP source address 192.168.3.7. IP destination address – 192.168.3.6. The ICMP message type 0 (echo reply). See the ping response in the command line of the host 192.168.3.6.

```

PC>ping 192.168.3.7

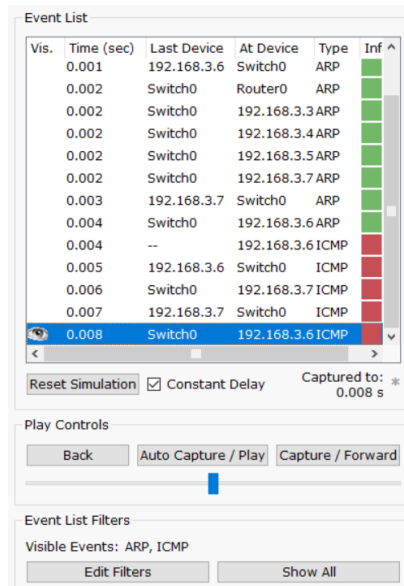
Pinging 192.168.3.7 with 32 bytes of data:

Reply from 192.168.3.7: bytes=32 time=8ms TTL=128
Reply from 192.168.3.7: bytes=32 time=4ms TTL=128
Reply from 192.168.3.7: bytes=32 time=4ms TTL=128
Reply from 192.168.3.7: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

```

The event window displays the routes taken by the ARP and ICMP requests, indicating the devices through which the packets were transmitted.



To remove the simulation script, you can utilize the "Reset Simulation" button or the "Delete" button in the User Created Packet Window.

At present, the ARP tables of hosts 192.168.3.6 and 192.168.3.7 are no longer empty and each contains a single entry. To view the contents of the ARP table, execute the command "arp -a" on the command line.

Here are the contents of the ARP table for node 192.168.3.6:

```

PC>arp -a
Internet Address      Physical Address      Type
192.168.3.7          0050.2148.49c9       dynamic

```

When sending a ping request to host 192.168.3.7 once again, only a single ICMP message packet will be generated at a time. This is because the corresponding local address is already stored in the source computer's ARP table, eliminating the need for ARP resolution.

Try sending the ping request again:

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	192.168.3.6	ICMP	
	0.001	192.168.3.6	Switch0	ICMP	
	0.002	Switch0	192.168.3.7	ICMP	
	0.003	192.168.3.7	Switch0	ICMP	
	0.004	Switch0	192.168.3.6	ICMP	
	1.005	--	192.168.3.6	ICMP	
	1.006	192.168.3.6	Switch0	ICMP	
	1.007	Switch0	192.168.3.7	ICMP	
	1.008	192.168.3.7	Switch0	ICMP	
	1.009	Switch0	192.168.3.6	ICMP	

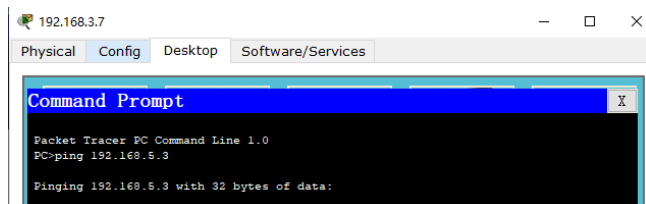
Reset Simulation ☒ Constant Delay Captured to: 1.009 s

6. Sending a ping request to an external network

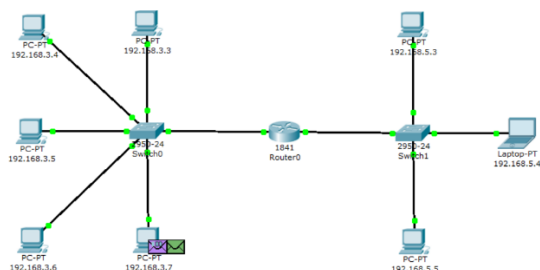
Send a test ping request from the destination node with the IP address **192.168.3.7** to the host with the IP address **192.168.5.3**.

In a scenario where the source node and destination node are situated in different networks, the ARP Protocol operates within the network segment to determine the MAC address of the router. This allows the packet to be forwarded to the router for further transmission. The router plays a crucial role in facilitating communication between different networks by routing the packets appropriately.

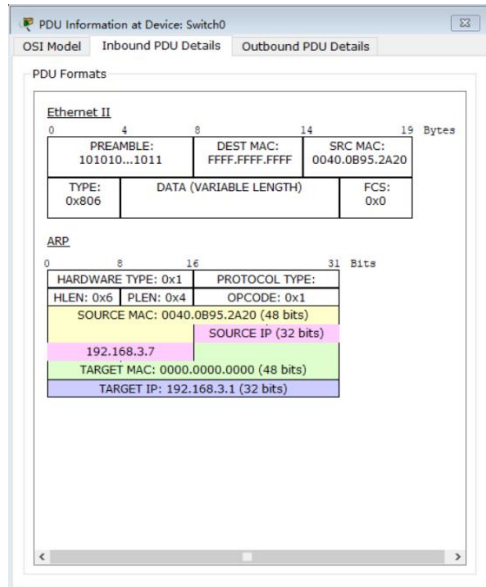
Open "Command Promt", which simulates the command line, on the computer 192.168.3.7 and send a ping request to the host 192.168.5.3.



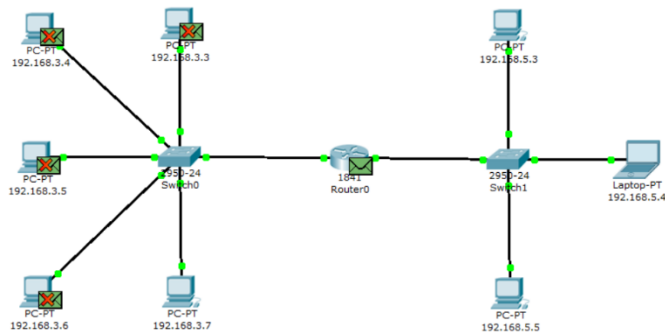
An ARP request is initiated by the source node to the router. This ARP request is essential to determine the MAC address of the router. Once the router obtains the packet, it forwards it to the destination network. As a result, two Protocol packets, namely ARP and ICMP, are generated on the source node to facilitate the communication process.



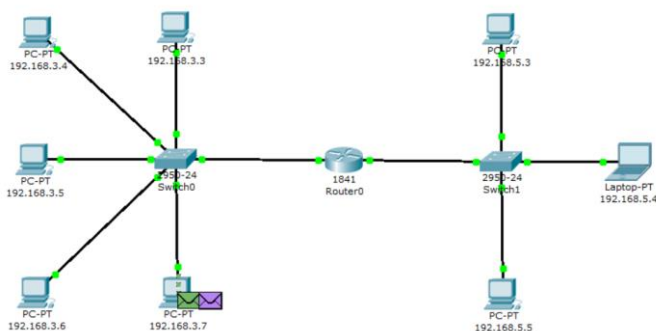
The format of the ARP request packet contains the same information as when resolving the local address of a device. It is broadcasted to all nodes within the subnet.



With the exception of the intended router, all other nodes within the subnet ignore the ARP request packet.

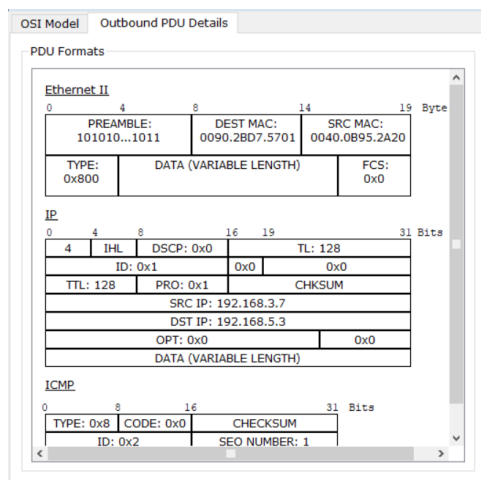


The router generates an ARP response, indicating its physical address, and sends it to node 192.168.3.7.

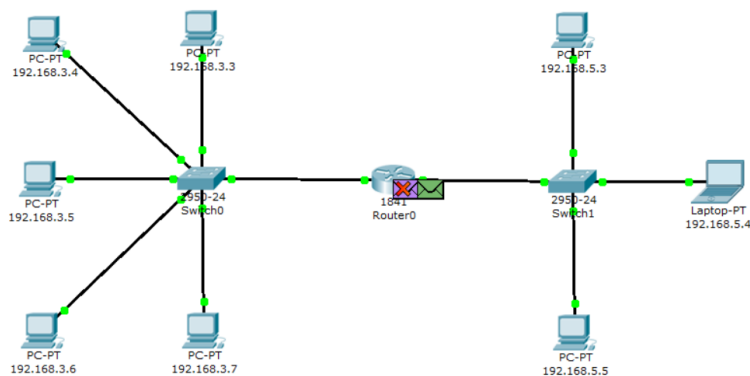


Upon receiving the ARP response, host 192.168.3.7 proceeds to send an ICMP ping request message through the router, directed towards the destination network.

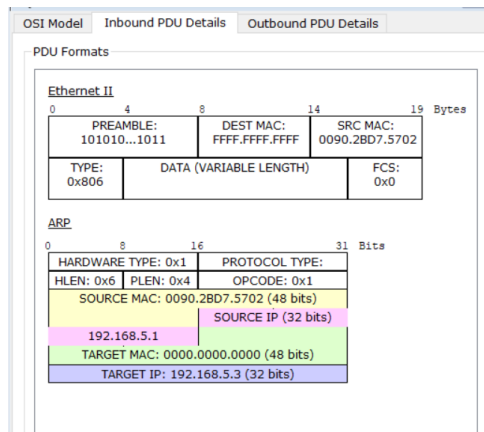
View the contents of the package by clicking on the package (envelope).



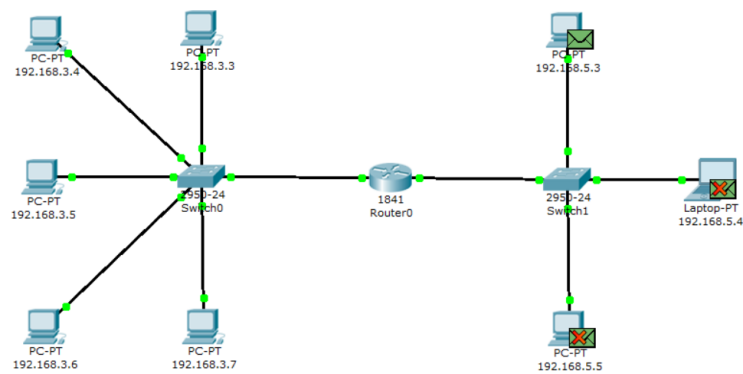
The ICMP ping request message has a source IP address of 192.168.3.7 and a destination IP address of 192.168.5.3. The message Type is 8, which corresponds to an echo request. When the request reaches the destination network, the router determines the MAC address of the recipient, especially if the MAC address is not present in the router's ARP table. This process resolves the issue of identifying the local address.



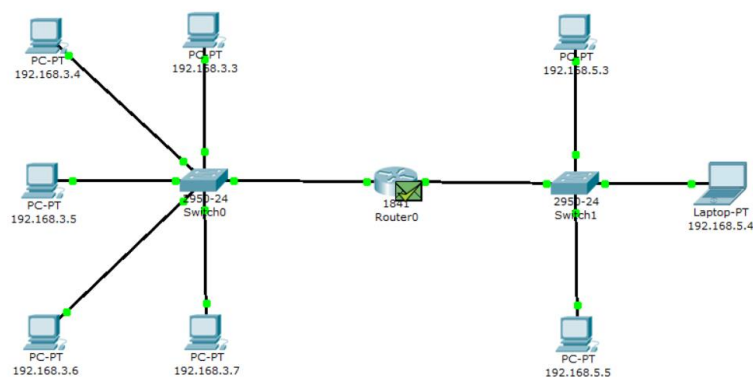
Before the router can send a ping request to the destination, it needs to determine the physical address (MAC address) of the recipient. As a result, when the ping request packet arrives at the router, it is rejected. In order to resolve this, the router sends a new ARP request as a broadcast message, containing its own IP address and MAC address. The destination IP address in this case is node 192.168.5.3.



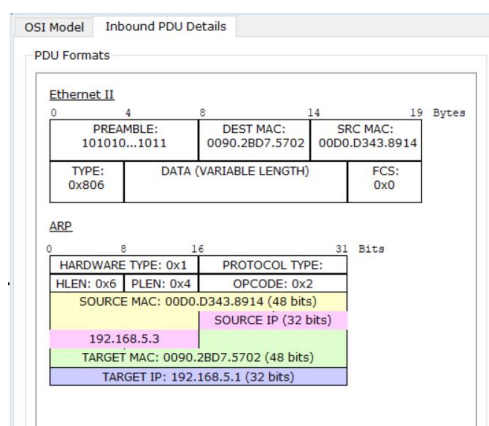
Indeed, within the subnet, any nodes that do not receive the packet will simply ignore it.



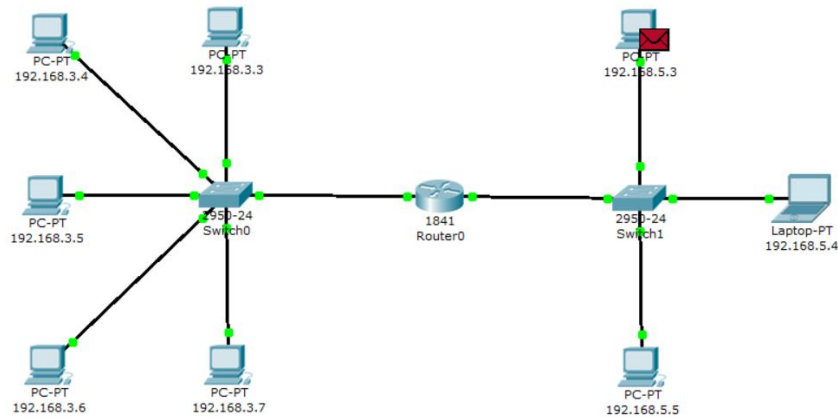
Node 192.168.5.3. generates an ARP response and sends it back to the router, specifying its MAC address, as evidenced by the contents of the packet.



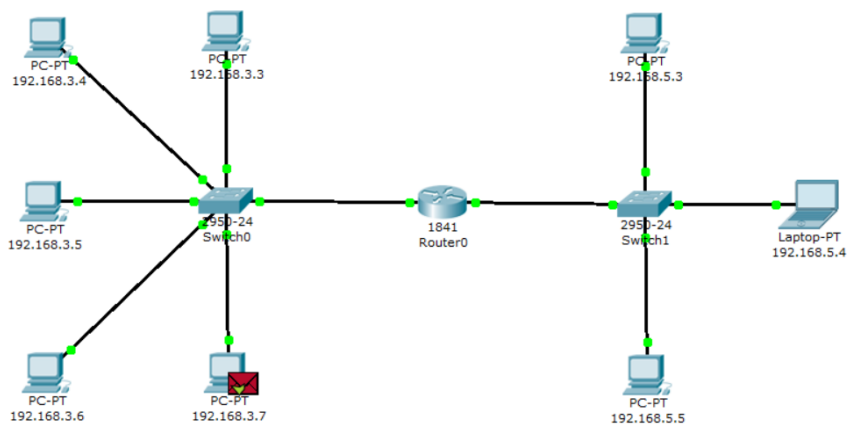
After the router determines the Mac address of the recipient of an incoming ping request, it sends an ICMP response to the router of the sender's host. (In this case, it is the same router Router0).



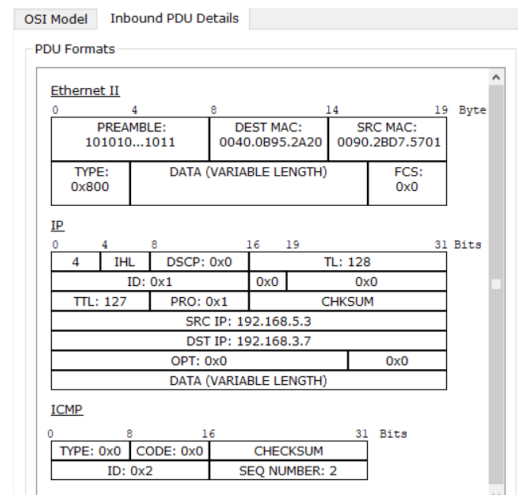
Node 192.168.3.7. tries again to send a ping request to the external network to node 192.168.5.3. Its route must lie through Switch 0, router Router0, switch1 and reach the destination node.



The node generates a ping response that is sent back to the node 192.168.3.7.



View the contents of the ping response packet sent to host 192.168.3.7.



IP source address 192.168.5.3. IP destination address – 192.168.3.7. The ICMP message type 0 (echo reply).

See the ping response in the command prompt of the host 192.168.3.7.

```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>arp -d
PC>ping 192.168.5.3

Pinging 192.168.5.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

You can view the packet route using the `tracert` command. Run this command, for example, in the command line of the computer 192.168.3.7:

```
PC>tracert 192.168.5.3

Tracing route to 192.168.5.3 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.3.7
  1  4 ms    4 ms    4 ms    192.168.3.1
  2  8 ms    8 ms    8 ms    192.168.5.3

Trace complete.
```

There is one intermediate router on the packet path to host 192.168.5.3.

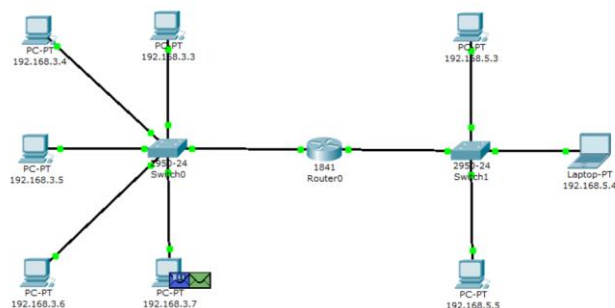
7. Sending a ping request to a non-existent host

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.

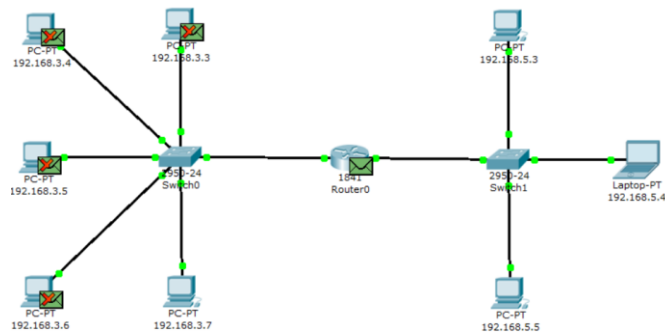
```
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:
```

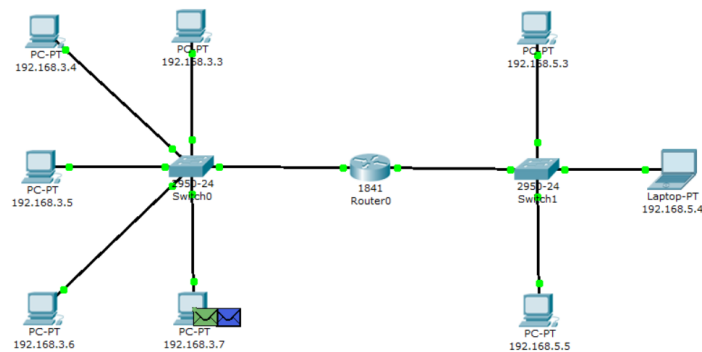
The ARP table on the source node does not contain a corresponding entry about the MAC address of the node 192.168.5.6, so an ARP request is generated.



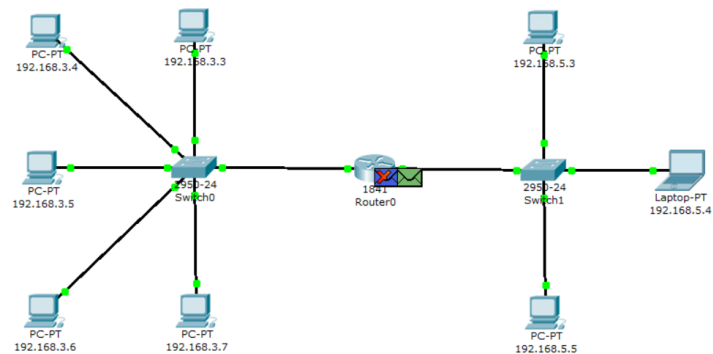
All nodes ignore the packet, except the router that the packet was intended for.



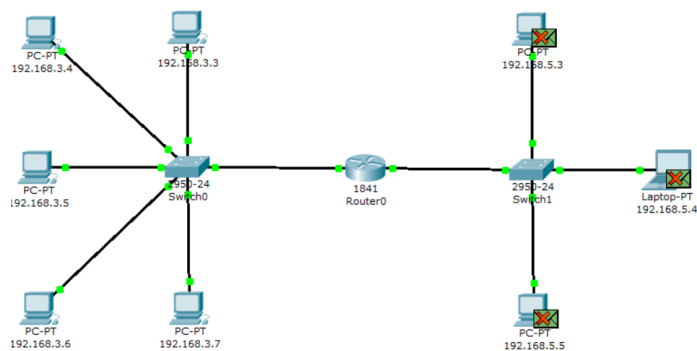
Node 192.168.3.7 receives an ARP response with the MAC address of the router. Now, knowing its hardware address, the host sends a ping request to node 192.168.5.6.



The 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.



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 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.

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.

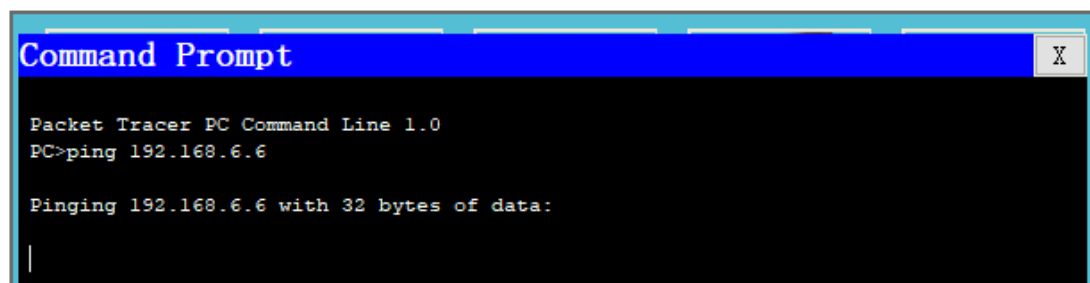
The response to the ping request in the command line of the source node 192.168.3.7: "timeout exceeded".

```
Pinging 192.168.5.6 with 32 bytes of data:

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

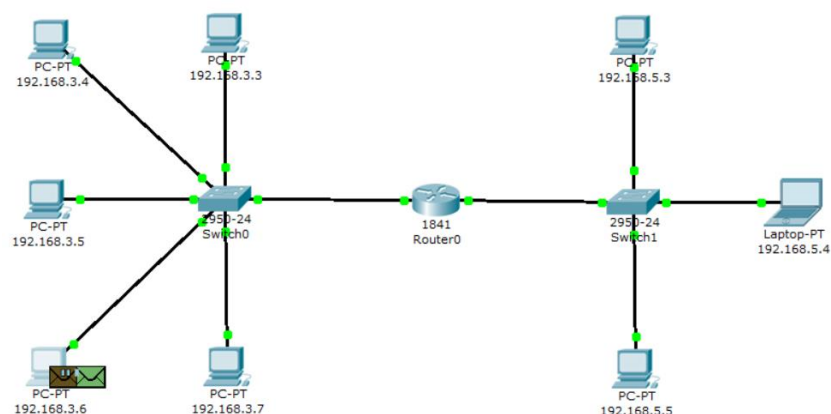
Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

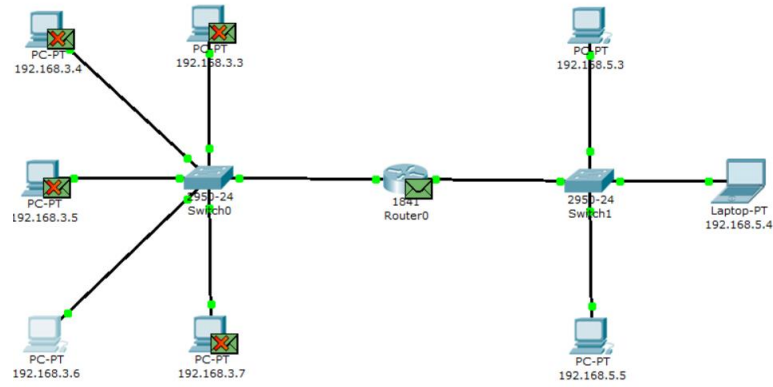


The screenshot shows a 'Command Prompt' window titled 'Packet Tracer PC Command Line 1.0'. The user has entered the command 'PC>ping 192.168.6.6'. The output shows 'Pinging 192.168.6.6 with 32 bytes of data:' followed by a cursor, indicating the ping is in progress or has just finished.

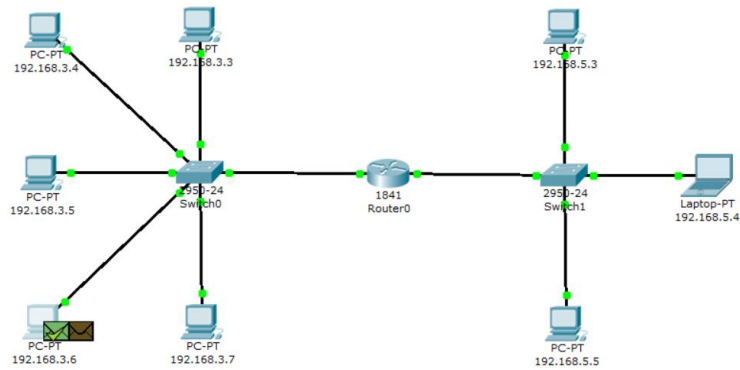
Since the source node's ARP table does not have a corresponding entry, an ARP request is generated for the specified node with the IP address 192.168.6.6.



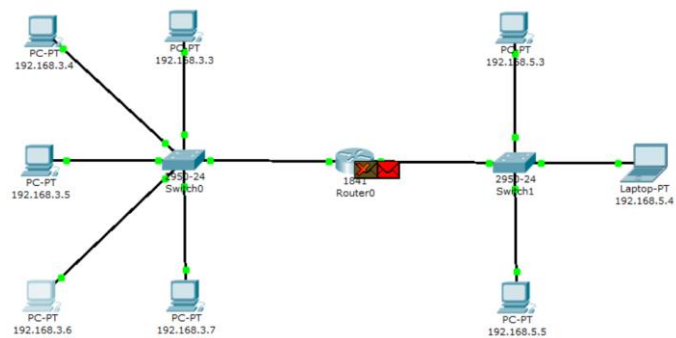
All nodes ignore the packet, except the router that the packet was intended for.



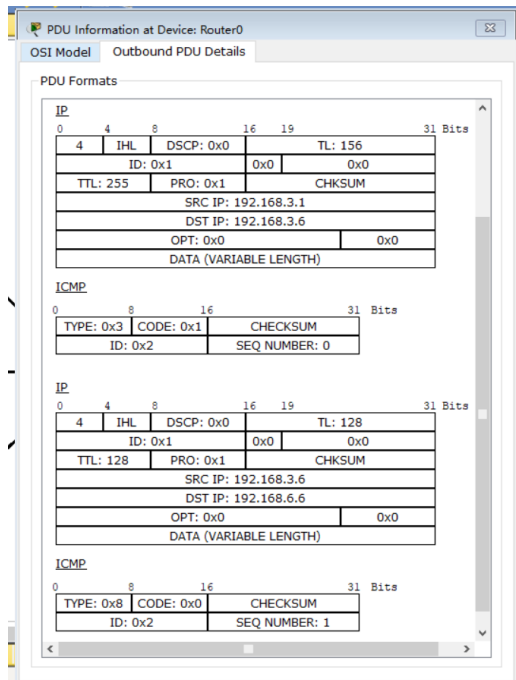
Node 192.168.3.6 receives an ARP response with the MAC address of the router. Now, knowing its hardware address, the host sends a ping request.



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 contents of the packet generated by the router.



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".

```

192.168.3.6
Physical  Config  Desktop  Software/Services

Command Prompt

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),
  
```

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