**2022**

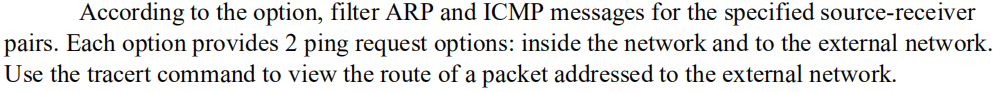
**Contents**

[Task 3](#_Toc5442)

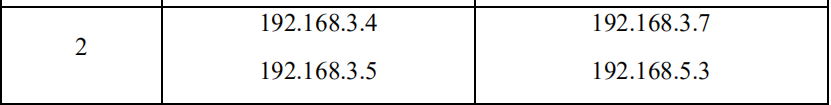
[Work progress 4](#_Toc10486)

[Questions&Conclusions 8](#_Toc12884)

# **Task**

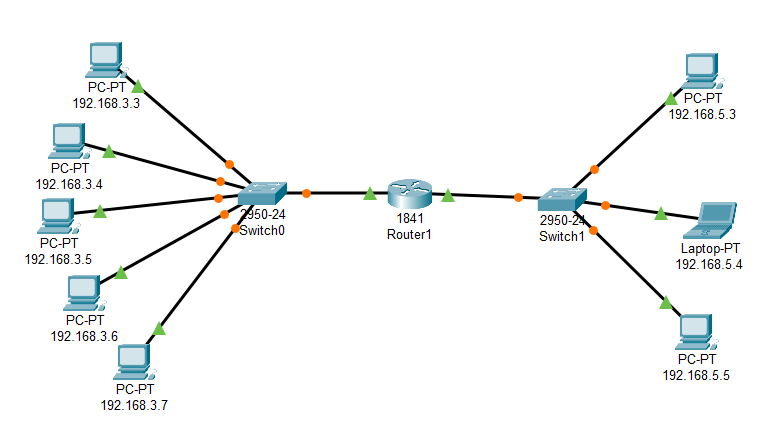


My work variant:



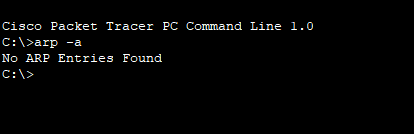
# **Work progress**

The network structure:



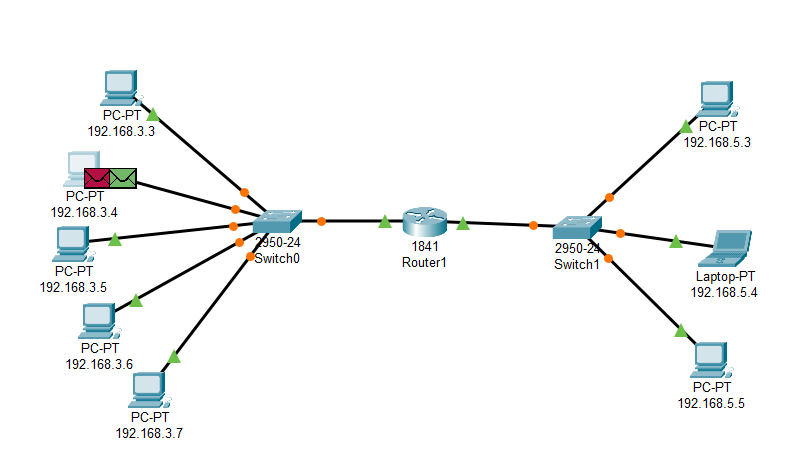
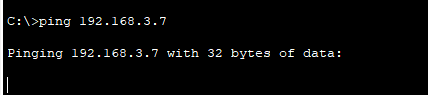
Request1 : 198.168.3.4 => 192.168.3.7

First we check the ARP list:

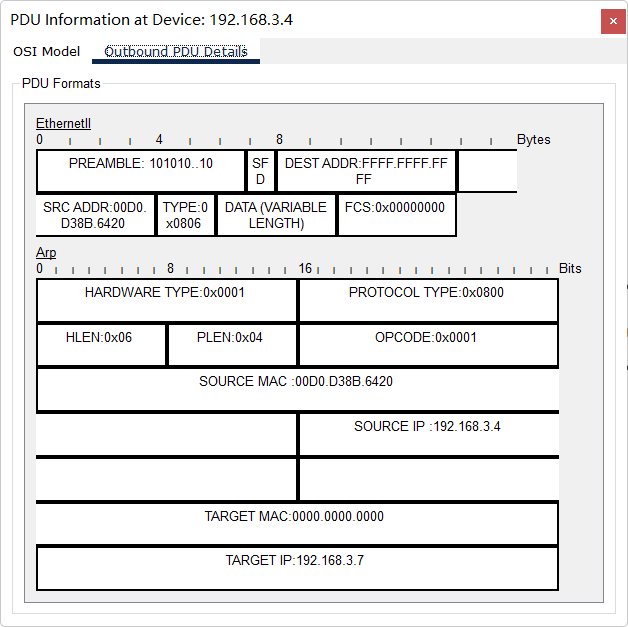


There is no MAC address in the ARP cache.

First, we start the ping function

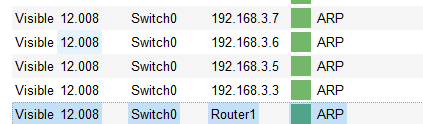
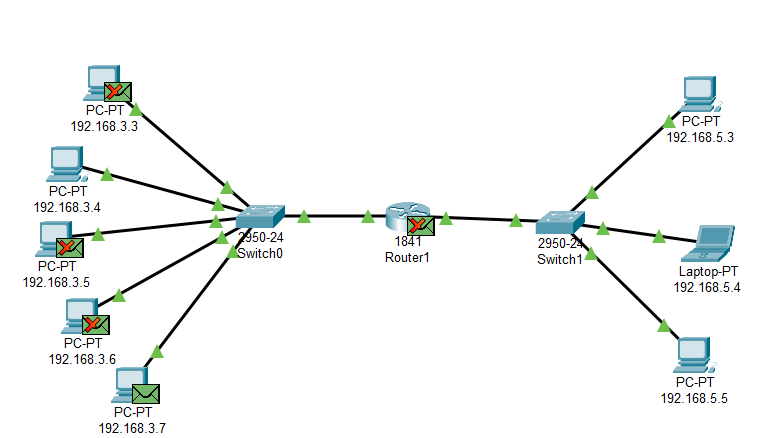


As we don’t know the MAC address of the target IP, a ARP request will go first.The ARP details:

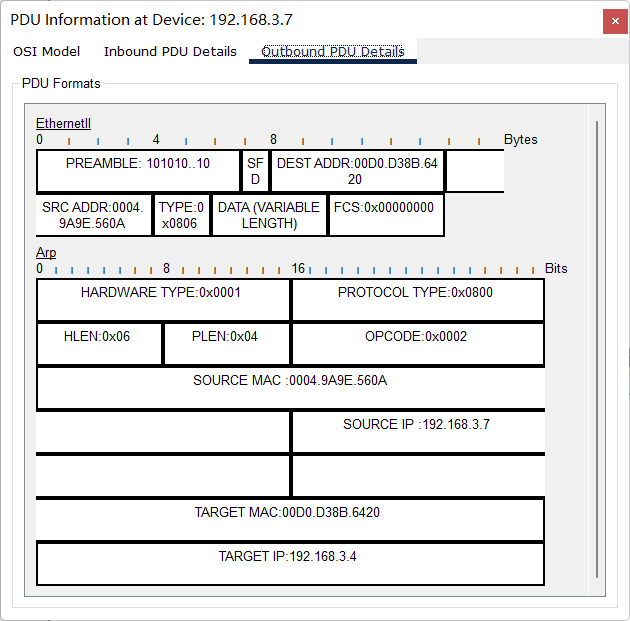
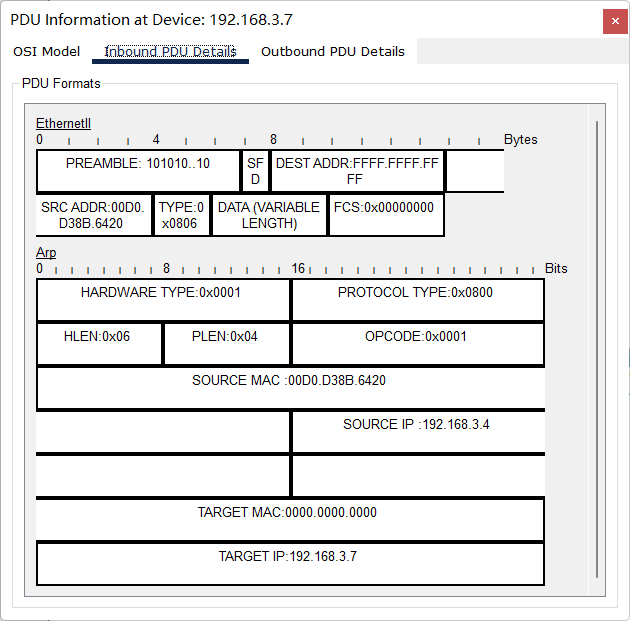


There is no MAC address (replace as 0000.0000.0000), but have the target IP address.

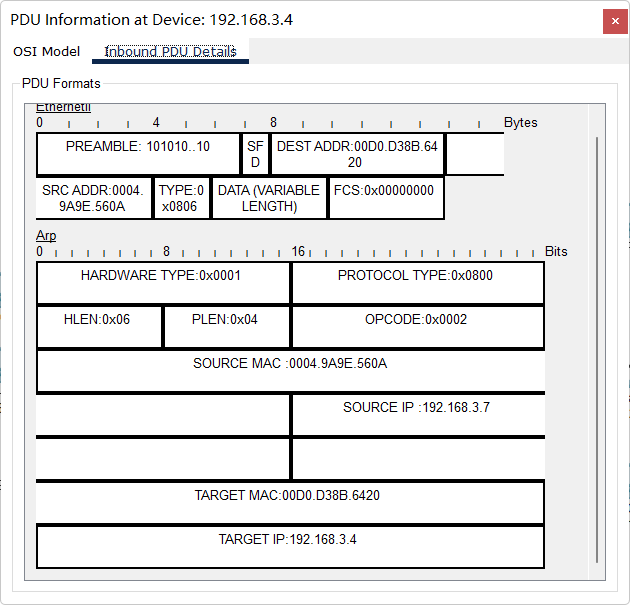
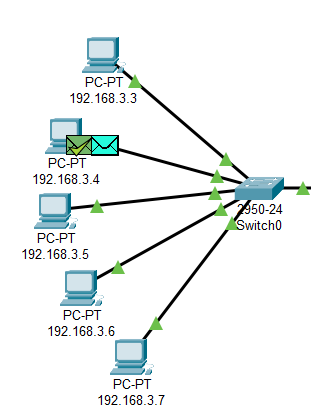
For the next step, the ARP will be broadcasting from the switch, only the right IP address can receive and return the package.



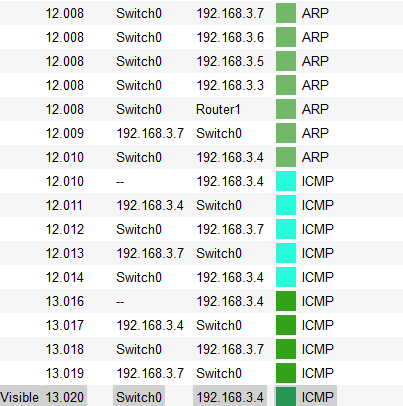
For the package from the 192.168.3.7:



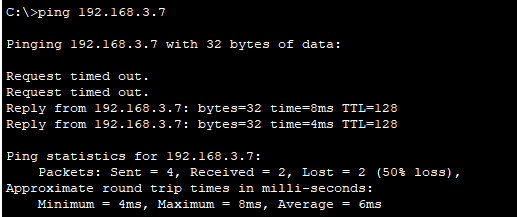
We can find the MAC address of the target has been written into the packages, and is waiting to be sent back to the source IP address.



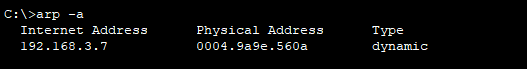
Now the source terminal get the mac address of the target, the ICMP package can be sent to it.



Here we can find the connection is successful.



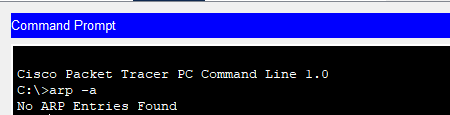
Now we check the ARP cache of the source machine.



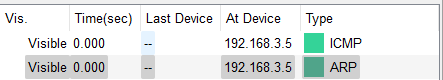
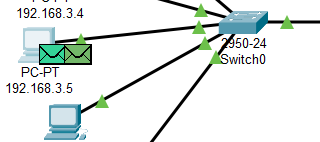
We can find the target mac address has been stored, which means for the after connection, there is no need to broadcasting the ARP request when sent the same information.

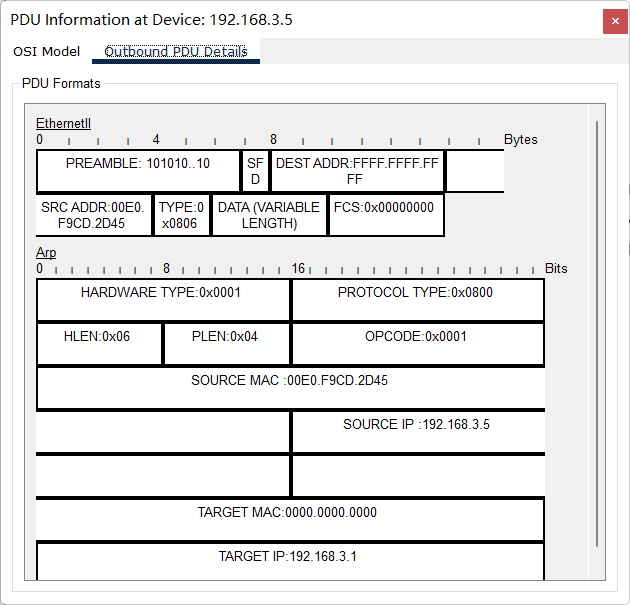
#### Request2 : 198.168.3.5 => 192.168.5.3

First we check the ARP cache.



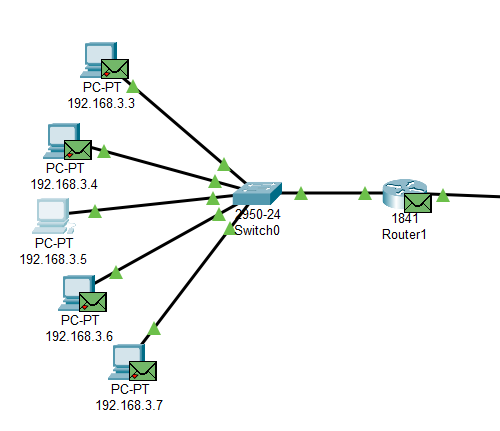
There is no address inside, now we sent the ping request.



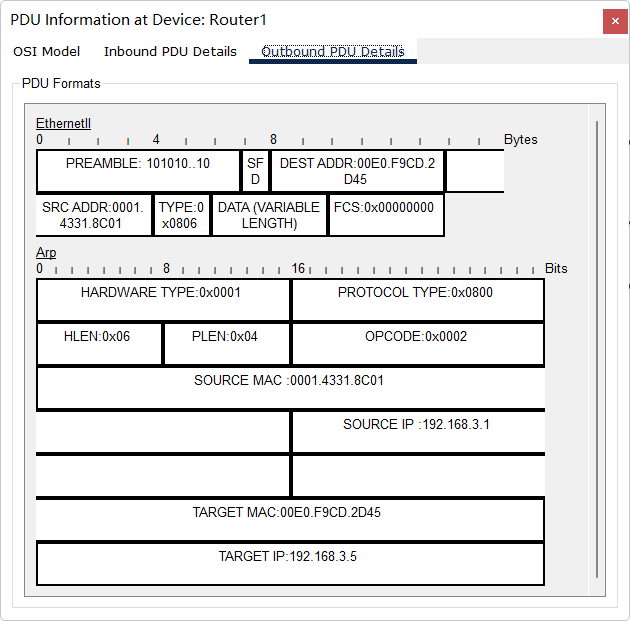
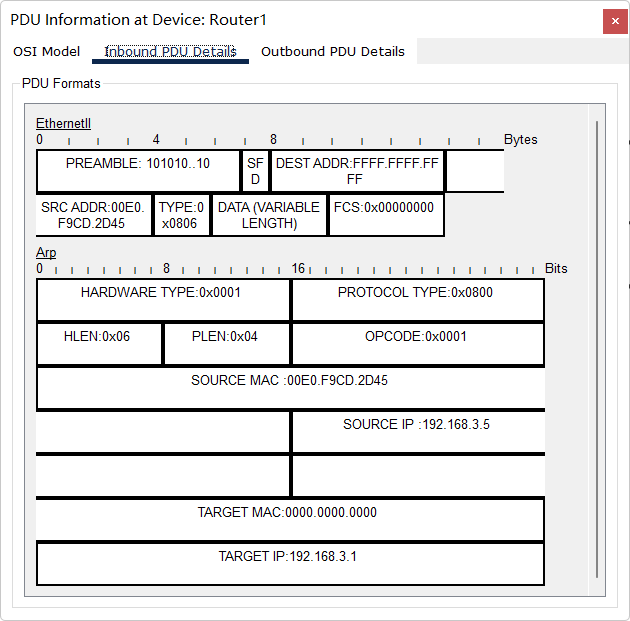


Same as the previous request, because we don’t have the MAC address of the target, we should broadcast the ARP request to find it.

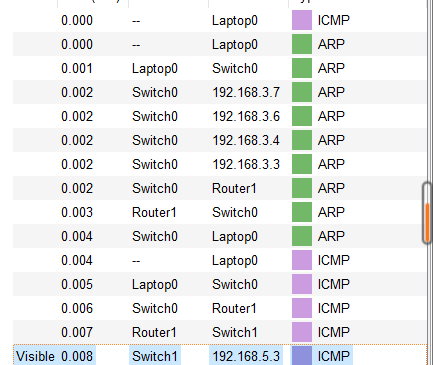
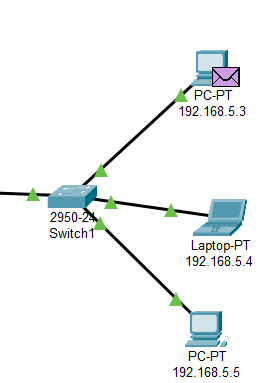
The switcher broadcast it to all the connected devices:



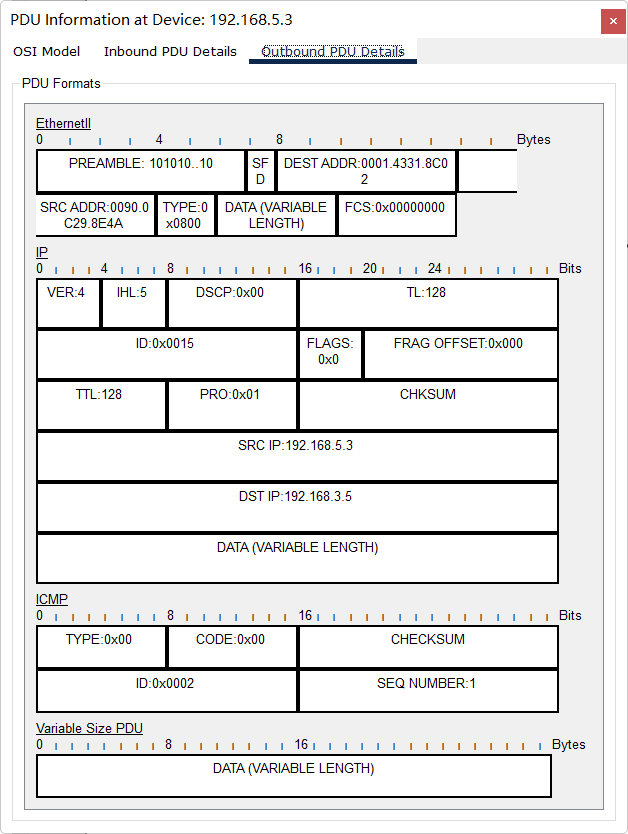
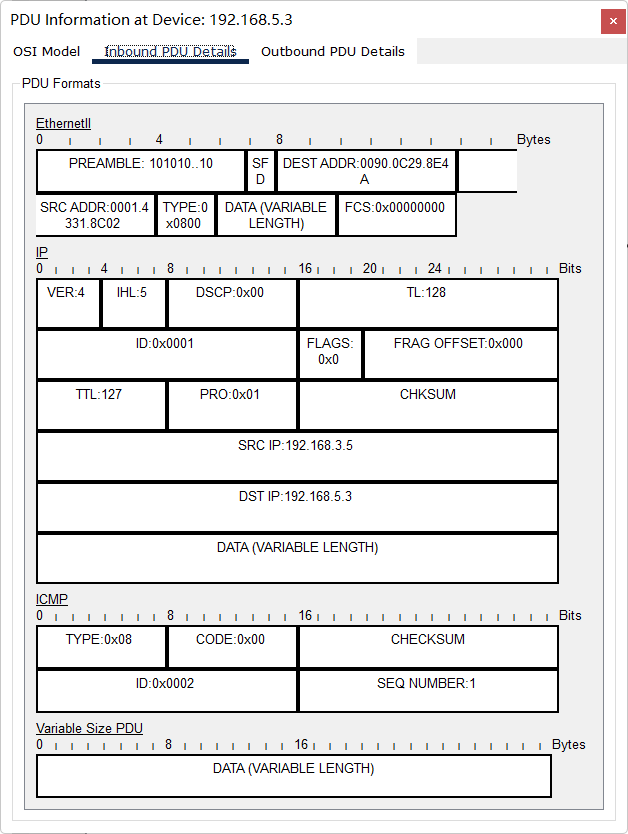
From here we can find only the router can accept the package, as it find the geteway address is inside its cache, so the router will return the package to the source:



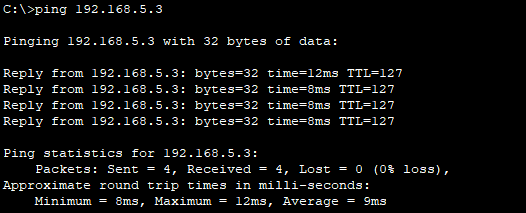
Then the source machine will sent the ICMP request to the target via the MAC address it get.



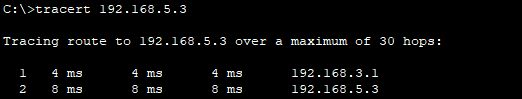
The return package of the ICMP:



Here we get the result of the ping function:



Now we use commend “tarcert” to explain:



To find the MAC address of outer subnet, the source should first get the address from the router, and them send the request within the right address.

# **Conclusions**

To summarize the meaning of the ARP protocol, when the host sends information, it broadcasts the ARP request containing the target IP address to all hosts on the network, and receives the return message to determine the physical address of the target; after receiving the return message, the IP address The ARP cache and the physical address are stored in the local ARP cache and kept for a certain period of time, and the ARP cache is directly queried in the next request to save resources.

There is also a big difference between the two special commands ping and tracert used in this experiment.

Both ping and tracert are used in the same way, adding the IP address or domain name after the command.

ping is mainly used to check the delay and packet loss of the destination address.

tracert is used to view each hop route passed through, and can specifically determine the point at which the delay increases or the packet is lost.

When pinging and checking the website, it is found that the request times out, that is, when the network fails, tracert can be used to find out where the failure occurred. The data that cannot be displayed in the figure below is the node that can be used to determine the problem.